Nokia Corporation

Infinera G42

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This is a non-proprietary cryptographic module security policy for Infinera G42 with firmware version R6.2.2 or R6.2.3 (hereinafter calls the Module). The following details how this module meets the security requirements of FIPS 140-3, SP 800-140 and ISO/IEC 19790 for a Security Level 1 hardware cryptographic module.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Infinera G42 is a next-generation compact modular transport network elements deployed as part of a point-to-point, point-to-multipoint network for terrestrial and/or subsea applications. The G42 chassis provides multi-service client access (e.g. Ethernet, Optical Transport Network (OTN), etc.) to the Dense Wavelength Division Multiplexing (DWDM) transport bandwidth. The module is operated in a limited operational environment.

Module Type: Hardware

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

The module is a multiple-chip standalone hardware cryptographic module. The cryptographic boundary is defined as the entire chassis unit’s physical perimeter encompassing the "top," "front," "left," "right," “rear” and "bottom" surfaces of the case and shown in the figures below and in the Physical Security section. These modules are described in more detail further below in this section.

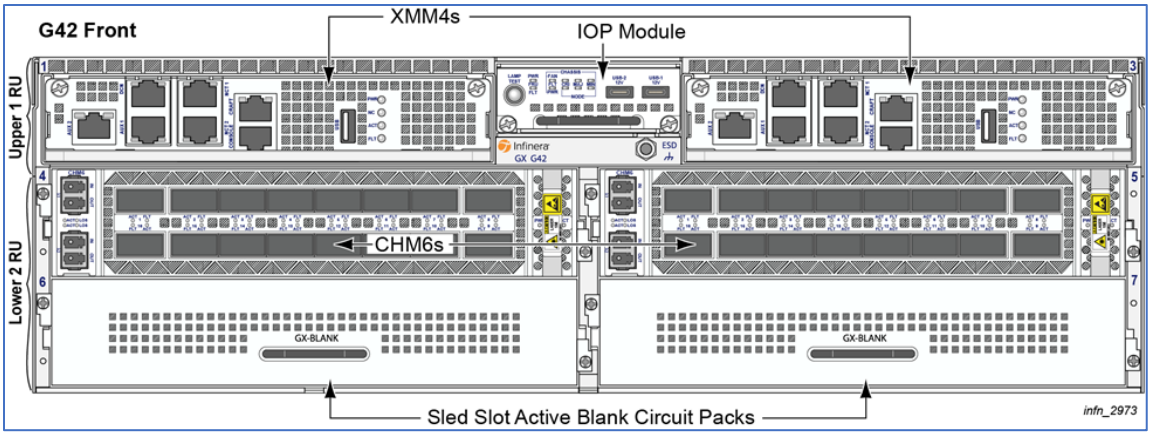

Figure 1: Infinera G42 Module Front View

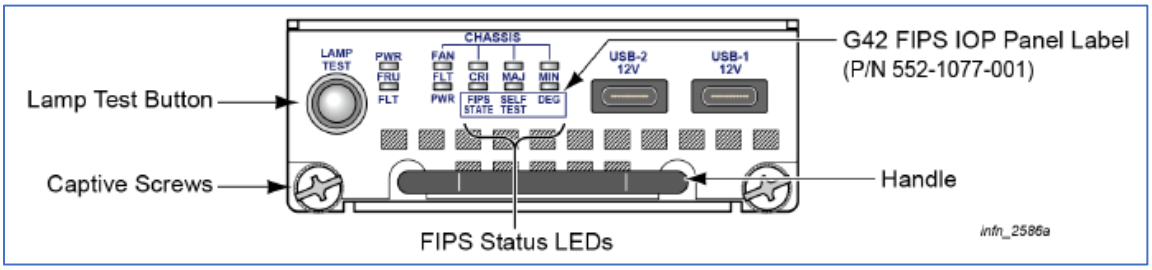

Figure 2: Infinera G42 IOP Card

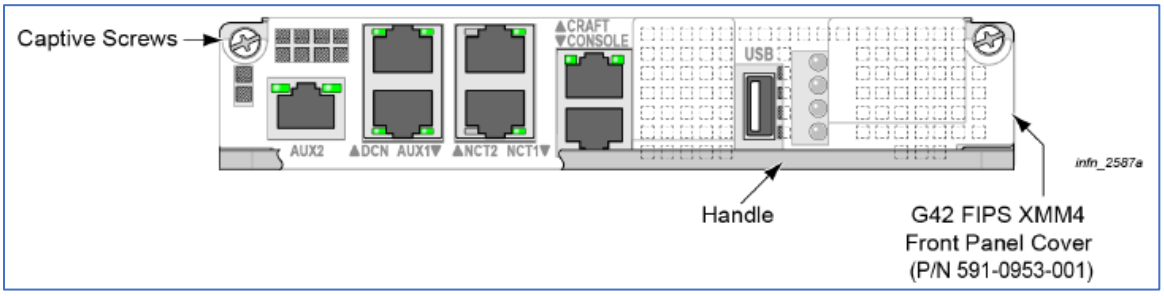

Figure 3: Infinera G42 XMM4 Card

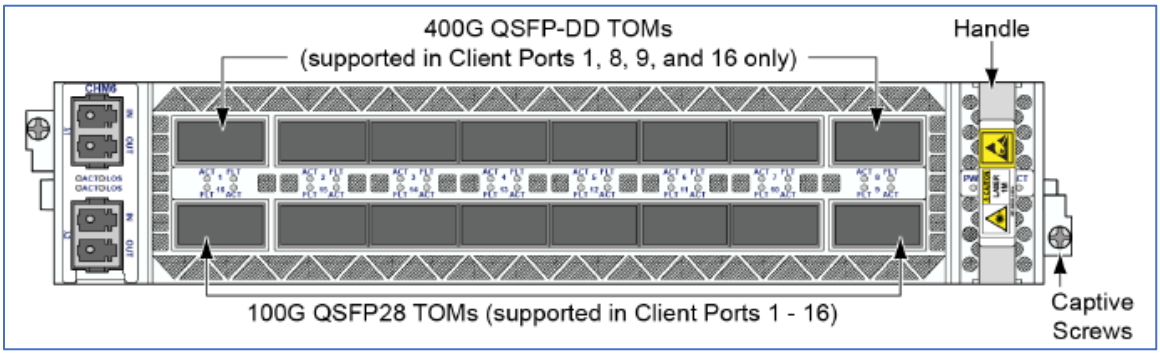

Figure 4: Infinera G42 CHM6 Card

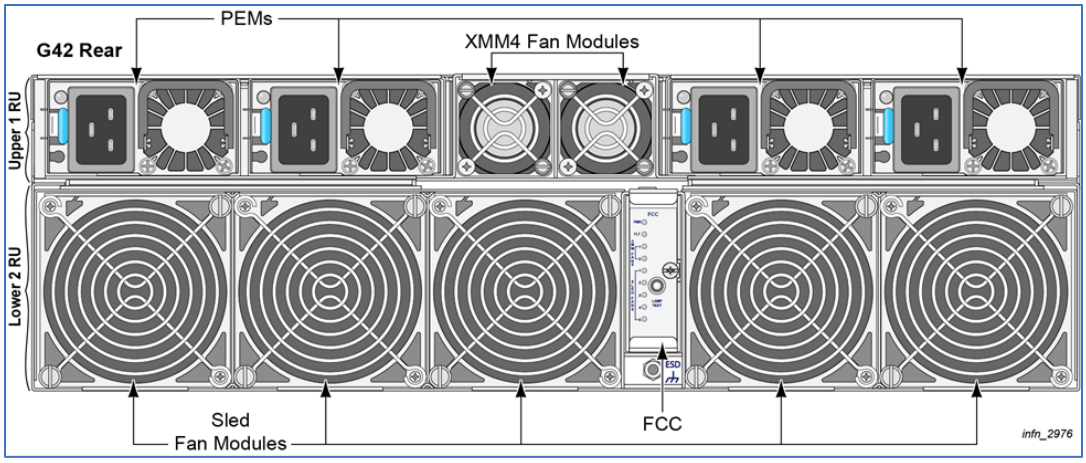

Figure 5**:** Infinera G42 Module Back View

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
G42	Chassis G42, Controller Card XMM4, GX-IOP, Line Card [CHM6-C8, CHM6S-C14, CHM6S-C15 or CHM6-L8], and Filler Plate (GX-BLANK)	R6.2.2 or R6.2.3	Intel Atom C3558, EFR32MG21B010F1024IM32, Zynq UltraScale+ and NXP LS1012	

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

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module is only operated in Approved mode of operation after initial operations are performed	Approved	Approved mode message is displayed via the module's status output interface

Table 3: Modes List and Description

By default, the module is delivered with a non-compliant state but supports an Approved mode of operation. Once the module is configured to operate in the Approved mode of operation by following the steps in section "Secure Operation" of this document by the Crypto Officer, the module can only operate in the Approved mode. The module does not claim implementation of a degraded mode of operation.

The tables in section 2.5 below list all Approved security functions of the module, including specific key size(s) (in bits unless noted otherwise) employed for Approved services, and implemented modes of operation. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in these tables

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4956	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A4958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A4959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A4956	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A4958	Key Length - 128, 192, 256	SP 800-38C
AES-CMAC	A4958	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A4956	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A4958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A4958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	C482	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-GCM	A4956	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A4958	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A4959	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	C501	Direction - Decrypt, Encrypt IV Generation - External Key Length - 256	SP 800-38D
Counter DRBG	A4958	Prediction Resistance - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A4959	Prediction Resistance - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4958	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A4959	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4958	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4959	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3366	Component - No Curve - P-192, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4948	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-4)	A4949	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4952	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4953	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4955	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4956	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4958	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4959	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4960	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4961	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4962	Component - No Curve - P-521 Hash Algorithm - SHA2-512	FIPS 186-4
HMAC-SHA-1	A4956	Key Length - Key Length: 128-512 Increment 128	FIPS 198-1
HMAC-SHA-1	A4958	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4956	Key Length - Key Length: 128-512 Increment 128	FIPS 198-1
HMAC-SHA2-256	A4957	Key Length - Key Length: 64-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4958	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4959	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4956	Key Length - Key Length: 384-1024 Increment 320	FIPS 198-1
HMAC-SHA2-384	A4958	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512	A4956	Key Length - Key Length: 512-1024 Increment 256	FIPS 198-1
HMAC-SHA2-512	A4958	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4959	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4958	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A4959	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A4958	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A4958	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 384-2048 Increment 1664 Derived Keying Material Length - Derived Keying Material Length: 1056, 2432 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF IKEv2 (CVL)	A4959	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 384-2048 Increment 1664 Derived Keying Material Length - Derived Keying Material Length: 1056, 2432 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SNMP (CVL)	A4958	Password Length - Password Length: 64, 96	SP 800-135 Rev. 1
KDF SSH (CVL)	A4958	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
PBKDF	A4958	Iteration Count - Iteration Count: 10-10000 Increment 1 Password Length - Password Length: 8-128 Increment 8	SP 800-132
RSA KeyGen (FIPS186-4)	A4958	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
		Primality Tests - Table C.2 Private Key Format - Standard	
RSA KeyGen (FIPS186-4)	A4959	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4958	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-4)	A4959	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4958	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4959	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A4958	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
SHA-1	A4956	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA-1	A4958	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-256	A3366	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4956	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	A4957	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	A4958	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-256	A4959	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-384	A4956	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A4958	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-512	A4948	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A4949	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A4952	Message Length - Message Length: 1536-4096 Increment 8	FIPS 180-4
SHA2-512	A4953	Message Length - Message Length: 1536-4096 Increment 8	FIPS 180-4
SHA2-512	A4954	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-512	A4955	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-512	A4956	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A4958	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-512	A4959	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-512	A4960	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-512	A4961	Message Length - Message Length: 1536-65536 Increment 8	FIPS 180-4
SHA2-512	A4962	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4958	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A4958	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	SP 800-133r2 Section 4, Method 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)	CKG KAS-KeyGen	KAS ECC KeyGen in SSH, TLS and Control Plane IKEv2 services		Counter DRBG CKG
KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)	CKG KAS-KeyGen	KAS FFC KeyGen in SSH, TLS and Control Plane IKEv2 services		Counter DRBG Safe Primes Key Generation CKG
KAS-ECC-KeyGen (Data Plane IKEv2)	CKG KAS-KeyGen	KAS ECC KeyGen in Data Plane Encryption service		Counter DRBG CKG
KAS-ECC (SSHv2)	KAS-Full	KAS-ECC for SSHv2 service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3 KDF SSH
KAS-FFC (SSHv2)	KAS-Full	KAS-FFC for SSHv2 service	Bit-strength Caveat:Provides between 112 and 200 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3 Domain Parameter Generation Method : MODP-2048, MODP-4096, and MODP-8192 KDF SSH
KAS-ECC (TLSv1.2/v1.3)	KAS-Full	KAS-ECC for TLSv1.2/v1.3 service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3 TLS v1.2 KDF RFC7627 TLS v1.3 KDF
KAS-FFC (TLSv1.2/v1.3)	KAS-Full	KAS-FFC for TLSv1.2/v1.3 service	Bit-strength Caveat:Provides 112 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3 Domain Parameter Generation Method: ffdhe2048 TLS v1.2 KDF RFC7627 TLS v1.3 KDF

Name	Type	Description	Properties	Algorithms
KAS-ECC (Control Plane IKEv2)	KAS-Full	KAS-ECC for Control Plane IKEv2 service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3 KDF IKEv2
KAS-FFC (Control Plane IKEv2)	KAS-Full	KAS-FFC for Control Plane IKEv2 service	Bit-strength Caveat:Provides between 112 and 200 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3 Domain Parameter Generation Method: MODP-2048, MODP-3072, MODP-4096, MODP-6144 and MODP-8192 KDF IKEv2
KAS-ECC (Data Plane IKEv2)	KAS-Full	KAS-ECC for Data Plane IKEv2 service	Bit-strength Caveat:Provides 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3 Curve: P-521 KDF IKEv2
ECDSA KeyGen (SSH, TLS and Control Plane IKEv2)	AsymKeyPair-KeyGen CKG	RSA Keypair generation for SSH, TLS and Control Plane IKEv2 services		ECDSA KeyGen (FIPS186-4) Counter DRBG CKG
ECDSA SigGen (SSH, TLS and Control Plane IKEv2)	DigSig-SigGen	ECDSA SigGen for SSH, TLS and Control Plane IKEv2 services		ECDSA SigGen (FIPS186-4)
ECDSA SigVer (SSH, TLS and Control Plane IKEv2)	DigSig-SigVer	ECDSA SigVer for SSH, TLS and Control Plane IKEv2 services		ECDSA SigVer (FIPS186-4)
RSA KeyGen (SSH, TLS and Control Plane IKEv2)	AsymKeyPair-KeyGen CKG	RSA Keypair generation for SSH, TLS and Control Plane IKEv2 services		RSA KeyGen (FIPS186-4) Counter DRBG CKG
RSA SigGen (SSH, TLS and Control Plane IKEv2)	DigSig-SigGen	RSA SigGen for SSH, TLS and Control Plane IKEv2 services		RSA SigGen (FIPS186-4)
RSA SigVer (SSH, TLS and	DigSig-SigVer	RSA SigVer for SSH, TLS and		RSA SigVer (FIPS186-4)

Name	Type	Description	Properties	Algorithms
Control Plane IKEv2)		Control Plane IKEv2 services		
ECDSA KeyGen (Data Plane IKEv2)	AsymKeyPair-KeyGen CKG	ECDSA Keypair generation for Data Plane IKEv2 services		Counter DRBG ECDSA KeyGen (FIPS186-4) CKG
ECDSA SigGen (Data Plane IKEv2)	DigSig-SigGen	ECDSA SigGen for Data Plane IKEv2 service		ECDSA SigGen (FIPS186-4)
ECDSA SigVer (Data Plane IKEv2)	DigSig-SigVer	ECDSA SigVer for Data Plane IKEv2 service		ECDSA SigVer (FIPS186-4)
RSA KeyGen (Data Plane IKEv2)	AsymKeyPair-KeyGen CKG	RSA Keypair generation for Data Plane IKEv2 services		RSA KeyGen (FIPS186-4) Counter DRBG CKG
RSA SigGen (Data Plane IKEv2)	DigSig-SigGen	RSA SigGen for Data Plane IKEv2 service		RSA SigGen (FIPS186-4)
RSA SigVer (Data Plane IKEv2)	DigSig-SigVer	RSA SigVer for Data Plane IKEv2 service		RSA SigVer (FIPS186-4)
TLS Keying Materials Development	KAS-135KDF	Keying materials, used to derive TLS session keys		TLS v1.2 KDF RFC7627 TLS v1.3 KDF
IPsec/IKEv2 Keying Materials Development	KAS-135KDF	Keying materials, used to derive IPSec/IKE session keys		KDF IKEv2
SNMPv3 Keying Materials Development	KAS-135KDF	Keying materials, used to derive SNMP session keys		KDF SNMP
Block Ciphers (SNMPv3)	BC-UnAuth MAC	Block Ciphers used for SNMPv3 service		AES-ECB HMAC-SHA-1 KDF SNMP SHA-1
Block Ciphers (SSHv2)	BC-Auth BC-UnAuth MAC	Block Cipher for SSHv2 serivce		AES-CBC AES-CTR HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512 SHA-1 SHA2-256

Name	Type	Description	Properties	Algorithms
				SHA2-512 AES-GCM
Block Ciphers (TLSv1.2/v1.3)	BC-Auth BC-UnAuth MAC	Block Cipher used for TLSv1.2/v1.3 service		AES-CBC AES-GCM HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 SHA2-256 SHA2-384 SHA2-512
Block Ciphers (Control Plane IKEv2)	BC-Auth BC-UnAuth MAC	Block Ciphers for Control Plane IKEv2 service		AES-CBC AES-CCM AES-GCM AES-CBC AES-CCM AES-GCM AES-CTR AES-CTR HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 SHA-1 SHA2-256 SHA2-384 SHA2-512 SHA-1 SHA2-256 SHA2-384 SHA2-512
Block Cipher (Data Plane IKEv2)	BC-Auth	Block Cipher for Data Plane IKEv2 service		AES-GCM AES-GCM AES-CBC HMAC-SHA2-256 HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				512 SHA2-256 SHA2-512 AES-ECB
SSH KTS (AES and HMAC)	KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	AES-CBC AES-CTR HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512 SHA-1 SHA2-256 SHA2-512
SSH KTS (GCM)	KTS-Wrap	KTS via SSHv2 service by using AES-GCM	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	AES-GCM
TLS KTS (AES and HMAC)	KTS-Wrap	KTS via TLSv1.2/v1.3 service by using AES and HMAC	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	AES-CBC HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 SHA2-256 SHA2-384 SHA2-512
TLS KTS (GCM)	KTS-Wrap	KTS via TLSv1.2/v1.3 service by using GCM	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	AES-GCM
OSPFv2 Authentication	MAC	OSPFv2 authentication		HMAC-SHA2-256 SHA2-256
LUKS Database Protection	MAC	Database integrity protection using HMAC-SHA2-512		SHA2-512 HMAC-SHA2-512 PBKDF
Firmware Load Test	DigSig-SigVer	ECDSA SigVer for firmware load test		ECDSA SigVer (FIPS186-4) Curve: P-521

Name	Type	Description	Properties	Algorithms
NTP Authentication	MAC	NTP authentication		SHA-1 SHA2-256 AES-CMAC
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG Counter DRBG
Firmware Integrity Test	DigSig-SigVer	Used for firmware integrity test		ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) SHA2-512 ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) SHA2-256 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

- The IV for AES-GCM is constructed in compliance with IG C.H scenario 1a (TLSv1.2). For TLS 1.2, the module offers the AES-GCM implementation and uses the context of Scenario 1a of IG C.H. The module is compliant with SP 800-52r2 section 3.3.1 and the mechanism for IV generation is compliant with RFC5288. The module's implementation

of AES-GCM is compliant to IG C.H option i) where module implements TLS protocol. The design of the TLS protocol implicitly ensures that the counter (the nonce_explicit part of the IV) does not exhaust the maximum number of possible values for a given session key. In the event the module's power is lost and restored, the consuming application must ensure that a new key for use with the AES-GCM key encryption or decryption under this scenario shall be established.

- For TLS 1.3, the Module offers the AES-GCM implementation and uses the context of Scenario #5 of FIPS 140-3 IG C.H. The protocol that provides this compliance is TLS 1.3, defined in RFC8446 of August 2018, using the cipher suites that explicitly select AES-GCM as the encryption/decryption cipher (Appendix B.4 of RFC8446). The Module supports acceptable AES-GCM cipher suites from Section 3.3.1 of SP800-52 Rev2. The Module implements, within its boundary, an IV generation unit for TLS 1.3 that keeps control of the 64-bit counter value within the AES-GCM IV. If the exhaustion condition is observed, the Module will return an error indication to the calling application, who will then need to either trigger a re-key of the session (i.e., a new key for AES-GCM), or terminate the connection.

- The IV for AES-GCM is constructed in compliance with IG C.H scenario 1a (IPsec-v3). This IV generation of IPsec AES-GCM implementation is compliant with RFC 4106 and an IKEv2 protocol RFC7296 shall be used to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. The IPsec AES-GCM IV is only be used in the context of the AES GCM mode encryptions within the IPsec protocol. In case the Module's power is lost and then restored, the key used for IPsec AES-GCM shall be regenerated.

- The PBKDF aligns with Option 1a in Section 5.4 of SP 800-132. The PBKDF algorithm parameters are: Password length 512 bits long, Salt length 256 bits long, and the number of iterations is 598502. The resulting key material is only used for storage applications.

- The module was algorithm tested based on the FIPS 186-4 standard for Digital Signatures. According to IG C.K, this module is 186-5 compliant as all 186-4 CAVP tests performed are mathematically identical to the 186-5 CAVP tests. The Module does not support 186-4 DSA or RSA X9.31 for Signature Generation or Signature Verification.

- In accordance with FIPS 140-3 IG D.H, the cryptographic Module performs Cryptographic Key Generation as per section 5 in SP800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90Arev1 DRBG.

2.8 RBG and Entropy

Cert Number	Vendor Name
E156	Silicon Laboratories

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
EFR32MG21B010F1024IM32	Physical	B with SE Firmware Version 1.2.13	128 bits	Full entropy	A3366 (AES-CBC-MAC)

Table 8: Entropy Sources

The module implements two approved CTR_DRBGs based on SP800-90Arev1, with Algo Certs. #A4958 and #A4959.

Each DRBG is used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions).

The DRBG is seeded by the entropy source described in the table above. The CTR_DRBG (AES-128/192/256) enables Derivation Function capability. The DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy) and provides at least 256 bits security strength for the following cryptographic keys generation.

The entropy source implementation generates an output that is considered to have full entropy. More information can be found in the public use document for ESV cert #E156.

2.9 Key Generation

The module generates RSA, ECDSA, EC Diffie-Hellman, and Diffie-Hellman asymmetric key pairs compliant with FIPS 186-4, using a NIST SP 800-90Arev1 CTR DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H.).

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

- KAS-FFC Shared Secret Computation:
  - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 200 bits of encryption strength.

  - The module supports the use of the safe primes defined in RFC 4419 (SSH), RFC 7919 (TLS) and RFC 3526 (IKE).

    - SSH (RFC 4419):

MODP-2048 (ID = 14)
MODP-4096 (ID = 16)
MODP-8192 (ID = 18)

- TLS (RFC 7919):
ffdhe2048 (ID = 256)

- IKE (RFC 3526):
MODP-2048 (ID = 14)
MODP-3072 (ID = 15)
MODP-4096 (ID = 16)
MODP-6144 (ID = 17)
MODP-8192 (ID = 18)

- KAS-ECC Shared Secret Computation:
  - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.

2.11 Industry Protocols

The module supports SSHv2, TLS v1.2, TLSv1.3, SNMPv3 and IKEv2 industrial protocols. No parts of SSH, TLS, SNMP and IKEv2 protocols, other than the KDFs, have been tested by the CAVP and CMVP. Please refer to SSPs Table for more information.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Ethernet Ports and Optical Ports on CHM6 Card; DCN, CRAFT, CONSOLE, AUX 1 & AUX 2 Ports on XMM4 Card	Data Input	Plaintext/Ciphertext Data input to the module for all approved services defined in the approved services table
Ethernet Ports and Optical Ports on CHM6 Card; DCN, CRAFT, CONSOLE, AUX 1 & AUX 2 Ports on XMM4 Card	Data Output	Plaintext/Ciphertext Data output from the module for all approved services defined in the approved services table
DCN, CRAFT, CONSOLE, AUX 1 & AUX 2 Ports on XMM4 Card; Lamp Test on IOP Card	Control Input	Control information input into the module for all the services defined in the approved services table
DCN, CRAFT, CONSOLE, AUX 1 & AUX 2 Ports on XMM4 Card, and LEDs	Status Output	Status Information output from the module for all the services defined in the approved services table
Power Interface	Power	Power supply

Table 9: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides physical ports which are mapped to logical interfaces provided by the module (data input, data output, control input, control output and status output) as above. The module's data output interface will be disabled when performing pre-operational self-tests, loading new firmware, zeroizing keys, or when in an error state.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password-based Authentication	The minimum length is eight (8) characters (94 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000. As the module supports at most ten failed attempts to authenticate in a one-minute period, the probability of successfully authenticating to the module within one minute is 10/(94^8), which is less than 1/100,000. This calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total.	Password Based	The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8). Please refer to Description section in this table for more details	The probability of successfully authenticating to the module within one minute is 10/(94^8). Please refer to Description section in this table for more details

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
RSA-based Authentication	The modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits, which provides 112 bits of security strength. The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112), which is less than 1/100,000.	RSA SigVer (FIPS186-4) (A4958)	The probability that a random attempt will succeed is 1/(2^112). Please refer to Description section in this table for more details	the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112). Please refer to Description section in this table for more details
ECDSA-based Authentication	The modules support ECDSA public-key based authentication mechanism using a minimum of curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new	ECDSA SigVer (FIPS186-4) (A4958)	The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. Please refer to Description section in this table for more details	the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128). Please refer to Description section in this table for more details

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128), which is less than 1/100,000.			

Table 10: Authentication Methods

The module supports identity-based authentication mechanism. The module supports the multiple Crypto Officer roles and User roles. Each role is authenticated by the module upon initial access to the module, as detailed below.

Crypto Officer Roles:

- Security Admin (SA): This role performs all security functions provided by the module. This role has read and write access to all security related operations, full access to security management model, remote server configurations. Implements all operations to manage the creation, enabling / disabling of new Users and Passwords, User session monitoring, and configuration.

- Network Admin (NA): This role has read and write access to overall system configuration. For example, DCN / networking infrastructure / software and firmware configuration and upgrade schedules or management interface configurations.

- Encryption Admin (EA): This role has permissions to configure the data and control plane encryption functions.

User Roles:

- Network Engineer (NE): This role has basic non-security related read and write access to equipment and traffic management model. For example, PM data, connectivity, provisioning status.

- Monitoring Access (MA): This role has read-only access to equipment and traffic management model. For example, PM data, connectivity, provisioning status.

- Provisioning (PR): This role has permissions to monitor the module, configure facility endpoints, and provision services. For example, provisioning of equipment and facility end-points.

- Turn-up and Test (TT): This role has required permissions for monitor, turn-up, and troubleshoot the module fix network problems.

The module also allows the concurrent operators.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Security Admin (SA)	Identity	Crypto Officer	Password-based Authentication RSA-based Authentication ECDSA-based Authentication
Network Admin (NA)	Identity	Crypto Officer	Password-based Authentication RSA-based Authentication ECDSA-based Authentication
Encryption Admin (EA)	Identity	Crypto Officer	Password-based Authentication RSA-based Authentication ECDSA-based Authentication
Network Engineer (NE)	Identity	User	Password-based Authentication RSA-based Authentication ECDSA-based Authentication
Monitoring Access (MA)	Identity	User	Password-based Authentication RSA-based Authentication ECDSA-based Authentication
Provisioning (PR)	Identity	User	Password-based Authentication RSA-based Authentication ECDSA-based Authentication
Turn-up and Test (TT)	Identity	User	Password-based Authentication RSA-based Authentication ECDSA-based Authentication

Table 11: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Version	Show module's ID and versioning information	N/A	Command used to show module's version	Module's ID and versioning information	None	Security Admin (SA) Network Admin (NA) Encryption Admin (EA) Network Engineer (NE) Monitoring Access (MA) Provisioning (PR) Turn-up and Test (TT)
Show Status	Show module's operational status	N/A	Command used to show Module's Status	Module's operational status	None	Security Admin (SA) Network Admin (NA) Encryption Admin (EA) Network Engineer (NE) Monitoring Access (MA) Provisioning (PR) Turn-up and Test (TT)
User Account Management	User account management	N/A	Command to manage the User account	Status of User account	None	Security Admin (SA) - Operator Password: G,R,W,Z - SSH RSA Public Key: G,R,W,Z - SSH ECDSA Public Key: G,R,W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Certificates Management	Certificates Management	N/A	Commands used to manage the certificates	Status of the completion of network configuration status	None	Security Admin (SA) - SSH ECDSA Private Key: G,R,W,E,Z - SSH ECDSA Public Key: G,R,W,E,Z - SSH RSA Private Key: G,R,W,E,Z - SSH RSA Public Key: G,R,W,E,Z - TLS ECDSA Private Key: G,R,W,E,Z - TLS ECDSA Public Key: G,R,W,E,Z - TLS RSA Private Key: G,R,W,E,Z - TLS RSA Public Key: G,R,W,E,Z - IPSec/IKE ECDSA Private Key: G,R,W,E,Z - IPSec/IKE ECDSA Public Key: G,R,W,E,Z - IPSec/IKE RSA Private Key: G,R,W,E,Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						RSA Public Key: G,R,W,E,Z - Data Plane Encryption ECDSA Private Key: G,R,W,E,Z - Data Plane Encryption ECDSA Public Key: G,R,W,E,Z - Data Plane Encryption RSA Private Key: G,R,W,E,Z - Data Plane Encryption RSA Public Key: G,R,W,E,Z
Setup Network (non-security relevant)	Commands to configure the non-security relevant network	N/A	Commands to configure the network	Status of the completion of network configuration status	None	Network Admin (NA) Provisioning (PR) Turn-up and Test (TT)
Enable/disable approved mode	Enable/disable approved mode	N/A	Command used to enable or disable approved mode	Module's approved mode status	None	Security Admin (SA)
Configure Network Access Control List	Configure network access control list	N/A	Commands used to configure network access control list	Network access control list configuration status	None	Security Admin (SA)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure Performance Monitoring Service	Configure Performance Monitoring Service	N/A	Commands used to configure performance monitoring service	performance monitoring service configuration status	None	Network Admin (NA) Turn-up and Test (TT)
Configure Equipment	Provision equipment	N/A	Commands used to configue equipment	Equipment configuration status	None	Network Admin (NA) Network Engineer (NE)
Configure Facilities (physical or logical Interfaces)	Configure Facilities (physical or logical interfaces)	N/A	Commands to configure the module's physical or logical interfaces	Module's physical or logical interfaces configruaiton status	None	Network Admin (NA) Provisioning (PR) Turn-up and Test (TT)
Perform Self-Test	Perform self-tests	N/A	Command to trigger self-tests	Self-tests completion status	Firmware Integrity Test	Security Admin (SA) Network Admin (NA) Encryption Admin (EA) Network Engineer (NE) Monitoring Access (MA) Provisioning (PR) Turn-up and Test (TT)
Firmware Update	Perform firmware update	Firmware update service completion status	Command to trigger firmware update	Firmware update status	Firmware Load Test	Network Admin (NA) - Firmware Load Test Key: R,E
Perform Zeroization	Zeroize all SSPs in the module	N/A	Command to zeroize the module	SSPs zeroization status	None	Security Admin (SA) - DRBG Entropy Input: Z - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Seed: Z - DRBG Internal State V value: Z - DRBG Key: Z - Operator Password: Z - LUKS DB Password: Z - LUKS DB Salt : Z - LUKS DB Integrity Key : Z - SSH DH Private Key: Z - SSH DH Public Key: Z - SSH Peer DH Public Key: Z - SSH DH Shared Secret: Z - SSH ECDH Private Key: Z - SSH ECDH Public Key: Z - SSH Peer ECDH Public Key: Z - SSH ECDH Shared Secret: Z - SSH ECDSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - SSH ECDSA Public Key: Z - SSH RSA Private Key: Z - SSH RSA Public Key: Z - SSH Encryption Key: Z - SSH Integrity Key: Z - TLS DH Private Key: Z - TLS DH Public Key: Z - TLS Peer DH Public Key: Z - TLS DH Shared Secret: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z - TLS Peer ECDH Public Key: Z - TLS ECDH Shared Secret: Z - TLS ECDSA Private Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS ECDSA Public Key: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS Master Secret: Z - TLS Encryption Key: Z - TLS Integrity Key: Z - IPSec/IKE DH Private Key: Z - IPSec/IKE DH Public Key: Z - IPSec/IKE Peer DH Public Key: Z - IPSec/IKE DH Shared Secret: Z - IPSec/IKE ECDH Private Key: Z - IPSec/IKE ECDH Public Key: Z - IPSec/IKE Peer ECDH Public Key: Z - IPSec/IKE ECDH Shared Secret: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- IPSec/IKE ECDSA Private Key: Z - IPSec/IKE ECDSA Public Key: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE Pre-shared Secret: Z - IPSec/IKE SKEYSEED: Z - IPSec/IKE Encryption Key: Z - IPSec/IKE Integrity Key: Z - SNMPv3 Encryption Key: Z - SNMPv3 Integrity Key: Z - Data Plane Encryption Pre-shared Secret: Z - Data Plane Encryption ECDH Private Key: Z - Data Plane Encryption ECDH Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - Data Plane Encryption Peer ECDH Public Key: Z - Data Plane Encryption ECDH Shared Secret: Z - Data Plane Encryption ECDSA Private Key: Z - Data Plane Encryption ECDSA Public Key: Z - Data Plane Encryption RSA Private Key: Z - Data Plane Encryption RSA Public Key: Z - Data Plane Encryption IKE-SA Session Key: Z - Data Plane Encryption Child-SA Session Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SNMPv3 Authentication Secret: Z
Configure SSHv2 service	Configure SSHv2 service	Global approved mode indicator and SSHv2 service configuration status	Commmands used to configure SSHv2 service	SSHv2 service configuration status	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-ECC (SSHv2) KAS-FFC (SSHv2) ECDSA KeyGen (SSH, TLS and Control Plane IKEv2) ECDSA SigGen (SSH, TLS and Control Plane IKEv2) ECDSA SigVer (SSH, TLS and Control Plane IKEv2) RSA KeyGen (SSH, TLS and Control Plane IKEv2) RSA SigGen (SSH, TLS and Control Plane	Security Admin (SA) - SSH DH Private Key: W,Z - SSH DH Public Key: W,Z - SSH Peer DH Public Key: W,Z - SSH DH Shared Secret: W,Z - SSH ECDH Private Key: W,Z - SSH ECDH Public Key: W,Z - SSH Peer ECDH Public Key: W,Z - SSH ECDH Shared Secret: W,Z - SSH ECDSA Private Key: W,Z - SSH ECDSA Public Key: W,Z - SSH RSA Private Key: W,Z - SSH RSA Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					IKEv2) RSA SigVer (SSH, TLS and Control Plane IKEv2) Block Ciphers (SSHv2) SSH KTS (AES and HMAC) SSH KTS (GCM) DRBG Function	W,Z - SSH Encryption Key: W,Z - SSH Integrity Key: W,Z - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V value: W,Z - DRBG Key: W,Z
Configure TLS (v1.2/v1.3) Service	Configure TLS (v1.2/v1.3) service	Global approved mode indicator and OSPF service configuration status	Commmands used to configure TLS (v1.2/v1.3) service	TLS (v1.2/v1.3) service configuration status	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-ECC (TLSv1.2/v1.3) KAS-FFC (TLSv1.2/v1.3) ECDSA KeyGen (SSH, TLS and Control Plane IKEv2) ECDSA SigGen (SSH, TLS and Control Plane IKEv2) ECDSA	Security Admin (SA) - TLS DH Private Key: W,Z - TLS DH Public Key: W,Z - TLS Peer DH Public Key: W,Z - TLS DH Shared Secret: W,Z - TLS ECDH Private Key: W,Z - TLS ECDH Public Key: W,Z - TLS Peer ECDH Public Key: W,Z - TLS ECDH Shared Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SigVer (SSH, TLS and Control Plane IKEv2) RSA KeyGen (SSH, TLS and Control Plane IKEv2) RSA SigGen (SSH, TLS and Control Plane IKEv2) RSA SigVer (SSH, TLS and Control Plane IKEv2) Block Ciphers (TLSv1.2/v1.3) TLS KTS (AES and HMAC) TLS KTS (GCM) DRBG Function TLS Keying Materials Development	W,Z - TLS ECDSA Private Key: W,Z - TLS ECDSA Public Key: W,Z - TLS RSA Private Key: W,Z - TLS RSA Public Key: W,Z - TLS Master Secret: W,Z - TLS Encryption Key: W,Z - TLS Integrity Key: W,Z - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V value: W,Z - DRBG Key: W,Z
Configure SNMP service	Configure SNMP service	Global approved mode indicator and SNMP service configuration status	Commmands used to configure SNMP service	SNMP service configuration status	Block Ciphers (SNMPv3) SNMPv3 Keying Materials Development	Security Admin (SA) - SNMPv3 Authentication Secret: W,Z - SNMPv3 Encryption Key: W,Z - SNMPv3 Integrity Key: W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure Control Plane IPSec/IKEv2 Service	Configure Control Plane IPSec/IKEv2 Service	Global approved mode indicator and Control Plane IPSec/IKEv2 service configuration status	Commmands used to configure Control Plane IPSec/IKEv2 service	Control Plane IPSec/IKEv2 service configuration status	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-ECC (Control Plane IKEv2) KAS-FFC (Control Plane IKEv2) ECDSA KeyGen (SSH, TLS and Control Plane IKEv2) ECDSA SigGen (SSH, TLS and Control Plane IKEv2) ECDSA SigVer (SSH, TLS and Control Plane IKEv2) RSA KeyGen (SSH, TLS and Control Plane IKEv2) RSA SigGen (SSH, TLS and Control Plane	Security Admin (SA) - IPSec/IKE DH Private Key: W,Z - IPSec/IKE DH Public Key: W,Z - IPSec/IKE Peer DH Public Key: W,Z - IPSec/IKE DH Shared Secret: W,Z - IPSec/IKE ECDH Private Key: W,Z - IPSec/IKE ECDH Public Key: W,Z - IPSec/IKE Peer ECDH Public Key: W,Z - IPSec/IKE ECDH Shared Secret: W,Z - IPSec/IKE ECDSA Private Key: W,Z - IPSec/IKE ECDSA Public Key: W,Z - IPSec/IKE RSA Private Key: W,Z - IPSec/IKE RSA Public Key: W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					IKEv2) RSA SigVer (SSH, TLS and Control Plane IKEv2) Block Ciphers (Control Plane IKEv2) DRBG Function IPsec/IKEv2 Keying Materials Development	- IPSec/IKE Pre-shared Secret: W,Z - IPSec/IKE SKEYSEED: W,Z - IPSec/IKE Encryption Key: W,Z - IPSec/IKE Integrity Key: W,Z - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V value: W,Z - DRBG Key: W,Z
Configure Data Plane Encryption Service	Configure Data Plane Encryption Service	Global approved mode indicator and Data Plane Encryption service configuration status	Commmands used to configure Data Plane Encryption service	Data Plane Encryption service configuration status	KAS-ECC-KeyGen (Data Plane IKEv2) KAS-ECC (Data Plane IKEv2) ECDSA KeyGen (Data Plane IKEv2) ECDSA SigGen (Data Plane IKEv2) ECDSA SigVer (Data Plane IKEv2) RSA KeyGen (Data Plane IKEv2) RSA SigGen	Encryption Admin (EA) - Data Plane Encryption ECDH Private Key: W,Z - Data Plane Encryption ECDH Public Key: W,Z - Data Plane Encryption Peer ECDH Public Key: W,Z - Data Plane Encryption ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(Data Plane IKEv2) RSA SigVer (Data Plane IKEv2) Block Cipher (Data Plane IKEv2) DRBG Function	Shared Secret: W,Z - Data Plane Encryption ECDSA Private Key: W,Z - Data Plane Encryption ECDSA Public Key: W,Z - Data Plane Encryption RSA Private Key: W,Z - Data Plane Encryption RSA Public Key: W,Z - Data Plane Encryption Pre-shared Secret: W,Z - Data Plane Encryption IKE-SA Session Key: W,Z - Data Plane Encryption Child-SA Session Key: W,Z - DRBG Entropy Input: W,Z - DRBG Seed: W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Internal State V value: W,Z - DRBG Key: W,Z
Configure OSPF Service	Configure OSPF Service	Global approved mode indicator and OSPF service configuration status log	Commands used to configure OSPF service	OSPF configuration status	OSPFv2 Authentication	Security Admin (SA) - OSPFv2 Authentication Key : W,Z Network Admin (NA) - OSPFv2 Authentication Key : W,Z
Configure LUKS Database Protection Service	Configure LUKS Database protection service	Global approved mode indicator and LUKS Database service configuration status	Commands to configure LUKS database service	Status of completion of LUKS database service configuration	LUKS Database Protection	Security Admin (SA) - LUKS DB Password: G,W,Z
Run SSHv2 service	Run SSHv2 service	Global approved mode indicator and SSHv2 service running status	Initiate SSHv2 service establishment request	SSHv2 service running status	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-ECC (SSHv2) KAS-FFC (SSHv2) ECDSA KeyGen (SSH, TLS and Control Plane	Security Admin (SA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - SSH DH Private Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					IKEv2) ECDSA SigGen (SSH, TLS and Control Plane IKEv2) ECDSA SigVer (SSH, TLS and Control Plane IKEv2) RSA KeyGen (SSH, TLS and Control Plane IKEv2) RSA SigGen (SSH, TLS and Control Plane IKEv2) RSA SigVer (SSH, TLS and Control Plane IKEv2) Block Ciphers (SSHv2) SSH KTS (AES and HMAC) SSH KTS (GCM) DRBG Function	- SSH DH Public Key: G,W,E,Z - SSH Peer DH Public Key: G,W,E,Z - SSH DH Shared Secret: G,W,E,Z - SSH ECDH Private Key: G,W,E,Z - SSH ECDH Public Key: G,W,E,Z - SSH Peer ECDH Public Key: G,W,E,Z - SSH ECDH Shared Secret: G,W,E,Z - SSH ECDSA Private Key: G,W,E,Z - SSH ECDSA Public Key: G,W,E,Z - SSH RSA Private Key: G,W,E,Z - SSH RSA Public Key: G,W,E,Z - SSH Encryption Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH Integrity Key: G,W,E,Z Network Admin (NA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - SSH DH Private Key: G,W,E,Z - SSH DH Public Key: G,W,E,Z - SSH Peer DH Public Key: G,W,E,Z - SSH DH Shared Secret: G,W,E,Z - SSH ECDH Private Key: G,W,E,Z - SSH ECDH Public Key: G,W,E,Z - SSH Peer ECDH Public Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH ECDH Shared Secret: G,W,E,Z - SSH ECDSA Private Key: G,W,E,Z - SSH ECDSA Public Key: G,W,E,Z - SSH RSA Private Key: G,W,E,Z - SSH RSA Public Key: G,W,E,Z - SSH Encryption Key: G,W,E,Z - SSH Integrity Key: G,W,E,Z Encryption Admin (EA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - SSH DH Private Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,W,E,Z - SSH DH Public Key: G,W,E,Z - SSH Peer DH Public Key: G,W,E,Z - SSH DH Shared Secret: G,W,E,Z - SSH ECDH Private Key: G,W,E,Z - SSH ECDH Public Key: G,W,E,Z - SSH Peer ECDH Public Key: G,W,E,Z - SSH ECDH Shared Secret: G,W,E,Z - SSH ECDSA Private Key: G,W,E,Z - SSH ECDSA Public Key: G,W,E,Z - SSH RSA Private Key: G,W,E,Z - SSH RSA Public Key: G,W,E,Z - SSH Encryption Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,W,E,Z - SSH Integrity Key: G,W,E,Z Network Engineer (NE) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - SSH DH Private Key: G,W,E,Z - SSH DH Public Key: G,W,E,Z - SSH Peer DH Public Key: G,W,E,Z - SSH DH Shared Secret: G,W,E,Z - SSH ECDH Private Key: G,W,E,Z - SSH ECDH Public Key: G,W,E,Z - SSH Peer ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: G,W,E,Z - SSH ECDH Shared Secret: G,W,E,Z - SSH ECDSA Private Key: G,W,E,Z - SSH ECDSA Public Key: G,W,E,Z - SSH RSA Private Key: G,W,E,Z - SSH RSA Public Key: G,W,E,Z - SSH Encryption Key: G,W,E,Z - SSH Integrity Key: G,W,E,Z Monitoring Access (MA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH DH Private Key: G,W,E,Z - SSH DH Public Key: G,W,E,Z - SSH Peer DH Public Key: G,W,E,Z - SSH DH Shared Secret: G,W,E,Z - SSH ECDH Private Key: G,W,E,Z - SSH ECDH Public Key: G,W,E,Z - SSH Peer ECDH Public Key: G,W,E,Z - SSH ECDH Shared Secret: G,W,E,Z - SSH ECDSA Private Key: G,W,E,Z - SSH ECDSA Public Key: G,W,E,Z - SSH RSA Private Key: G,W,E,Z - SSH RSA Public Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH Encryption Key: G,W,E,Z - SSH Integrity Key: G,W,E,Z Provisioning (PR) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - SSH DH Private Key: G,W,E,Z - SSH DH Public Key: G,W,E,Z - SSH Peer DH Public Key: G,W,E,Z - SSH DH Shared Secret: G,W,E,Z - SSH ECDH Private Key: G,W,E,Z - SSH ECDH Public Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH Peer ECDH Public Key: G,W,E,Z - SSH ECDH Shared Secret: G,W,E,Z - SSH ECDSA Private Key: G,W,E,Z - SSH ECDSA Public Key: G,W,E,Z - SSH RSA Private Key: G,W,E,Z - SSH RSA Public Key: G,W,E,Z - SSH Encryption Key: G,W,E,Z - SSH Integrity Key: G,W,E,Z Turn-up and Test (TT) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,W,E,Z - SSH DH Private Key: G,W,E,Z - SSH DH Public Key: G,W,E,Z - SSH Peer DH Public Key: G,W,E,Z - SSH DH Shared Secret: G,W,E,Z - SSH ECDH Private Key: G,W,E,Z - SSH ECDH Public Key: G,W,E,Z - SSH Peer ECDH Public Key: G,W,E,Z - SSH ECDH Shared Secret: G,W,E,Z - SSH ECDSA Private Key: G,W,E,Z - SSH ECDSA Public Key: G,W,E,Z - SSH RSA Private Key: G,W,E,Z - SSH RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: G,W,E,Z - SSH Encryption Key: G,W,E,Z - SSH Integrity Key: G,W,E,Z
Run TLS (v1.2/v1.3) Service	Run TLS (v1.2/v1.3) Service	Global approved mode indicator and TLS (v1.2/v1.3) service running status	Initiate TLS (v1.2/v1.3) service establishment request	TLS (v1.2/v1.3) service running status	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-ECC (TLSv1.2/v1.3) KAS-FFC (TLSv1.2/v1.3) ECDSA KeyGen (SSH, TLS and Control Plane IKEv2) ECDSA SigGen (SSH, TLS and Control Plane IKEv2) ECDSA SigVer (SSH, TLS and Control Plane IKEv2) RSA KeyGen (SSH, TLS	Security Admin (SA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - TLS DH Private Key: G,W,E,Z - TLS DH Public Key: G,W,E,Z - TLS Peer DH Public Key: G,W,E,Z - TLS DH Shared Secret: G,W,E,Z - TLS ECDH Private Key: G,W,E,Z - TLS ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					and Control Plane IKEv2) RSA SigGen (SSH, TLS and Control Plane IKEv2) RSA SigVer (SSH, TLS and Control Plane IKEv2) Block Ciphers (TLSv1.2/v 1.3) TLS KTS (AES and HMAC) TLS KTS (GCM) DRBG Function TLS Keying Materials Development	Public Key: G,W,E,Z - TLS Peer ECDH Public Key: G,W,E,Z - TLS ECDH Shared Secret: G,W,E,Z - TLS ECDSA Private Key: G,W,E,Z - TLS ECDSA Public Key: G,W,E,Z - TLS RSA Private Key: G,W,E,Z - TLS RSA Public Key: G,W,E,Z - TLS Master Secret: G,W,E,Z - TLS Encryption Key: G,W,E,Z - TLS Integrity Key: G,W,E,Z Network Admin (NA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - TLS DH Private Key: G,W,E,Z - TLS DH Public Key: G,W,E,Z - TLS Peer DH Public Key: G,W,E,Z - TLS DH Shared Secret: G,W,E,Z - TLS ECDH Private Key: G,W,E,Z - TLS ECDH Public Key: G,W,E,Z - TLS Peer ECDH Public Key: G,W,E,Z - TLS ECDH Shared Secret: G,W,E,Z - TLS ECDSA Private Key: G,W,E,Z - TLS ECDSA Public Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS RSA Private Key: G,W,E,Z - TLS RSA Public Key: G,W,E,Z - TLS Master Secret: G,W,E,Z - TLS Encryption Key: G,W,E,Z - TLS Integrity Key: G,W,E,Z Encryption Admin (EA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - TLS DH Private Key: G,W,E,Z - TLS DH Public Key: G,W,E,Z - TLS Peer DH Public Key: G,W,E,Z - TLS DH Shared

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: G,W,E,Z - TLS ECDH Private Key: G,W,E,Z - TLS ECDH Public Key: G,W,E,Z - TLS Peer ECDH Public Key: G,W,E,Z - TLS ECDH Shared Secret: G,W,E,Z - TLS ECDSA Private Key: G,W,E,Z - TLS ECDSA Public Key: G,W,E,Z - TLS RSA Private Key: G,W,E,Z - TLS RSA Public Key: G,W,E,Z - TLS Master Secret: G,W,E,Z - TLS Encryption Key: G,W,E,Z - TLS Integrity Key: G,W,E,Z Network

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Engineer (NE) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - TLS DH Private Key: G,W,E,Z - TLS DH Public Key: G,W,E,Z - TLS Peer DH Public Key: G,W,E,Z - TLS DH Shared Secret: G,W,E,Z - TLS ECDH Private Key: G,W,E,Z - TLS ECDH Public Key: G,W,E,Z - TLS Peer ECDH Public Key: G,W,E,Z - TLS ECDH Shared Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,W,E,Z - TLS ECDSA Private Key: G,W,E,Z - TLS ECDSA Public Key: G,W,E,Z - TLS RSA Private Key: G,W,E,Z - TLS RSA Public Key: G,W,E,Z - TLS Master Secret: G,W,E,Z - TLS Encryption Key: G,W,E,Z - TLS Integrity Key: G,W,E,Z Monitoring Access (MA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - TLS DH Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,W,E,Z - TLS DH Public Key: G,W,E,Z - TLS Peer DH Public Key: G,W,E,Z - TLS DH Shared Secret: G,W,E,Z - TLS ECDH Private Key: G,W,E,Z - TLS ECDH Public Key: G,W,E,Z - TLS Peer ECDH Public Key: G,W,E,Z - TLS ECDH Shared Secret: G,W,E,Z - TLS ECDSA Private Key: G,W,E,Z - TLS ECDSA Public Key: G,W,E,Z - TLS RSA Private Key: G,W,E,Z - TLS RSA Public Key: G,W,E,Z - TLS Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: G,W,E,Z - TLS Encryption Key: G,W,E,Z - TLS Integrity Key: G,W,E,Z Provisioning (PR) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - TLS DH Private Key: G,W,E,Z - TLS DH Public Key: G,W,E,Z - TLS Peer DH Public Key: G,W,E,Z - TLS DH Shared Secret: G,W,E,Z - TLS ECDH Private Key: G,W,E,Z - TLS ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: G,W,E,Z - TLS Peer ECDH Public Key: G,W,E,Z - TLS ECDH Shared Secret: G,W,E,Z - TLS ECDSA Private Key: G,W,E,Z - TLS ECDSA Public Key: G,W,E,Z - TLS RSA Private Key: G,W,E,Z - TLS RSA Public Key: G,W,E,Z - TLS Master Secret: G,W,E,Z - TLS Encryption Key: G,W,E,Z - TLS Integrity Key: G,W,E,Z Turn-up and Test (TT) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - TLS DH Private Key: G,W,E,Z - TLS DH Public Key: G,W,E,Z - TLS Peer DH Public Key: G,W,E,Z - TLS DH Shared Secret: G,W,E,Z - TLS ECDH Private Key: G,W,E,Z - TLS ECDH Public Key: G,W,E,Z - TLS Peer ECDH Public Key: G,W,E,Z - TLS ECDH Shared Secret: G,W,E,Z - TLS ECDSA Private Key: G,W,E,Z - TLS ECDSA Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,W,E,Z - TLS RSA Private Key: G,W,E,Z - TLS RSA Public Key: G,W,E,Z - TLS Master Secret: G,W,E,Z - TLS Encryption Key: G,W,E,Z - TLS Integrity Key: G,W,E,Z
Run Control Plane IPsec/IKEv2 Service	Run Control Plane IPsec/IKEv2 Service	Global approved mode indicator and Run IPsec/IKEv2 service completion status log	Command to run Run Control Plane IPsec/IKEv2 service	Control Plane IPsec/IKEv2 service running status	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2) KAS-ECC (Control Plane IKEv2) KAS-FFC (Control Plane IKEv2) ECDSA KeyGen (SSH, TLS and Control Plane IKEv2) ECDSA SigGen (SSH, TLS	Security Admin (SA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - IPSec/IKE DH Private Key: G,W,E,Z - IPSec/IKE DH Public Key: G,W,E,Z - IPSec/IKE Peer DH Public Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					and Control Plane IKEv2) ECDSA SigVer (SSH, TLS and Control Plane IKEv2) RSA KeyGen (SSH, TLS and Control Plane IKEv2) RSA SigGen (SSH, TLS and Control Plane IKEv2) RSA SigVer (SSH, TLS and Control Plane IKEv2) Block Ciphers (Control Plane IKEv2) DRBG Function IPsec/IKEv2 Keying Materials Development	- IPSec/IKE DH Shared Secret: G,W,E,Z - IPSec/IKE ECDH Private Key: G,W,E,Z - IPSec/IKE ECDH Public Key: G,W,E,Z - IPSec/IKE Peer ECDH Public Key: G,W,E,Z - IPSec/IKE ECDH Shared Secret: G,W,E,Z - IPSec/IKE ECDSA Private Key: G,W,E,Z - IPSec/IKE ECDSA Public Key: G,W,E,Z - IPSec/IKE RSA Private Key: G,W,E,Z - IPSec/IKE RSA Public Key: G,W,E,Z - IPSec/IKE Pre-shared Secret: G,W,E,Z - IPSec/IKE SKEYSEED: G,W,E,Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key: G,W,E,Z - IPSec/IKE Integrity Key: G,W,E,Z Network Admin (NA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - IPSec/IKE DH Private Key: G,W,E,Z - IPSec/IKE DH Public Key: G,W,E,Z - IPSec/IKE Peer DH Public Key: G,W,E,Z - IPSec/IKE DH Shared Secret: G,W,E,Z - IPSec/IKE ECDH Private Key: G,W,E,Z - IPSec/IKE ECDH Public Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- IPSec/IKE Peer ECDH Public Key: G,W,E,Z - IPSec/IKE ECDH Shared Secret: G,W,E,Z - IPSec/IKE ECDSA Private Key: G,W,E,Z - IPSec/IKE ECDSA Public Key: G,W,E,Z - IPSec/IKE RSA Private Key: G,W,E,Z - IPSec/IKE RSA Public Key: G,W,E,Z - IPSec/IKE Pre-shared Secret: G,W,E,Z - IPSec/IKE SKEYSEED: G,W,E,Z - IPSec/IKE Encryption Key: G,W,E,Z - IPSec/IKE Integrity Key: G,W,E,Z Encryption Admin (EA) - DRBG Entropy Input: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - IPSec/IKE DH Private Key: G,W,E,Z - IPSec/IKE DH Public Key: G,W,E,Z - IPSec/IKE Peer DH Public Key: G,W,E,Z - IPSec/IKE DH Shared Secret: G,W,E,Z - IPSec/IKE ECDH Private Key: G,W,E,Z - IPSec/IKE ECDH Public Key: G,W,E,Z - IPSec/IKE Peer ECDH Public Key: G,W,E,Z - IPSec/IKE ECDH Shared Secret: G,W,E,Z - IPSec/IKE ECDSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,W,E,Z - IPSec/IKE ECDSA Public Key: G,W,E,Z - IPSec/IKE RSA Private Key: G,W,E,Z - IPSec/IKE RSA Public Key: G,W,E,Z - IPSec/IKE Pre-shared Secret: G,W,E,Z - IPSec/IKE SKEYSEED: G,W,E,Z - IPSec/IKE Encryption Key: G,W,E,Z - IPSec/IKE Integrity Key: G,W,E,Z Network Engineer (NE) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DH Private Key: G,W,E,Z - IPSec/IKE DH Public Key: G,W,E,Z - IPSec/IKE Peer DH Public Key: G,W,E,Z - IPSec/IKE DH Shared Secret: G,W,E,Z - IPSec/IKE ECDH Private Key: G,W,E,Z - IPSec/IKE ECDH Public Key: G,W,E,Z - IPSec/IKE Peer ECDH Public Key: G,W,E,Z - IPSec/IKE ECDH Shared Secret: G,W,E,Z - IPSec/IKE ECDSA Private Key: G,W,E,Z - IPSec/IKE ECDSA Public Key: G,W,E,Z - IPSec/IKE RSA Private Key: G,W,E,Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						RSA Public Key: G,W,E,Z - IPSec/IKE Pre-shared Secret: G,W,E,Z - IPSec/IKE SKEYSEED: G,W,E,Z - IPSec/IKE Encryption Key: G,W,E,Z - IPSec/IKE Integrity Key: G,W,E,Z Provisioning (PR) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - IPSec/IKE DH Private Key: G,W,E,Z - IPSec/IKE DH Public Key: G,W,E,Z - IPSec/IKE Peer DH Public Key: G,W,E,Z - IPSec/IKE DH Shared

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: G,W,E,Z - IPSec/IKE ECDH Private Key: G,W,E,Z - IPSec/IKE ECDH Public Key: G,W,E,Z - IPSec/IKE Peer ECDH Public Key: G,W,E,Z - IPSec/IKE ECDH Shared Secret: G,W,E,Z - IPSec/IKE ECDSA Private Key: G,W,E,Z - IPSec/IKE ECDSA Public Key: G,W,E,Z - IPSec/IKE RSA Private Key: G,W,E,Z - IPSec/IKE RSA Public Key: G,W,E,Z - IPSec/IKE Pre-shared Secret: G,W,E,Z - IPSec/IKE SKEYSEED: G,W,E,Z - IPSec/IKE Encryption Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,W,E,Z - IPSec/IKE Integrity Key: G,W,E,Z Turn-up and Test (TT) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - IPSec/IKE DH Private Key: G,W,E,Z - IPSec/IKE DH Public Key: G,W,E,Z - IPSec/IKE Peer DH Public Key: G,W,E,Z - IPSec/IKE DH Shared Secret: G,W,E,Z - IPSec/IKE ECDH Private Key: G,W,E,Z - IPSec/IKE ECDH Public Key: G,W,E,Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Peer ECDH Public Key: G,W,E,Z - IPSec/IKE ECDH Shared Secret: G,W,E,Z - IPSec/IKE ECDSA Private Key: G,W,E,Z - IPSec/IKE ECDSA Public Key: G,W,E,Z - IPSec/IKE RSA Private Key: G,W,E,Z - IPSec/IKE RSA Public Key: G,W,E,Z - IPSec/IKE Pre-shared Secret: G,W,E,Z - IPSec/IKE SKEYSEED: G,W,E,Z - IPSec/IKE Encryption Key: G,W,E,Z - IPSec/IKE Integrity Key: G,W,E,Z Monitoring Access (MA) - DRBG Entropy Input: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - IPSec/IKE DH Private Key: G,W,E,Z - IPSec/IKE DH Public Key: G,W,E,Z - IPSec/IKE Peer DH Public Key: G,W,E,Z - IPSec/IKE DH Shared Secret: G,W,E,Z - IPSec/IKE ECDH Private Key: G,W,E,Z - IPSec/IKE ECDH Public Key: G,W,E,Z - IPSec/IKE Peer ECDH Public Key: G,W,E,Z - IPSec/IKE ECDH Shared Secret: G,W,E,Z - IPSec/IKE ECDSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,W,E,Z - IPSec/IKE ECDSA Public Key: G,W,E,Z - IPSec/IKE RSA Private Key: G,W,E,Z - IPSec/IKE RSA Public Key: G,W,E,Z - IPSec/IKE Pre-shared Secret: G,W,E,Z - IPSec/IKE SKEYSEED: G,W,E,Z - IPSec/IKE Encryption Key: G,W,E,Z - IPSec/IKE Integrity Key: G,W,E,Z
Run SNMP Service	Run SNMP Service	Global approved mode indicator and SNMP service running status	Initiate SNMP service establishment request	SNMP service running status	Block Ciphers (SNMPv3) SNMPv3 Keying Materials Development	Security Admin (SA) - SNMPv3 Authentication Secret: G,W,E,Z - SNMPv3 Encryption Key: G,W,E,Z - SNMPv3 Integrity Key: G,W,E,Z Network Admin (NA) - SNMPv3 Authentication Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,W,E,Z - SNMPv3 Encryption Key: G,W,E,Z - SNMPv3 Integrity Key: G,W,E,Z Encryption Admin (EA) - SNMPv3 Authentication Secret: G,W,E,Z - SNMPv3 Encryption Key: G,W,E,Z - SNMPv3 Integrity Key: G,W,E,Z Network Engineer (NE) - SNMPv3 Authentication Secret: G,W,E,Z - SNMPv3 Encryption Key: G,W,E,Z - SNMPv3 Integrity Key: G,W,E,Z Monitoring Access (MA) - SNMPv3 Authentication Secret: G,W,E,Z - SNMPv3 Encryption Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SNMPv3 Integrity Key: G,W,E,Z Provisioning (PR) - SNMPv3 Authentication Secret: G,W,E,Z - SNMPv3 Encryption Key: G,W,E,Z - SNMPv3 Integrity Key: G,W,E,Z Turn-up and Test (TT) - SNMPv3 Authentication Secret: G,W,E,Z - SNMPv3 Encryption Key: G,W,E,Z - SNMPv3 Integrity Key: G,W,E,Z
Run Data Plane Encrypiton Service	Run Data Plane Encrypiton Service	Global approved mode indicator and Data Plane Encryption service completion status log	Command to run OSPF service	Data Plane Encryption service running status	KAS-ECC-KeyGen (Data Plane IKEv2) KAS-ECC (Data Plane IKEv2) ECDSA KeyGen (Data Plane IKEv2) ECDSA SigGen (Data Plane IKEv2) ECDSA	Security Admin (SA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SigVer (Data Plane IKEv2) RSA KeyGen (Data Plane IKEv2) RSA SigGen (Data Plane IKEv2) RSA SigVer (Data Plane IKEv2) Block Cipher (Data Plane IKEv2) DRBG Function	G,W,E,Z - Data Plane Encryption ECDH Private Key: G,W,E,Z - Data Plane Encryption ECDH Public Key: G,W,E,Z - Data Plane Encryption Peer ECDH Public Key: G,W,E,Z - Data Plane Encryption ECDH Shared Secret: G,W,E,Z - Data Plane Encryption ECDSA Private Key: G,W,E,Z - Data Plane Encryption ECDSA Public Key: G,W,E,Z - Data Plane Encryption RSA Private Key: G,W,E,Z - Data

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Plane Encryption RSA Public Key: G,W,E,Z - Data Plane Encryption Pre-shared Secret: G,W,E,Z - Data Plane Encryption IKE-SA Session Key: G,W,E,Z - Data Plane Encryption Child-SA Session Key: G,W,E,Z Network Admin (NA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - Data Plane Encryption ECDH Private Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Data Plane Encryption ECDH Public Key: G,W,E,Z - Data Plane Encryption Peer ECDH Public Key: G,W,E,Z - Data Plane Encryption ECDH Shared Secret: G,W,E,Z - Data Plane Encryption ECDSA Private Key: G,W,E,Z - Data Plane Encryption ECDSA Public Key: G,W,E,Z - Data Plane Encryption RSA Private Key: G,W,E,Z - Data Plane Encryption RSA Public Key: G,W,E,Z - Data Plane Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Pre-shared Secret: G,W,E,Z - Data Plane Encryption IKE-SA Session Key: G,W,E,Z - Data Plane Encryption Child-SA Session Key: G,W,E,Z Encryption Admin (EA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - Data Plane Encryption ECDH Private Key: G,W,E,Z - Data Plane Encryption ECDH Public Key: G,W,E,Z - Data Plane

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Peer ECDH Public Key: G,W,E,Z - Data Plane Encryption ECDH Shared Secret: G,W,E,Z - Data Plane Encryption ECDSA Private Key: G,W,E,Z - Data Plane Encryption ECDSA Public Key: G,W,E,Z - Data Plane Encryption RSA Private Key: G,W,E,Z - Data Plane Encryption RSA Public Key: G,W,E,Z - Data Plane Encryption Pre-shared Secret: G,W,E,Z - Data Plane Encryption IKE-SA Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,W,E,Z - Data Plane Encryption Child-SA Session Key: G,W,E,Z Network Engineer (NE) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - Data Plane Encryption ECDH Private Key: G,W,E,Z - Data Plane Encryption ECDH Public Key: G,W,E,Z - Data Plane Encryption Peer ECDH Public Key: G,W,E,Z - Data Plane

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption ECDH Shared Secret: G,W,E,Z - Data Plane Encryption ECDSA Private Key: G,W,E,Z - Data Plane Encryption ECDSA Public Key: G,W,E,Z - Data Plane Encryption RSA Private Key: G,W,E,Z - Data Plane Encryption RSA Public Key: G,W,E,Z - Data Plane Encryption Pre-shared Secret: G,W,E,Z - Data Plane Encryption IKE-SA Session Key: G,W,E,Z - Data Plane Encryption Child-SA Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,W,E,Z Monitoring Access (MA) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - Data Plane Encryption ECDH Private Key: G,W,E,Z - Data Plane Encryption ECDH Public Key: G,W,E,Z - Data Plane Encryption Peer ECDH Public Key: G,W,E,Z - Data Plane Encryption ECDH Shared Secret: G,W,E,Z - Data Plane

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption ECDSA Private Key: G,W,E,Z - Data Plane Encryption ECDSA Public Key: G,W,E,Z - Data Plane Encryption RSA Private Key: G,W,E,Z - Data Plane Encryption RSA Public Key: G,W,E,Z - Data Plane Encryption Pre-shared Secret: G,W,E,Z - Data Plane Encryption IKE-SA Session Key: G,W,E,Z - Data Plane Encryption Child-SA Session Key: G,W,E,Z Provisioning (PR) - DRBG Entropy Input:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V value: G,W,E,Z - DRBG Key: G,W,E,Z - Data Plane Encryption ECDH Private Key: G,W,E,Z - Data Plane Encryption ECDH Public Key: G,W,E,Z - Data Plane Encryption Peer ECDH Public Key: G,W,E,Z - Data Plane Encryption ECDH Shared Secret: G,W,E,Z - Data Plane Encryption ECDSA Private Key: G,W,E,Z - Data Plane Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDSA Public Key: G,W,E,Z - Data Plane Encryption RSA Private Key: G,W,E,Z - Data Plane Encryption RSA Public Key: G,W,E,Z - Data Plane Encryption Pre-shared Secret: G,W,E,Z - Data Plane Encryption IKE-SA Session Key: G,W,E,Z - Data Plane Encryption Child-SA Session Key: G,W,E,Z Turn-up and Test (TT) - DRBG Entropy Input: G,W,E,Z - DRBG Seed: G,W,E,Z - DRBG Internal State V

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						value: G,W,E,Z - DRBG Key: G,W,E,Z - Data Plane Encryption ECDH Private Key: G,W,E,Z - Data Plane Encryption ECDH Public Key: G,W,E,Z - Data Plane Encryption Peer ECDH Public Key: G,W,E,Z - Data Plane Encryption ECDH Shared Secret: G,W,E,Z - Data Plane Encryption ECDSA Private Key: G,W,E,Z - Data Plane Encryption ECDSA Public Key: G,W,E,Z - Data Plane Encryption RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: G,W,E,Z - Data Plane Encryption RSA Public Key: G,W,E,Z - Data Plane Encryption Pre-shared Secret: G,W,E,Z - Data Plane Encryption IKE-SA Session Key: G,W,E,Z - Data Plane Encryption Child-SA Session Key: G,W,E,Z
Run OSPF Service	Run OSPF Service	Global approved mode indicator and OSPF service completion status log	Command to run OSPF Function	OSPF running status	OSPFv2 Authentication	Security Admin (SA) - OSPFv2 Authentication Key : W,E Network Admin (NA) - OSPFv2 Authentication Key : W,E Encryption Admin (EA) - OSPFv2 Authentication Key : W,E Network Engineer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(NE) - OSPFv2 Authentication Key : W,E Monitoring Access (MA) - OSPFv2 Authentication Key : W,E Provisioning (PR) - OSPFv2 Authentication Key : W,E Turn-up and Test (TT) - OSPFv2 Authentication Key : W,E
Configure NTP Authentication	Configure NTP Authentication Scheme and Key	Global approved mode indicator and NTP service configuration status	Commands to configure NTP service	Status of the completion of NTP configuration	NTP Authentication	Security Admin (SA) - NTP Authentication Key : G,W,Z
Run LUKS Database Protection Service	Run LUKS database protection service	Global approved mode indicator and LUKS service completion status log	Command to run LUKS protection service	LUKS running status	LUKS Database Protection	Security Admin (SA) - LUKS DB Password: W,E,Z - LUKS DB Salt : W,E,Z

Table 12: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using ECDSA with Curve P-521 and SHA2-512 (ECDSA Cert. #A4956) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails. 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.

4.6 Bypass Actions and Status

N/A for this module.

4.7 Cryptographic Output Actions and Status

The module implements Self-initiated cryptographic output capability without external operator request. The Crypto Officer shall configure self-initiated cryptographic output capability. Prior to executing the self-initiated cryptographic output capability, the module conducts two independent internal actions to activate the capability to prevent the inadvertent output due to a single error.

4.8 Additional Information

The module supports unauthenticated service. The unauthenticated User/Operators can trigger the self-test service by power-cycling the module, and is able to observe the module's LEDs status.

5 Software/Firmware Security

5.1 Integrity Techniques

The module is provided in the form of binary executable code. To ensure firmware security, the module is protected by conducting multiple layers firmware integrity tests. Please refer to section 10.1 Pre-Operational Self-Tests of this Security Policy document for more details. If the firmware integrity test fails, the module would enter to an Error state with all crypto functionality inhibited.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can power-cycle or reboot the module to initiate the firmware integrity test on-demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

Module is operated in a limited operational environment. New firmware versions within the scope of this validation must be validated through the FIPS 140-3 CMVP. Any firmware loaded into the module that is not shown on the module certificate, is out of scope of this validation and requires a separate FIPS 140-3 validation.

7 Physical Security

The module meets the FIPS 140-3 Level 1 security requirements as production grade equipment.

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Production grade components	N/A	N/A

Table 13: Mechanisms and Actions Required

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM	Volatile memory	Dynamic
Flash	Non-Volatile memory	Static

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Module Public Key Output	Module	External (Outside the Module's Boundary)	Plaintext	Automated	Electronic	
Peer Public Key Input	External (Outside the Module's Boundary)	Module	Plaintext	Automated	Electronic	
SSPs Input/Output protected by TLS KTS (GCM)	External (Outside the Module's Boundary)	Module	Encrypted	Automated	Electronic	TLS KTS (GCM)
SSPs Input/Output protected by TLS KTS (AES and HMAC)	External (Outside the Module's Boundary)	Module	Encrypted	Automated	Electronic	TLS KTS (AES and HMAC)
SSPs Input/Output protected by SSH KTS (GCM)	External (Outside the Module's Boundary)	Module	Encrypted	Automated	Electronic	SSH KTS (GCM)
SSPs Input/Output protected by SSH KTS (AES and HMAC)	External (Outside the Module's Boundary)	Module	Encrypted	Automated	Electronic	SSH KTS (AES and HMAC)

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization command	CO issues zeroization service: "fips zeroize" to zeroize all SSPs	The zeroization command will erase all SSPs stored in the RAM and in the Flash of the module.	Module Reboot
Session termination	Zeroization upon session termination	Session termination will automatically zeroize all session based temporary SSPs	Terminate session

Zeroization Method	Description	Rationale	Operator Initiation
Reboot	Zeroization upon rebooting the module	Reboot to zeroize all temporary SSPs stored in Module's DRAM	Reboot

Table 16: SSP Zeroization Methods

Please note that the Firmware Load Test Key is only used for Firmware Load Test Authentication and not subject to the zeroization requirement.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input	Used to seed the DRBG	384 bits - At least 256 bits	Entropy Inputs - CSP			DRBG Function
DRBG Seed	Used for DRBG generation	256 bits - 256 bits	DRBG Seed - CSP			DRBG Function
DRBG Internal State V value	Used for DRBG generation	256 bits - 256 bits	DRBG Internal State V value - CSP			DRBG Function
DRBG Key	Used for DRBG generation	256 bits - 256 bits	DRBG Key - CSP			DRBG Function
Operator Password	Used for operator authentication	8-30 characters - N/A	Authentication Data - CSP			
LUKS DB Password	Used for LUKS DB Integrity Key derivation	512 bits - 512 bits	HMAC key - CSP	DRBG Function		LUKS Database Protection
LUKS DB Salt	Used for LUKS DB Integrity Key derivation	256 bits - 256 bits	Salt - CSP	DRBG Function		LUKS Database Protection
LUKS DB Integrity Key	Used for LUKS Database integrity protection	512 bits - 512 bits	Authentication - CSP		PBKDF (A4958)	LUKS Database Protection
Firmware Load Test Key	Used for firmware load test	P-521 - 256 bits	Public Key - PSP			Firmware Load Test

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH DH Private Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-4096, and MODP-8192 - 112-200 bits	Private Key - CSP	KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)		KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)
SSH DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-4096, and MODP-8192 - 112-200 bits	Public Key - PSP		KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)	
SSH Peer DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-4096, and MODP-8192 - N/A	Public Key - PSP			KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)
SSH DH Shared Secret	Used to derive SSH Encryption Key and SSH Integrity Key	MODP-2048, MODP-4096, and MODP-8192 - 112-200 bits	Shared Secret - CSP		KAS-FFC (SSHv2)	KAS-FFC (SSHv2)
SSH ECDH Private Key	Used to derive SSH ECDH Shared Secret	P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)		KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)
SSH ECDH Public Key	Used to derive SSH ECDH	P-256, P-384, P-521 -	Public Key - PSP		KAS-ECC-KeyGen (SSH, TLS and Control	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Shared Secret	128-256 bits			Plane IKEv2)	
SSH Peer ECDH Public Key	Used to derive SSH ECDH Shared Secret	P-256, P-384, P-521 - N/A	Public Key - PSP			KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)
SSH ECDH Shared Secret	Used to derive SSH Encryption Key and SSH Integrity Key	P-256, P-384, P-521 - 128-256 bits	Shared Secret - CSP		KAS-ECC (SSHv2)	KAS-ECC (SSHv2)
SSH ECDSA Private Key	Used for SSH authenticati on	P-256, P-384 and P-521 - 128-256 bits	Private Key - CSP	ECDSA KeyGen (SSH, TLS and Control Plane IKEv2)		ECDSA SigGen (SSH, TLS and Control Plane IKEv2)
SSH ECDSA Public Key	Used for SSH authetnicati on	P-256, P-384 and P-521 - 128-256 bits	Public Key - PSP		ECDSA KeyGen (SSH, TLS and Control Plane IKEv2)	ECDSA SigVer (SSH, TLS and Control Plane IKEv2)
SSH RSA Private Key	Used for SSH authetnicati on	2048, 3072 and 4096 bits - 112 -152 bits	Private Key - CSP	RSA KeyGen (SSH, TLS and Control Plane IKEv2)		RSA SigGen (SSH, TLS and Control Plane IKEv2)
SSH RSA Public Key	Used for SSH authetnicati on	2048, 3072 and 4096 bits - 112 -152 bits	Public Key - PSP		RSA KeyGen (SSH, TLS and Control Plane IKEv2)	RSA SigVer (SSH, TLS and Control Plane IKEv2)
SSH Encryption Key	Used for SSH traffic protection	128-256 bits - 128-256 bits	Symmetric Key - CSP		KAS-ECC (SSHv2) KAS-FFC (SSHv2)	Block Ciphers (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH Integrity Key	Used for SSH traffic integrity protection	at least 112 bits - at least 112 bits	Authentication Key - CSP		KAS-ECC (SSHv2) KAS-FFC (SSHv2)	Block Ciphers (SSHv2)
TLS DH Private Key	Used to drive TLS DH Shared Secret	ffdhe2048 - 112 bits	Private Key - CSP	KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)		KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)
TLS DH Public Key	Used to drive TLS DH Shared Secret	ffdhe2048 - 112 bits	Public Key - PSP		KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)	
TLS Peer DH Public Key	Used to derive TLS DH Shared Secret	ffdhe2048 - 112 bits	Public Key - PSP			KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)
TLS DH Shared Secret	Used to derive TLS encryption Key and TLS Integrity Key	ffdhe2048 - 112 bits	Shared Secret - CSP		KAS-FFC (TLSv1.2/v1.3)	KAS-FFC (TLSv1.2/v1.3)
TLS ECDH Private Key	Used to drive TLS ECDH Shared Secret	P-256, P-384 and P-521 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)		KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)
TLS ECDH Public Key	Used to drive TLS ECDH Shared Secret	P-256, P-384 and P-521 - 128-256 bits	Public Key - PSP		KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS Peer ECDH Public Key	Used to derive TLS ECDH Shared Secret	P-256, P-384 and P-521 - N/A	Public Key - PSP			KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)
TLS ECDH Shared Secret	Used to derive TLS Encryption Key and TLS Integrity Key	P-256, P-384 and P-521 - 128-256 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2/v1.3)	KAS-ECC (TLSv1.2/v1.3)
TLS ECDSA Private Key	Used for TLS authentication	P-256, P-384 and P-521 - 128-256 bits	Private Key - CSP	ECDSA KeyGen (SSH, TLS and Control Plane IKEv2)		ECDSA SigGen (SSH, TLS and Control Plane IKEv2)
TLS ECDSA Public Key	Used for TLS authentication	P-256, P-384 and P-521 - 128-256 bits	Public Key - PSP		ECDSA KeyGen (SSH, TLS and Control Plane IKEv2)	ECDSA SigVer (SSH, TLS and Control Plane IKEv2)
TLS RSA Private Key	Used for TLS authentication	2048 bits - 112 bits	Private Key - CSP	RSA KeyGen (SSH, TLS and Control Plane IKEv2)		RSA SigGen (SSH, TLS and Control Plane IKEv2)
TLS RSA Public Key	Used for TLS peer authentication	2048 bits - 112 bits	Public Key - PSP		RSA KeyGen (SSH, TLS and Control Plane IKEv2)	RSA SigVer (SSH, TLS and Control Plane IKEv2)
TLS Master Secret	Used to derive TLS Encryption Key and TLS Integrity Key	384 bits - 384 bits	TLS Master Secret - CSP		TLS Keying Materials Development	TLS Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS Encryption Key	Used to protect TLS traffic confidentiality.	128-256 bits - 128-256 bits	Encryption Key - CSP		KAS-ECC (TLSv1.2/v1.3) KAS-FFC (TLSv1.2/v1.3)	Block Ciphers (TLSv1.2/v1.3)
TLS Integrity Key	Used to protect traffic confidentiality.	at least 112 bits - at least 112 bits	Authentication Key - CSP		KAS-ECC (TLSv1.2/v1.3) KAS-FFC (TLSv1.2/v1.3)	Block Ciphers (TLSv1.2/v1.3)
IPSec/IKE DH Private Key	Used for IPsec/IKE DH Shared Secret derivation	MODP-2048, MODP-3072, MODP-4096, MODP-6144 and MODP-8192 - 112-200 bits	Private Key - CSP	KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)		KAS-FFC-SSC Sp800-56Ar3 (A4958)
IPSec/IKE DH Public Key	Used for IPsec/IKE DH Shared Secret derivation	MODP-2048, MODP-3072, MODP-4096, MODP-6144 and MODP-8192 - 112-200 bits	Public Key - PSP		KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)	
IPSec/IKE Peer DH Public Key	Used for IPsec/IKE DH Shared Secret derivation	MODP-2048, MODP-3072, MODP-4096, MODP-6144 and	Public Key - PSP			KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		MODP-8192 - N/A				
IPSec/IKE DH Shared Secret	Used for IPSec/IKE Encryption Key and IPSec/IKE Integrity key derivation	MODP-2048, MODP-3072, MODP-4096, MODP-6144 and MODP-8192 - 112-200 bits	Shared Secret - CSP		KAS-FFC-KeyGen (SSH, TLS and Control Plane IKEv2)	KAS-FFC (Control Plane IKEv2)
IPSec/IKE ECDH Private Key	Used for IPSec/IKE ECDH Shared Secret derivation	P-256, P-384 and P-521 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)		KAS-ECC (Control Plane IKEv2)
IPSec/IKE ECDH Public Key	Used for IPSec/IKE ECDH Shared Secret derivation	P-256, P-384 and P-521 - 128-256 bits	Public Key - PSP		KAS-ECC-KeyGen (SSH, TLS and Control Plane IKEv2)	
IPSec/IKE Peer ECDH Public Key	Used for IPSec/IKE ECDH Shared Secret derivation	P-256, P-384 and P-521 - 128-256 bits	Public Key - PSP			KAS-ECC (Control Plane IKEv2)
IPSec/IKE ECDH Shared Secret	Used for IPSec/IKE Encryption Key and IPSec/IKE Integrity Key derivation	P-256, P-384 and P-521 - 128-256 bits	Shared Secret - CSP		KAS-ECC (Control Plane IKEv2)	KAS-ECC (Control Plane IKEv2)
IPSec/IKE ECDSA Private Key	Used for IPSec/IKE peer	P-256, P-384 and P-	Private Key - CSP	ECDSA SigGen (SSH,		ECDSA SigGen (SSH, TLS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	authentication	521 - 128-256 bits		TLS and Control Plane IKEv2)		and Control Plane IKEv2)
IPSec/IKE ECDSA Public Key	Used for IPSec/IKE peer authentication	P-256, P-384 and P-521 - 128-256 bits	Public Key - PSP		ECDSA KeyGen (SSH, TLS and Control Plane IKEv2)	ECDSA SigVer (SSH, TLS and Control Plane IKEv2)
IPSec/IKE RSA Private Key	Used for IPSec/IKE peer authentication	2048, 3072 and 4096 bits - 112-152 bits	Private Key - CSP	RSA KeyGen (SSH, TLS and Control Plane IKEv2)		RSA SigGen (SSH, TLS and Control Plane IKEv2)
IPSec/IKE RSA Public Key	Used for IPSec/IKE peer authentication	2048, 3072 and 4096 bits - 112-152 bits	Public Key - PSP		RSA KeyGen (SSH, TLS and Control Plane IKEv2)	RSA SigVer (SSH, TLS and Control Plane IKEv2)
IPSec/IKE Pre-shared Secret	Used for IPSec/IKE peer authentication	256 bits - N/A	Shared Secret - CSP			IPsec/IKEv2 Keying Materials Development
IPSec/IKE SKEYSEED	Keying material used to derive the IPSec/IKE Encryption Key and IPSec/IKE Integrity Key	160 bits - N/A	Keying Material - CSP			IPsec/IKEv2 Keying Materials Development
IPSec/IKE Encryption Key	Used for IPSec/IKE traffic confidentiality protection	128-256 bits - 128-256 bits	Encryption Key - CSP		IPsec/IKEv2 Keying Materials Development	Block Ciphers (Control Plane IKEv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IPSec/IKE Integrity Key	Used for IPSec/IKE traffic integrity protection	At least 112 bits - At least 112 bits	Authentication Key - CSP		Block Ciphers (Control Plane IKEv2)	Block Ciphers (Control Plane IKEv2)
SNMPv3 Authentication Secret	Used to SNMPv3 authentication	64 characters - N/A	Authentication Secret - CSP			SNMPv3 Keying Materials Development
SNMPv3 Encryption Key	Used to secure SNMPv3 traffic confidentiality	128-256 bits - 128-256 bits	Symmetric Key - CSP		SNMPv3 Keying Materials Development	Block Ciphers (SNMPv3)
SNMPv3 Integrity Key	Used to secure SNMPv3 traffic integrity	At least 112 bits - At least 112 bits	Authentication Key - CSP		SNMPv3 Keying Materials Development	Block Ciphers (SNMPv3)
Data Plane Encryption ECDH Private Key	Used to derive Data Plane Encryption ECDH Shared Secret	P-521 - 256 bits	Private Key - CSP	KAS-ECC-KeyGen (Data Plane IKEv2)		KAS-ECC (Data Plane IKEv2)
Data Plane Encryption ECDH Public Key	Used to derive Data Plane Encryption ECDH Shared Secret	P-521 - 256 bits	Public Key - PSP		KAS-ECC-KeyGen (Data Plane IKEv2)	
Data Plane Encryption ECDH Shared Secret	Used to derive Data Plane Encryption IKE-SA Session Key and Data Plane Encryption Child-SA Session Key	P-521 - 256 bits	Shared Secret - CSP		KAS-ECC (Data Plane IKEv2)	KAS-ECC (Data Plane IKEv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Data Plane Encryption Peer ECDH Public Key	Used to derive Data Plane Encryption ECDH Shared Secret	P-521 - 256 bits	Public Key - PSP			KAS-ECC (Data Plane IKEv2)
Data Plane Encryption ECDSA Private Key	Used for Data Plane Encryption authentication	P-256, P-384 and P-521 - 128-256 bits	Private Key - CSP	ECDSA KeyGen (Data Plane IKEv2)		ECDSA SigGen (Data Plane IKEv2)
Data Plane Encryption ECDSA Public Key	Used for Data Plane Encryption authentication	P-256, P-384 and P-521 - 128-256 bits	Public Key - PSP		ECDSA KeyGen (Data Plane IKEv2)	ECDSA SigVer (Data Plane IKEv2)
Data Plane Encryption RSA Private Key	Used for Data Plane Encryption authentication	2048, 3072 and 4096 bits - 112- 152 bits	Private Key - CSP	RSA KeyGen (Data Plane IKEv2)		RSA SigGen (Data Plane IKEv2)
Data Plane Encryption RSA Public Key	Used for Data Plane Encryption authentication	2048, 3072 and 4096 bits - 112- 152 bits	Public Key - PSP		RSA KeyGen (Data Plane IKEv2)	RSA SigVer (Data Plane IKEv2)
Data Plane Encryption Pre-shared Secret	Used for Data Plane Encryption service authentication	Curves: P-256, P-384, P-521 - 128-256 bits	Shared Secret - CSP			KAS-ECC (Data Plane IKEv2)
Data Plane Encryption IKE-SA Session Key	Used to secure Data Plane Encryption traffic confidentiality	256 bits - 256 bits	Authenticated Symmetric Key - CSP		KAS-ECC (Data Plane IKEv2)	Block Cipher (Data Plane IKEv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Data Plane Encryption Child-SA Session Key	Used to secure Data Plane Encryption Child-SA traffic confidentiality	256 bits - 256 bits	Authenticated Symmetric Key - CSP		KAS-ECC (Data Plane IKEv2)	Block Cipher (Data Plane IKEv2)
NTP Authentication Key	Used for NTP authentication	8-40 characters - N/A	Authentication - CSP			NTP Authentication
OSPFv2 Authentication Key	Used for OSPFv2 authentication	8-25 characters - N/A	Authentication - CSP			OSPFv2 Authentication

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		DRAM:Plaintext	Until Reboot	Zeroization command Session termination Reboot	DRBG Seed:Used With DRBG Internal State V value:Used With DRBG Key:Used With
DRBG Seed		DRAM:Plaintext	Until Reboot	Zeroization command Session termination Reboot	DRBG Entropy Input:Used With DRBG Internal State V value:Used With DRBG Key:Used With
DRBG Internal State V value		DRAM:Plaintext	Until Reboot	Zeroization command Session termination Reboot	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Key:Used With
DRBG Key		DRAM:Plaintext	Until Reboot	Zeroization command Session terminatio	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Internal

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
				n Reboot	State V value:Used With
Operator Password	SSPs Input/Outp ut protected by TLS KTS (GCM) SSPs Input/Outp ut protected by TLS KTS (AES and HMAC) SSPs Input/Outp ut protected by SSH KTS (GCM) SSPs Input/Outp ut protected by SSH KTS (AES and HMAC)	Flash:Obfuscat ed	Until zeroized	Zeroizatio n command	
LUKS DB Password		Flash:Plaintext	Until zeroized	Zeroizatio n command	LUKS DB Salt :Used With
LUKS DB Salt		Flash:Plaintext	Until zeroized	Zeroizatio n command	LUKS DB Password:Used With
LUKS DB Integrity Key		Flash:Plaintext	Until zeroized	Zeroizatio n command	LUKS DB Password:Derived From LUKS DB Salt :Derived From
Firmware Load Test Key		Flash:Plaintext	N/A. This PSP is only used for Firmware Load Test,	N/A	

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
			which is not subject to the zeroization requirement s.		
SSH DH Private Key		DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio n Reboot	SSH DH Public Key:Paired With
SSH DH Public Key	Module Public Key Output	DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio n Reboot	SSH DH Private Key:Paired With
SSH Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio n Reboot	SSH DH Private Key:Used With
SSH DH Shared Secret		DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio n Reboot	SSH Encryption Key:Derived To SSH Integrity Key:Derived To SSH DH Private Key:Derived From SSH Peer DH Public Key:Derived From
SSH ECDH Private Key		DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio n Reboot	SSH ECDH Public Key:Paired With
SSH ECDH Public Key	Module Public Key Output	DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio	SSH ECDH Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
				n Reboot	
SSH Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio n Reboot	SSH ECDH Private Key:Used With
SSH ECDH Shared Secret		DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio n Reboot	SSH ECDH Private Key:Derived From SSH Peer ECDH Public Key:Derived From SSH Encryption Key:Derive To SSH Integrity Key:Derive To
SSH ECDSA Private Key		Flash:Plaintext	Until zeroized	Zeroizatio n command	SSH ECDSA Public Key:Paired With
SSH ECDSA Public Key	SSPs Input/Outp ut protected by TLS KTS (GCM) SSPs Input/Outp ut protected by TLS KTS (AES and HMAC) SSPs Input/Outp ut protected by SSH KTS (GCM) SSPs Input/Outp ut protected	Flash:Plaintext	Until zeroized	Zeroizatio n command	SSH ECDSA Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
	by SSH KTS (AES and HMAC)				
SSH RSA Private Key		Flash:Plaintext	Until zeroized	Zeroizatio n command	SSH RSA Public Key:Paired With
SSH RSA Public Key	SSPs Input/Outp ut protected by TLS KTS (GCM) SSPs Input/Outp ut protected by TLS KTS (AES and HMAC) SSPs Input/Outp ut protected by SSH KTS (GCM) SSPs Input/Outp ut protected by SSH KTS (AES and HMAC)	Flash:Plaintext	Until zeroized	Zeroizatio n command	SSH RSA Private Key:Paired With
SSH Encryption Key		DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session terminatio n Reboot	SSH Integrity Key:Used With
SSH Integrity Key		DRAM:Plaintext	while SSH session is on	Zeroizatio n command Session	SSH Encryption Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				termination Reboot	
TLS DH Private Key		DRAM:Plaintext	while TLS session is on	Zeroization command Session termination Reboot	TLS DH Public Key:Paired With
TLS DH Public Key	Module Public Key Output	DRAM:Plaintext	while TLS tunnel is on	Zeroization command Session termination Reboot	TLS DH Private Key:Paired With
TLS Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization command Session termination Reboot	TLS DH Private Key:Used With TLS DH Shared Secret:Derived To
TLS DH Shared Secret		DRAM:Plaintext	while TLS tunnel is on	Zeroization command Session termination Reboot	TLS DH Private Key:Derived From TLS Peer DH Public Key:Derived From
TLS ECDH Private Key		DRAM:Plaintext	while TLS tunnel is on	Zeroization command Session termination Reboot	TLS ECDH Public Key:Paired With
TLS ECDH Public Key	Module Public Key Output	DRAM:Plaintext	while TLS tunnel is on	Zeroization command Session termination Reboot	TLS ECDH Private Key:Paired With
TLS Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization command	TLS ECDH Private Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session termination Reboot	
TLS ECDH Shared Secret		DRAM:Plaintext	while TLS tunnel is on	Zeroization command Session termination Reboot	TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From
TLS ECDSA Private Key		Flash:Plaintext	Until zeroized	Zeroization command	TLS ECDSA Public Key:Paired With
TLS ECDSA Public Key	SSPs Input/Output protected by TLS KTS (GCM) SSPs Input/Output protected by TLS KTS (AES and HMAC) SSPs Input/Output protected by SSH KTS (GCM) SSPs Input/Output protected by SSH KTS (AES and HMAC)	Flash:Plaintext	Until zeroized	Zeroization command	TLS ECDSA Private Key:Paired With
TLS RSA Private Key		Flash:Plaintext	Until zeroized	Zeroization command	TLS RSA Public Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS RSA Public Key	SSPs Input/Output protected by TLS KTS (GCM) SSPs Input/Output protected by TLS KTS (AES and HMAC) SSPs Input/Output protected by SSH KTS (GCM) SSPs Input/Output protected by SSH KTS (AES and HMAC)	Flash:Plaintext	Until zeroized	Zeroization command	TLS RSA Private Key:Paired With
TLS Master Secret		DRAM:Plaintext	while TLS session is on	Zeroization command Session termination Reboot	TLS DH Shared Secret:Derived From
TLS Encryption Key		DRAM:Plaintext	while TLS session is on	Zeroization command Session termination Reboot	TLS Integrity Key:Used With
TLS Integrity Key		DRAM:Plaintext	while TLS session is on	Zeroization command Session	TLS Encryption Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				termination Reboot	
IPSec/IKE DH Private Key		DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE DH Public Key:Paired With
IPSec/IKE DH Public Key	Module Public Key Output	DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE DH Private Key:Paired With
IPSec/IKE Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE DH Private Key:Used With
IPSec/IKE DH Shared Secret		DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE SKEYSEED:Derive TO
IPSec/IKE ECDH Private Key		DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE ECDH Public Key:Paired With
IPSec/IKE ECDH Public Key	Module Public Key Output	DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE ECDH Private Key:Paired With
IPSec/IKE Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	while Control Panel	Zeroization command	IPSec/IKE ECDH Private Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			IPSec/IKE session is on	Session termination Reboot	
IPSec/IKE ECDH Shared Secret		DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE SKEYSEED:Derive To
IPSec/IKE ECDSA Private Key		Flash:Plaintext	Until zeroized	Zeroization command	IPSec/IKE ECDSA Public Key:Paired With
IPSec/IKE ECDSA Public Key	SSPs Input/Output protected by TLS KTS (GCM) SSPs Input/Output protected by TLS KTS (AES and HMAC) SSPs Input/Output protected by SSH KTS (GCM) SSPs Input/Output protected by SSH KTS (AES and HMAC)	Flash:Plaintext	Until zeroized	Zeroization command	IPSec/IKE ECDSA Private Key:Paired With
IPSec/IKE RSA Private Key		Flash:Plaintext	Until zeroized	Zeroization command	IPSec/IKE RSA Public Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IPSec/IKE RSA Public Key	SSPs Input/Output protected by TLS KTS (GCM) SSPs Input/Output protected by TLS KTS (AES and HMAC) SSPs Input/Output protected by SSH KTS (GCM) SSPs Input/Output protected by SSH KTS (AES and HMAC)	Flash:Plaintext	Until zeroized	Zeroization command	IPSec/IKE RSA Private Key:Paired With
IPSec/IKE Pre-shared Secret	SSPs Input/Output protected by TLS KTS (GCM) SSPs Input/Output protected by TLS KTS (AES and HMAC) SSPs Input/Output protected	Flash:Plaintext	Until zeroized	Zeroization command	IPSec/IKE SKEYSEED:Derived To

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	by SSH KTS (GCM) SSPs Input/Output protected by SSH KTS (AES and HMAC)				
IPSec/IKE SKEYSEED		DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	TLS ECDH Shared Secret:Derived From IPSec/IKE DH Shared Secret:Derived From
IPSec/IKE Encryption Key		DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE SKEYSEED:Derived From
IPSec/IKE Integrity Key		DRAM:Plaintext	while Control Panel IPSec/IKE session is on	Zeroization command Session termination Reboot	IPSec/IKE SKEYSEED:Derived From
SNMPv3 Authentication Secret	SSPs Input/Output protected by TLS KTS (GCM) SSPs Input/Output protected by TLS KTS (AES and HMAC)	Flash:Plaintext	Until zeroized	Zeroization command	

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
	SSPs Input/Outp ut protected by SSH KTS (GCM) SSPs Input/Outp ut protected by SSH KTS (AES and HMAC)				
SNMPv3 Encryption Key		DRAM:Plaintext	while SNMPv3 session is on	Zeroizatio n command Session terminatio n Reboot	SNMPv3 Authentication Secret:Derived From SNMPv3 Integrity Key:Used With
SNMPv3 Integrity Key		DRAM:Plaintext	while SNMPv3 session is on	Zeroizatio n command Session terminatio n Reboot	SNMPv3 Authentication Secret:Derived From SNMPv3 Encryption Key:Used With
Data Plane Encryption ECDH Private Key		DRAM:Plaintext	while Data Plane Encryption session is on	Zeroizatio n command Session terminatio n Reboot	Data Plane Encryption ECDH Public Key:Paired With
Data Plane Encryption ECDH Public Key	Module Public Key Output	DRAM:Plaintext	while Data Plane Encryption session is on	Zeroizatio n command Session terminatio n Reboot	IPSec/IKE ECDH Private Key:Paired With
Data Plane Encryption ECDH Shared Secret		DRAM:Plaintext	while Data Plane Encryption session is on	Zeroizatio n command Session terminatio	Data Plane Encryption ECDH Private Key:Derived From Data Plane

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
				n Reboot	Encryption Peer ECDH Public Key:Derived From Data Plane Encryption IKE-SA Session Key:Derived To Data Plane Encryption Child-SA Session Key :Derived To
Data Plane Encryption Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	while Data Plane Encryption session is on	Zeroizatio n command Session terminatio n Reboot	Data Plane Encryption ECDH Private Key:Used With
Data Plane Encryption ECDSA Private Key		Flash:Plaintext	Until zeroized	Zeroizatio n command	Data Plane Encryption ECDSA Private Key:Paired With
Data Plane Encryption ECDSA Public Key	SSPs Input/Outp ut protected by TLS KTS (GCM) SSPs Input/Outp ut protected by TLS KTS (AES and HMAC) SSPs Input/Outp ut protected by SSH KTS (GCM) SSPs Input/Outp ut protected	Flash:Plaintext	Until zeroized	Zeroizatio n command	Data Plane Encryption ECDSA Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	by SSH KTS (AES and HMAC)				
Data Plane Encryption RSA Private Key		Flash:Plaintext	Until zeroized	Zeroization command	Data Plane Encryption RSA Public Key:Paired With
Data Plane Encryption RSA Public Key	SSPs Input/Output protected by TLS KTS (GCM) SSPs Input/Output protected by TLS KTS (AES and HMAC) SSPs Input/Output protected by SSH KTS (GCM) SSPs Input/Output protected by SSH KTS (AES and HMAC)	Flash:Plaintext	Until zeroized	Zeroization command	Data Plane Encryption RSA Private Key:Paired With
Data Plane Encryption Pre-shared Secret	SSPs Input/Output protected by TLS KTS (GCM) SSPs Input/Output	Flash:Obfuscated	Until zeroized	Zeroization command	IPSec/IKE SKEYSEED:Used With IPSec/IKE Encryption Key:Derived to IPSec/IKE Authentication Key:Derived to

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
	protected by TLS KTS (AES and HMAC) SSPs Input/Outp ut protected by SSH KTS (GCM) SSPs Input/Outp ut protected by SSH KTS (AES and HMAC)				
Data Plane Encryption IKE-SA Session Key		DRAM:Plaintext	while Data Plane Encryption session is on	Zeroizatio n command Session terminatio n Reboot	Data Plane Encryption ECDH Shared Secret:Derived From
Data Plane Encryption Child-SA Session Key		DRAM:Plaintext	while Data Plane Encryption session is on	Zeroizatio n command Session terminatio n Reboot	Data Plane Encryption ECDH Shared Secret:Derived From
NTP Authenticati on Key	SSPs Input/Outp ut protected by TLS KTS (GCM) SSPs Input/Outp ut protected by TLS KTS (AES and	Flash:Plaintext	Until zeroized	Zeroizatio n command	

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
	HMAC) SSPs Input/Outp ut protected by SSH KTS (GCM) SSPs Input/Outp ut protected by SSH KTS (AES and HMAC)				
OSPFv2 Authenticati on Key	SSPs Input/Outp ut protected by TLS KTS (GCM) SSPs Input/Outp ut protected by TLS KTS (AES and HMAC) SSPs Input/Outp ut protected by SSH KTS (GCM) SSPs Input/Outp ut protected by SSH KTS (AES and HMAC)	Flash:Plaintext	Until Zeroized	Zeroizatio n command	

Table 18: SSP Table 2

9.5 Transitions

- SHA-1: The module includes an implementation of SHA-1 for hashing and digital signature verification. This implementation will be non-Approved for all uses starting January 1, 2031. At this time, the user should move to SHA2, which is available in this module.

- FIPS 186-4/186-5: As of February 5, 2024, the CMVP does not accept module submissions that implement DSA or RSA X9.31 in the approved mode, other than for signature verification which is approved for legacy use. This module does not implement DSA or RSA X9.31 for signature generation and therefore is unaffected by the current transition from 186-4 to 186-5. As detailed in section 2.7, the CAVP testing performed on the 186-4 algorithms is mathematically similar to the testing performed on the 186-5 algorithms and therefore this module claims compliance with 186-5. This means that no timeline exists in which any of the implemented algorithms will transition from approved to non-approved.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Gecko Firmware Bootloader Integrity Test	ECDSA SigVer P-256 with SHA2-256	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A3366
Gecko Firmware Application Integrity Test	ECDSA SigVer P-256 with SHA2-256	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A3366
CHM6_Zynq Firmware Bootloader Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4955
DCO_NXP Firmware Bootloader Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4955
DCO_Zynq Firmware Bootloader Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4955
XMM4_Intel Firmware Bootloader Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4955

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
CHM6_Zynq Firmware Kernel Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4952
CHM6_Zynq Firmware init script Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4948
CHM6_Zynq Firmware Application Manifest file Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4948
CHM6_Zynq Firmware Application Integrity Test	SHA2-512	KAT	SW/FW Integrity	Module is in normal state	SHA2-512 from SHA Cert. #A4954
DCO_NXP Firmware Kernel Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA from ECDSA Cert. #A4953
DCO_NXP Firmware init script Integrity	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4949
DCO_NXP Firmware Application Manifest file Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4949
DCO_NXP Firmware Application Integrity Test	SHA2-512	KAT	SW/FW Integrity	Module is in normal state	SHA2-512 from SHA Cert. #A4954
DCO_Zynq Firmware Kernel Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4961
DCO_Zynq Firmware Application Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4960
XMM4_Intel Firmware Kernel Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4962
XMM4_Intel Firmware init script Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA from ECDSA Cert. #A4956
XMM4 Intel Firmware Application Manifest file Integrity Test	ECDSA SigVer P-521 with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	ECDSA SigVer from ECDSA Cert. #A4956

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
XMM4 Intel Firmware Application Integrity Test	SHA2-512	KAT	SW/FW Integrity	Module is in normal state	SHA2-512 from SHA Cert. #A4958

Table 19: Pre-Operational Self-Tests

The module performs the following self-tests, including the pre-operational self-tests and Conditional self-tests. Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-tests. Following the successful pre-operational self-tests, the module executes the Conditional Cryptographic Algorithm Self-tests (CASTs). If anyone of the self-tests fails, the module transitions into an error state and outputs the error message via the module's status output interface. While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The error state can only be cleared by reloading the module. All self-tests must be completed successfully before the module transitions to the operational state.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 KAT (A3366)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A3366)	Curve: P-256	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4955)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4955)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4960)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4960)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-512 KAT (A4961)	SHA2-512	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4961)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4948)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4948)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4952)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4952)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4949)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4949)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4953)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4953)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4954)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
AES-CBC Encrypt KAT (A4959)	128 bits	Known Answer	CAST	Module is in	Encryption KAT	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
		Test (KAT)		normal state		
AES-CBC Decrypt KAT (A4959)	128 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Decryption KAT	Power up
AES-GCM Authenticated Encrypt KAT (A4959)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption KAT	Power up
AES-GCM Authenticated Decrypt KAT (A4959)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption KAT	Power up
Counter DRBG Generate/Reseed/Instantiate KAT (A4959)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	Generate KAT, Reseed KAT, and Instantiate KAT	Power up
KDF IKEv2 KAT (A4959)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
KAS-ECC-SSC Sp800-56Ar3 KAT (A4959)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
RSA SigGen (FIPS186-4) KAT (A4959)	Modulus: 2048 bits	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
RSA SigVer (FIPS186-4) KAT (A4959)	Modulus: 2048 bits	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4959)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-512 KAT (A4959)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4962)	Curve: P-521	Known Answer	CAST	Module is in	N/A	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
		Test (KAT)		normal state		
SHA2-512 KAT (A4962)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
AES-CBC Encrypt KAT (A4956)	128, 192 and 256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Encryption KAT	Power up
AES-CBC Decrypt KAT (A4956)	128, 192 and 256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Decryption KAT	Power up
AES-CCM Authenticated Encrypt KAT (A4956)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption KAT	Power up
AES-CCM Authenticated Decrypt KAT (A4956)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption KAT	Power up
AES-GCM Authenticated Encrypt KAT (A4956)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption KAT	Power up
AES-GCM Authenticated Decrypt KAT (A4956)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption KAT	Power up
HMAC-SHA-1 KAT (A4956)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-256 KAT (A4956)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-384 KAT (A4956)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-512 KAT (A4956)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4) KAT (A4956)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-256 KAT (A4957)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-256 KAT (A4957)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
AES-ECB Encrypt KAT (A4958)	128 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Encryption KAT	Power up
AES-ECB Decrypt KAT (A4958)	128 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Decryption KAT	Power up
AES-GCM Authenticated Encrypt KAT (A4958)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption KAT	Power up
AES-GCM Authenticated Decrypt KAT (A4958)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption KAT	Power up
Counter DRBG Generate/Reseed/Instantiate KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	Generate KAT, Reseed KAT, and Instantiate KAT	Power up
ECDSA SigGen (FIPS186-4) KAT (A4958)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) KAT (A4958)	Curve: P-521	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-256 KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SSH KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
KDF IKEv2 KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
KDF SNMP KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
TLS v1.2 KDF RFC7627 KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
TLS v1.3 KDF KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
KAS-ECC-SSC KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	KAS-ECC-SSC Primitive Z	Power up
KAS-FFC-SSC KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	KAS-FFC-SSC Primitive Z	Power up
PBKDF KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
RSA SigGen KAT (A4958)	Modulus: 2048 bits	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
RSA SigVer KAT (A4958)	Modulus: 2048 bits	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA-1 KAT (A4958)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA2-512 KAT (A4958)	N/A	Known Answer	CAST	Module is in	N/A	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
		Test (KAT)		normal state		
AES-GCM Authenticated Encrypt KAT (C501)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption KAT	Power up
AES-GCM Authenticated Decrypt KAT (C501)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption KAT	Power up
Entropy Source Start-up Health Test (RCT)	N/A	RCT	CAST	Module is in normal state	N/A	Power up
Entropy Source Start-up Health Test (APT)	N/A	APT	CAST	Module is in normal state	N/A	Power up
Entropy Source Continuous Health Test (RCT)	N/A	RCT	CAST	Module is in normal state	N/A	Power up
Entropy Source Continuous Health Test (APT)	N/A	APT	CAST	Module is in normal state	N/A	Power up
ECDSA KeyGen (FIPS186-4) PCT (A4958)	Curve: P-256	Pair-Wise Consistency Test (PCT)	PCT	Module is in normal state	N/A	ECDSA Keypair generation
RSA KeyGen (FIPS186-4) PCT (A4958)	Modulus: 2048 bits	Pair-Wise Consistency Test (PCT)	PCT	Module is in normal state	N/A	RSA Keypair generation
KAS-ECC-SSC (FIPS186-4) PCT (A4958)	Curve: P-256	Pair-Wise Consistency Test (PCT)	PCT	Module is in normal state	N/A	KAS-ECC Keypair generation
KAS-FFC-SSC (FIPS186-4) PCT (A4958)	MODP-2048	Pair-Wise Consistency Test (PCT)	PCT	Module is in normal state	N/A	KAS-FFC Keypair generation
KAS-ECC-SSC Sp800-56Ar3 PCT (A4959)	Curve: P-256	Pair-Wise Consistency Test (PCT)	PCT	Module is in normal state	N/A	ECDSA Keypair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA KeyGen (FIPS186-4) PCT (A4959)	Curve: P-256	Pair-Wise Consistency Test (PCT)	PCT	Module is in normal state	N/A	ECDSA Keypair generation
Firmware Load Test	Curve: P-521	ECDSA SigVer	SW/FW Load	Module is in normal state	N/A	Firmware Load Test

Table 20: Conditional Self-Tests

The module performs on-demand self-tests initiated by the operator, by powering off and powering the module back on. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Gecko Firmware Bootloader Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
Gecko Firmware Application Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
CHM6_Zynq Firmware Bootloader Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
DCO_NXP Firmware Bootloader Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
DCO_Zynq Firmware Bootloader Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
XMM4_Intel Firmware Bootloader Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
CHM6_Zynq Firmware Kernel Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
CHM6_Zynq Firmware init	KAT	SW/FW Integrity	On-demand	Module Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
script Integrity Test				
CHM6_Zynq Firmware Application Manifest file Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
CHM6_Zynq Firmware Application Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
DCO_NXP Firmware Kernel Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
DCO_NXP Firmware init script Integrity	KAT	SW/FW Integrity	On-demand	Module Reboot
DCO_NXP Firmware Application Manifest file Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
DCO_NXP Firmware Application Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
DCO_Zynq Firmware Kernel Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
DCO_Zynq Firmware Application Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
XMM4_Intel Firmware Kernel Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
XMM4_Intel Firmware init script Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
XMM4 Intel Firmware Application Manifest file Integrity Test	KAT	SW/FW Integrity	On-demand	Module Reboot
XMM4 Intel Firmware	KAT	SW/FW Integrity	On-demand	Module Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Application Integrity Test				

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 KAT (A3366)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A3366)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4955)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4955)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4960)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4960)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4961)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4961)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4948)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4948)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4952)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4952)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4949)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) KAT (A4949)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4953)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4953)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4954)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-CBC Encrypt KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-CBC Decrypt KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-GCM Authenticated Encrypt KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-GCM Authenticated Decrypt KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
Counter DRBG Generate/Reseed/Instantiate KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
KDF IKEv2 KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
RSA SigGen (FIPS186-4) KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
RSA SigVer (FIPS186-4) KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
HMAC-SHA2-512 KAT (A4959)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4962)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-512 KAT (A4962)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-CBC Encrypt KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-CBC Decrypt KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-CCM Authenticated Encrypt KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-CCM Authenticated Decrypt KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-GCM Authenticated Encrypt KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-GCM Authenticated Decrypt KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
HMAC-SHA-1 KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
HMAC-SHA2-256 KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
HMAC-SHA2-384 KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
HMAC-SHA2-512 KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4956)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-256 KAT (A4957)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
HMAC-SHA2-256 KAT (A4957)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-ECB Encrypt KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-ECB Decrypt KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM Authenticated Encrypt KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-GCM Authenticated Decrypt KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
Counter DRBG Generate/Reseed/Instantiate KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigGen (FIPS186-4) KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
ECDSA SigVer (FIPS186-4) KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
HMAC-SHA2-256 KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
KDF SSH KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
KDF IKEv2 KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
KDF SNMP KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
TLS v1.2 KDF RFC7627 KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
TLS v1.3 KDF KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
KAS-ECC-SSC KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
KAS-FFC-SSC KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
PBKDF KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
RSA SigGen KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
RSA SigVer KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
SHA2-512 KAT (A4958)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-GCM Authenticated Encrypt KAT (C501)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
AES-GCM Authenticated Decrypt KAT (C501)	Known Answer Test (KAT)	CAST	On-demand	Module Reboot
Entropy Source Start-up Health Test (RCT)	RCT	CAST	On-demand	Module Reboot
Entropy Source Start-up Health Test (APT)	APT	CAST	On-demand	Module Reboot
Entropy Source Continuous Health Test (RCT)	RCT	CAST	On-demand	Module Reboot
Entropy Source Continuous Health Test (APT)	APT	CAST	On-demand	Module Reboot
ECDSA KeyGen (FIPS186-4) PCT (A4958)	Pair-Wise Consistency Test (PCT)	PCT	On-demand	Module Reboot
RSA KeyGen (FIPS186-4) PCT (A4958)	Pair-Wise Consistency Test (PCT)	PCT	On-demand	Module Reboot
KAS-ECC-SSC (FIPS186-4) PCT (A4958)	Pair-Wise Consistency Test (PCT)	PCT	On-demand	Module Reboot
KAS-FFC-SSC (FIPS186-4) PCT (A4958)	Pair-Wise Consistency Test (PCT)	PCT	On-demand	Module Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A4959)	Pair-Wise Consistency Test (PCT)	PCT	On-demand	Module Reboot
ECDSA KeyGen (FIPS186-4) PCT (A4959)	Pair-Wise Consistency Test (PCT)	PCT	On-demand	Module Reboot
Firmware Load Test	ECDSA SigVer	SW/FW Load	On-demand	Module Reboot

Table 22: Conditional Periodic Information

10.4 Operator Initiation of Self-Tests

On demand and periodic self-tests are performed by powering off the module and powering it on again. This service performs the same cryptographic algorithm tests executed during pre-operational self-tests and CASTs. During the execution of the periodic and on-demand

self-tests, crypto services are not available and no data output or input is possible.

10.5 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	If self-test tests fail, the module is put into an error state	Self-tests failure	Reboot the module	System Halt

Table 23: Error States

If any of the above-mentioned self-tests fail, the module reports the error and enters the Error state. In the Error State, no cryptographic services are provided, and data output is prohibited. The only method to recover from the error state is to reboot the module and perform the self-tests, including the pre-operational firmware integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational firmware integrity test and the conditional CASTs.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module meets all the Level 1 requirements for FIPS 140-3. Follow the secure operations provided below to place the module in approved mode. Operating this module without maintaining the following settings would put module operated in a non-compliance state.

Secure Operation

The Security Admin (SA) must configure and enforce the following initialization steps.

Step 1. Strictly follow up the steps in section Physical Security to place the Opacity Shield and Tamper Evident Labels on the module.

Step 2. Ensure that the firmware version R6.2.2 or R6.2.3 is running on the module. To verify the firmware version, the Security Admin (SA) shall use the following command.

```
>show sw-management software-load-active swload-version swload-label
software-load-active

swload-version              'R6.2.2'
```

or

```
>show sw-management software-load-active swload-version swload-label
software-load-active

swload-version              'R6.2.3'
```

Step 3. Enable approved mode.

Execute the following steps to enable approved mode on the module:

- To enable approved mode via CLI:

  Execute the following command from the CLI interface:

  ‘fips mode-enable’

  A confirmation message is displayed.

  Enter y to proceed with the operation.

  This operation will cold reboot the system, delete the entire system configuration, including networking details, and may leave the system unreachable until the reboot is complete.

- To enable approved mode via WebGUI:

  Navigate to Security > FIPS tab.

  Click ‘FIPS Control’.

  A pop-up window is displayed.

  Select mode-enable against Action field and click Submit.

  A success message is displayed

Step 4. Create the User account and privileges for other roles defined in the Security Policy.

Step 5. Ensuring that any of the deleted/deprecated algorithms by NIST SP800-140Crev2 and/or NIST SP800-131Arev2 are disabled as applicable in the FIPS 140-3 validated firmware.

11.2 Administrator Guidance

No specific Administrator guidance.

11.3 Non-Administrator Guidance

No specific Non-Administrator guidance.

12 Mitigation of Other Attacks

N/A for this module.