SUSE LLC

SUSE Linux Enterprise GnuTLS Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Prepared by:

atsec information security corporation
4516 Seton Center Pkwy, Suite 250
Austin, TX 78759
www.atsec.com

Document version: 1.2
Last update: 2026-06-03

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 1.2 of the SUSE Linux Enterprise GnuTLS Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

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	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	N/A
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

1.3 Additional Information

In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy was submitted to the vendor, who would then edit, modify, and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The SUSE Linux Enterprise GnuTLS Cryptographic Module (hereafter referred to as "the module") is a software module in a multi-chip standalone embodiment. The module is an open-source, general-purpose set of libraries designed to support cross-platform development of security-enabled client and server applications and provides cryptographic services to applications running in the user space of the underlying operating system through a C language Application Program Interface (API).

Module Type: Software

Module Embodiment: MultiChipStand

Cryptographic Boundary:

The block diagram in Figure 1 shows the cryptographic boundary of the module, its interfaces with the operational environment and the flow of information between the module and operator (depicted through the arrows).

The entropy source is located within the module's physical perimeter and outside of the module's cryptographic boundary.

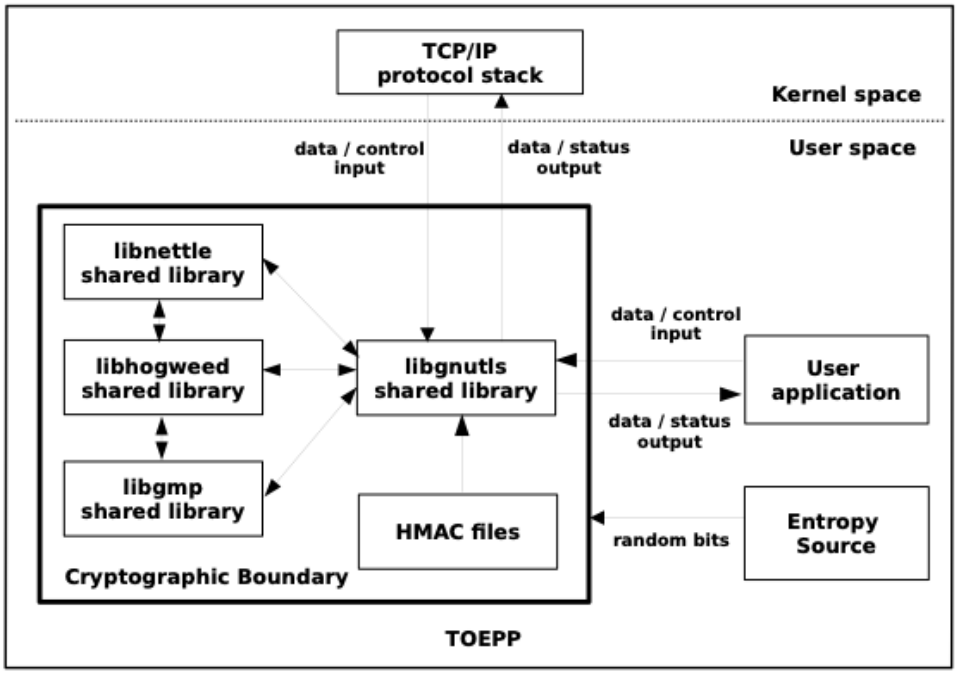

Figure 1: Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP of the module is defined as the general-purpose computer on which the module is installed. The module makes use of an SP800-90B-compliant Entropy Source (described in Section 2.8) located within the TOEPP.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
/usr/lib64/libgnutls.so.30, /usr/lib64/libnettle.so.8, /usr/lib64/libhogweed.so.6, /usr/lib64/libgmp.so.10, /usr/lib64/.libgnutls.so.30.hmac, /libs/usr/lib64/.libnettle.so.8.hmac, /libs/usr/lib64/.libhogweed.so.6.hmac, /libs/usr/lib64/.libgmp.so.10.hmac on AMD EPYCTM 7343 or Intel® Xeon® Gold 5416S	1.2	N/A	HMAC-SHA-256
/usr/lib64/libgnutls.so.30, /usr/lib64/libnettle.so.8, /usr/lib64/libhogweed.so.6, /usr/lib64/libgmp.so.10, /usr/lib64/.libgnutls.so.30.hmac, /libs/usr/lib64/.libnettle.so.8.hmac, /libs/usr/lib64/.libhogweed.so.6.hmac, /libs/usr/lib64/.libgmp.so.10.hmac on Ampere® Altra® Q80-30	1.2	N/A	HMAC-SHA-256
/usr/lib64/libgnutls.so.30, /usr/lib64/libnettle.so.8, /usr/lib64/libhogweed.so.6, /usr/lib64/libgmp.so.10, /usr/lib64/.libgnutls.so.30.hmac, /libs/usr/lib64/.libnettle.so.8.hmac, /libs/usr/lib64/.libhogweed.so.6.hmac, /libs/usr/lib64/.libgmp.so.10.hmac on IBM® TelumTM	1.2	N/A	HMAC-SHA-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
SUSE Linux Enterprise Server 15 SP6	SuperMicro SuperChassis 825BTQC-R1K23LPB and Motherboard H12DSi-NT6	AMD EPYC(TM) 7343	Yes	N/A	1.2
SUSE Linux Enterprise Server 15 SP6	SuperMicro SuperChassis 825BTQC-R1K23LPB and Motherboard H12DSi-NT6	AMD EPYC(TM) 7343	No	N/A	1.2
SUSE Linux Enterprise Server 15 SP6	GIGABYTE R152-P30	Ampere® Altra® Q80-30	Yes	N/A	1.2
SUSE Linux Enterprise Server 15 SP6	GIGABYTE R152-P30	Ampere® Altra® Q80-30	No	N/A	1.2
SUSE Linux Enterprise Server 15 SP6	IBM z16 A01	IBM® Telum(TM)	Yes	N/A	1.2
SUSE Linux Enterprise Server 15 SP6	IBM z16 A01	IBM® Telum(TM)	No	N/A	1.2
SUSE Linux Enterprise Server 15 SP6	ASUS RS700-E11-RS4U	Intel® Xeon® Gold 5416S	Yes	N/A	1.2
SUSE Linux Enterprise Server 15 SP6	ASUS RS700-E11-RS4U	Intel® Xeon® Gold 5416S	No	N/A	1.2

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

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

Operating System	Hardware Platform
SUSE Linux Enterprise Server for SAP 15SP6	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Server for SAP 15SP6	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Desktop 15SP6	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Desktop 15SP6	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343

Operating System	Hardware Platform
SUSE Linux Enterprise Base Container Image 15SP6	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Base Container Image 15SP6	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Base Container Image 15SP6	GIGABYTE R152-P30 on Ampere® Altra® Q80-30
SUSE Linux Enterprise Base Container Image 15SP6	IBM z16 A01 on IBM® Telum(TM)
SUSE Linux Enterprise Server 15SP6	IBM LinuxONE III Model LT1 on z15
SUSE Linux Enterprise Server Real Time 15SP6	QEMU VM on AMD EPYC(TM) 7773X
SUSE Linux Enterprise Desktop 15SP6	QEMU VM on AMD EPYC(TM) 7773X
SUSE Linux Enterprise Desktop 15SP6	QEMU VM on Intel® i7-1195G7
SUSE Linux Enterprise Base Container Image 15SP6	QEMU VM on Intel® Xeon® Gold 6338
SUSE Linux Enterprise Base Container Image 15SP6	QEMU VM on Ampere® Altra® Q80-30
SUSE Linux Enterprise Base Container Image 15SP6	IBM LinuxONE III Model LT1 QEMU VM on z15
SUSE Linux Enterprise Server 15SP6	IBM LinuxONE III Model LT1 QEMU VM on z15
SUSE Linux Enterprise Server 15SP6	QEMU VM on AMD EPYC(TM) 7773X
SUSE Linux Enterprise Server 15SP6	QEMU VM on Ampere® Altra® Q80-30
SUSE Linux Enterprise Server for SAP 15SP6	QEMU VM on Intel® Xeon® Gold 5218R
SUSE Linux Enterprise Server for SAP 15SP7	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Server for SAP 15SP7	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Desktop 15SP7	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S

Operating System	Hardware Platform
SUSE Linux Enterprise Desktop 15SP7	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Base Container Image 15SP7	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Base Container Image 15SP7	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Base Container Image 15SP7	GIGABYTE R152-P30 on Ampere® Altra® Q80-30
SUSE Linux Enterprise Base Container Image 15SP7	IBM z16 A01 on IBM® Telum(TM)
SUSE Linux Enterprise Base Container Image 15SP7	IBM LinuxONE III Model LT1 on z15
SUSE Linux Enterprise Server 15SP7	IBM LinuxONE III Model LT1 on z15
SUSE Linux Enterprise Server 15SP7	IBM z16 A01 on IBM® Telum(TM)
SUSE Linux Enterprise Server 15SP7	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Server 15SP7	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Server 15SP7	GIGABYTE R152-P30 on Ampere® Altra® Q80-30

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

The module is considered to maintain compliance with the FIPS 140-3 validation for SUSE products when operating on any general-purpose platform/processor that supports the SUSE Linux Enterprise Server operating system per the vendor affirmation from SUSE based on the allowance FIPS 140-3 management manual [FIPS140-3_MM] section 7.9.1 bullet 1 a i).

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

There are no components within the cryptographic boundary excluded from the FIPS 140-3 requirements.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	Automatically entered whenever an approved service is requested.	Approved	Equivalent to the indicator of the requested service (gnutls_fips140_get_operation_state() query function returns GNUTLS_FIPS140_OP_APPROVED)
Non-Approved	Automatically entered whenever a non-approved service is requested.	Non-Approved	Equivalent to the indicator of the requested service (gnutls_fips140_get_operation_state() query function returns GNUTLS_FIPS140_OP_NOT_APPROVED)

Table 5: Modes List and Description

When the module starts up successfully, after passing all the pre-operational and conditional cryptographic algorithms self-tests (CASTs), the module is operating in the approved mode of operation by default

Mode Change Instructions and Status:

If the module is in the approved mode, it can only be transitioned into the non-approved mode by calling one of the non-approved services listed in the Non-Approved, Not Allowed Algorithms Table. Please see section 4 for the details on service indicator provided by the module that identifies when an approved service is called.

Degraded Mode Description:

The module does not implement a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6360, A6361, A6362, A6363, A6368, A6372, A6374, A6375	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A6360, A6372, A6374	Key Length - 128, 256	SP 800-38C
AES-CFB8	A6365, A6366, A6371	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A6360, A6363, A6368, A6374	Direction - Generation Key Length - 128, 256	SP 800-38B
AES-ECB	A6373	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6360, A6361, A6362, A6363,	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
	A6368, A6372, A6374, A6375		
AES-GMAC	A6368	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D
AES-XTS Testing Revision 2.0	A6369	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A6368	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - No	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6368	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-4)	A6368	Curve - P-192	FIPS 186-4
ECDSA KeyVer (FIPS186-5)	A6368	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6368	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6368	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA-1	A6363, A6368, A6372, A6376	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6363, A6368, A6372, A6376	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6363, A6368, A6372, A6376	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6363, A6368, A6372, A6376	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6363, A6368, A6372, A6376	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6368	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme -	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
		ephemeralUnified - KAS Role - initiator, responder	
KAS-FFC-SSC Sp800-56Ar3	A6368	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
KDA HKDF Sp800-56Cr1	A6367	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-65336 Increment 8 HMAC Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-56C Rev. 2
KDF TLS (CVL)	A6368	TLS Version - v1.0/1.1	SP 800-135 Rev. 1
PBKDF	A6368	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-5)	A6368	Key Generation Mode - provable Hash Algorithm - SHA2-384 Modulo - 2048, 3072, 4096, 6144, 8192 Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A6368	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6368	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
Safe Primes Key Generation	A6368	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
SHA-1	A6363, A6368, A6372, A6376	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-224	A6363, A6368, A6372, A6376	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A6363, A6368, A6372, A6376	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A6363, A6368, A6372, A6376	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A6363, A6368, A6372, A6376	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA3-224	A6364, A6370	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-256	A6364, A6370	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-384	A6364, A6370	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-512	A6364, A6370	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
TLS v1.2 KDF RFC7627 (CVL)	A6368	Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1

Table 6: Approved Algorithms

The above table lists all approved cryptographic algorithms of the module, including specific key lengths employed for approved services, and implemented modes or methods of operation of the algorithms.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Asymmetric Key Pair Generation (CKG)	Key Type:Asymmetric	N/A	SP 800-133r2, section 4 example 1

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
MD5	Only allowed as the PRF in TLSv1.0 and v1.1 per IG 2.4.A	Message digest used in TLSv1.0/v1.1 KDF only for legacy use

Table 8: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
Blowfish	Symmetric encryption; Symmetric decryption
Camellia	Symmetric encryption; Symmetric decryption
CAST	Symmetric encryption; Symmetric decryption
ChaCha20	Symmetric encryption; Symmetric decryption
ChaCha20 and Poly1305	Authenticated encryption; Authenticated decryption
AES-GCM (when not used in the context of the TLS protocol)	Authenticated encryption; Authenticated decryption
DES	Symmetric encryption; Symmetric decryption
Diffie-Hellman with keys generated with domain parameters other than safe primes	Key agreement; Shared secret computation
DRBG when key length is less than 112 bits	Symmetric key generation
DSA	Key generation; Domain parameter generation; Digital signature generation; Digital signature verification
ECDSA with curves not listed in Table "Approved Algorithms"	Key generation; Public key verification
ECDSA with curves not listed in Table "Approved Algorithms" or hash functions other than SHA2-224, SHA2-256, SHA2-384, SHA2-512	Digital signature generation; Digital signature verification
EC Diffie-Hellman with curves not listed in Table "Approved Algorithms"	Key agreement; Shared secret computation
GOST	Symmetric encryption; Symmetric decryption; Message digest
HMAC with keys smaller than 112-bit	Message authentication code (MAC)
HMAC with GOST	Message authentication code (MAC)
MD2	Message digest; Message authentication code (MAC)
MD4	Message digest; Message authentication code (MAC)

Name	Use and Function
MD5	Message digest; Message authentication code (MAC)
Non-supported cipher suites (not listed in Appendix A)	Transport Layer Security (TLS) Network Protocol
PBKDF with non-approved message digest algorithms	Key derivation
RC2	Symmetric encryption; Symmetric decryption
RC4	Symmetric encryption; Symmetric decryption
RMD160	Message digest; Message authentication code (MAC)
RSA (with keys smaller than 2048 bits and/or hash functions other than SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature generation; Digital signature verification
RSA (with keys smaller than 2048 bits)	Key generation
RSA (with any key sizes)	Key encapsulation; Key unencapsulation
Salsa20	Symmetric encryption; Symmetric decryption
SM3	Message digest
Serpent	Symmetric encryption; Symmetric decryption
STREEBOG	Message digest; Message authentication code (MAC)
Triple-DES	Symmetric encryption; Symmetric decryption
Twofish	Symmetric encryption; Symmetric decryption
UMAC	Message authentication code (MAC)
Yarrow	Random number generation

Table 9: Non-Approved, Not Allowed Algorithms

The above table lists non-Approved security functions that are not allowed in the approved mode of operation.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric Encryption with AES	BC-UnAuth	Encryption using AES		AES-CBC: (A6360, A6361, A6362, A6363, A6368, A6372, A6374, A6375) AES-CFB8: (A6365, A6366, A6371)

Name	Type	Description	Properties	Algorithms
				AES-XTS Testing Revision 2.0: (A6369)
Symmetric Decryption with AES	BC-UnAuth	Decryption using AES		AES-CBC: (A6360, A6361, A6362, A6363, A6368, A6372, A6374, A6375) AES-CFB8: (A6365, A6366, A6371) AES-XTS Testing Revision 2.0: (A6369)
Authenticated Encryption with AES	BC-Auth	Authenticated encryption using AES		AES-CCM: (A6360, A6372, A6374)
Authenticated Decryption with AES	BC-Auth	Authenticated decryption using AES		AES-CCM: (A6360, A6372, A6374)
Authenticated Encryption in the context of TLS protocol	BC-Auth	Authenticated encryption using AES-GCM, AES-CCM, HMAC+AES-CBC (in the context of the TLS 1.2/1.3 protocol)		AES-GCM: (A6360, A6361, A6362, A6363, A6368, A6372, A6374, A6375) HMAC-SHA-1: (A6363, A6368, A6372, A6376) HMAC-SHA2-224: (A6363, A6368, A6372, A6376) HMAC-SHA2-256: (A6363, A6368, A6372, A6376) HMAC-SHA2-384: (A6363, A6368, A6372, A6376) HMAC-SHA2-512: (A6363, A6368, A6372, A6376) AES-CBC: (A6360, A6361, A6362, A6363, A6368, A6372, A6374, A6375)

Name	Type	Description	Properties	Algorithms
Authenticated Decryption in the context of TLS protocol	BC-Auth	Authenticated decryption using AES-GCM, AES-CCM, HMAC+AES-CBC (in the context of the TLS 1.2/1.3 protocol)		AES-GCM: (A6360, A6361, A6362, A6363, A6368, A6372, A6374, A6375) HMAC-SHA-1: (A6363, A6368, A6372, A6376) HMAC-SHA2-224: (A6363, A6368, A6372, A6376) HMAC-SHA2-256: (A6363, A6368, A6372, A6376) HMAC-SHA2-384: (A6363, A6368, A6372, A6376) HMAC-SHA2-512: (A6363, A6368, A6372, A6376) AES-CBC: (A6360, A6361, A6362, A6363, A6368, A6372, A6374, A6375)
Message Digest with SHA	SHA	Message digest using SHA		SHA-1: (A6363, A6368, A6372, A6376) SHA2-224: (A6363, A6368, A6372, A6376) SHA2-256: (A6363, A6368, A6372, A6376) SHA2-384: (A6363, A6368, A6372, A6376) SHA2-512: (A6363, A6368, A6372, A6376) SHA3-224: (A6364, A6370) SHA3-256: (A6364, A6370) SHA3-384: (A6364, A6370)

Name	Type	Description	Properties	Algorithms
				SHA3-512: (A6364, A6370)
Random Number Generation with CTR_DRBG	DRBG	Random number generation using CTR_DRBG		Counter DRBG: (A6368) AES-ECB: (A6373)
Message Authentication Code (MAC) with HMAC	MAC	Message authentication code using HMAC		HMAC-SHA-1: (A6363, A6368, A6372, A6376) HMAC-SHA2-224: (A6363, A6368, A6372, A6376) HMAC-SHA2-256: (A6363, A6368, A6372, A6376) HMAC-SHA2-384: (A6363, A6368, A6372, A6376) HMAC-SHA2-512: (A6363, A6368, A6372, A6376)
Message Authentication Code (MAC) with AES	MAC	Message authentication code using AES		AES-CMAC: (A6360, A6363, A6368, A6374) AES-GMAC: (A6368)
Digital Signature Generation with RSA	DigSig-SigGen	Digital signature generation using RSA		RSA SigGen (FIPS186-5): (A6368)
Digital Signature Verification with RSA	DigSig-SigVer	Digital signature verification using RSA		RSA SigVer (FIPS186-5): (A6368)
Digital Signature Generation with ECDSA	DigSig-SigGen	Digital signature generation using ECDSA		ECDSA SigGen (FIPS186-5): (A6368)
Digital Signature Verification with ECDSA	DigSig-SigVer	Digital signature verification using ECDSA		ECDSA SigVer (FIPS186-5): (A6368)
Public Key Verification with ECDSA	AsymKeyPair-KeyVer	Public key verification using ECDSA		ECDSA KeyVer (FIPS186-5): (A6368)

Name	Type	Description	Properties	Algorithms
Public Key Verification with ECDSA (Legacy)	AsymKeyPair-KeyVer	Public key verification using ECDSA (FIPS 186-4)	Compliance:IG C.M resolution 3c and 3d	ECDSA KeyVer (FIPS186-4): (A6368)
Shared Secret Computation with EC Diffie-Hellman	KAS-SSC	Shared secret computation per SP800-56ARev3	Compliance:IG D.F scenario 2 path (1)	KAS-ECC-SSC Sp800-56Ar3: (A6368)
Shared Secret Computation with Diffie-Hellman	KAS-SSC	Shared secret computation per SP800-56ARev3	Compliance:IG D.F scenario 2 path (1)	KAS-FFC-SSC Sp800-56Ar3: (A6368)
Key Derivation with PBKDF	PBKDF	Key derivation using PBKDF		PBKDF: (A6368)
Key Derivation with TLS 1.0, 1.1, 1.2 KDF	KAS-135KDF	Key derivation using TLS KDF (CVL) / TLS v1.2 KDF RFC7627 (CVL)		TLS v1.2 KDF RFC7627: (A6368) KDF TLS: (A6368)
Key Derivation (as part of TLSv1.3) with KDA HKDF	KAS-56CKDF	Key derivation using KDA HKDF		KDA HKDF Sp800-56Cr1: (A6367)
TLS Handshake (KAS)	KAS-Full	ECDH/DH Key Agreement	IG:IG D.F scenario 2 path (2) Key confirmation:No Key derivation:IG 2.4.B SP 800-135rev1 CVL and KDA (separately tested) Caveat:Key establishment methodology provides between 112 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A6368) KAS-FFC-SSC Sp800-56Ar3: (A6368) KDA HKDF Sp800-56Cr1: (A6367) TLS v1.2 KDF RFC7627: (A6368) KDF TLS: (A6368)
Key Pair Generation with RSA	AsymKeyPair-KeyGen CKG	Key Generation using RSA		RSA KeyGen (FIPS186-5): (A6368) Asymmetric Key Pair Generation (CKG): ()

Name	Type	Description	Properties	Algorithms
Key Pair Generation with ECDSA	AsymKeyPair-KeyGen CKG	Generate ECDSA key pairs		ECDSA KeyGen (FIPS186-5): (A6368) Asymmetric Key Pair Generation (CKG): ()
Key Pair Generation with Safe Primes	AsymKeyPair-KeyGen CKG	Key Pair Generation with Safe Primes		Safe Primes Key Generation: (A6368) Asymmetric Key Pair Generation (CKG): ()

Table 10: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES-XTS

The AES algorithm in XTS mode can be only used for the cryptographic protection of data on storage devices, as specified in [SP800-38E]. The length of a single data unit encrypted with the XTS-AES shall not exceed 2^{20} AES blocks, that is 16MB of data.

To meet the requirement stated in IG C.I, the module implements a check that ensures, before performing any cryptographic operation, that the two AES keys used in AES XTS mode are not identical. As the module does not generate symmetric keys, the check is performed when keys are input to the service APIs.

The two XTS keys shall be generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133rev2, Sec. 6.3.

Note: AES-XTS shall be used with 128 and 256-bit keys only.

2.7.2 AES-GCM IV

The module implements AES GCM for being used in the TLS v1.2 and v1.3 protocols. AES GCM IV generation is compliant with [FIPS140-3_IG] IG C.H for both protocols as follows:

- For TLS v1.2, IV generation is compliant with scenario 1.a of IG C.H and [RFC5288]. The module supports acceptable AES-GCM cipher suites from section 3.3.1 of [SP800-52rev2].
- For TLS v1.3, IV generation is compliant with scenario 5 of IG C.H and [RFC8446]. The module supports acceptable AES-GCM cipher suites from section 3.3.1 of [SP800-52rev2].

The IV generated in both scenarios is only used within the context of the TLS protocol implementation. The nonce explicit part of the IV does not exhaust the maximum number of possible values for a given session key. The design of the TLS protocol in this module implicitly ensures that the nonce explicit, or counter portion of the IV will not exhaust all its possible values.

In case the module's power is lost and then restored, the key used for the AES-GCM encryption or decryption shall be redistributed.

2.7.3 Key Derivation using SP 800-132 PBKDF2

The module provides password-based key derivation (PBKDF), compliant with SP800-132 and IG D.N. The module supports option 1a from section 5.4 of [SP800-132], in which the Master Key (MK) or a segment of it is used directly as the Data Protection Key (DPK).

In accordance with [SP800-132], the following requirements shall be met.

- Derived keys shall only be used in storage applications. The Master Key (MK) shall not be used for other purposes. The module only allows use of MK or DPK with at least 112 bits.
- The module only allows a portion of the salt with a length of at least 128 bits, which shall be generated randomly using the SP800- 90Arev1 DRBG.
- The iteration count shall be selected as large as possible, as long as the time required to generate the key using the entered password is acceptable for the users. The minimum value allowed by the module is 1000.
- Passwords or passphrases, used as an input for the PBKDF, shall not be used as cryptographic keys.
- The module only allows password or passphrase with at least 8 characters, consisting of lower-case, upper-case, and numeric characters. The probability of guessing the value is estimated to be $1/62^8 = 10^{-14}$, which is less than 2^{-112}. If the password consists of only digits (worst case), the probability of guessing the value is estimated to be 10^{-8} which is less than 2^{-112}.

2.7.4 SP 800-56ARev3 Assurances

To comply with the assurances listed in section 5.6.2 of SP 800-56ARev3, the operator must use the module in the context of the TLS protocol and the following steps shall be performed:

1. The entity using the module, must use the module's "Key pair generation" service for generating DH/ECDH ephemeral keys. This meets the assurances required by key pair owner defined in the section 5.6.2.1 of SP 800-56ARev3.
2. As part of the module's shared secret computation (SSC) service, the module internally performs the public key validation on the peer's public key passed in as input to the SSC function. This meets the public key validity assurance required by the sections 5.6.2.2.1/5.6.2.2.2 of SP 800-56ARev3.

The module does not support static keys therefore the "assurance of peer's possession of private key" is not applicable.

2.7.5 RSA Key Generation

In compliance with IG C.E, the module generates RSA signature keys using an approved method of FIPS 186-5: generation of random primes that are provably prime. The RSA key generation has been tested for all module lengths available in CAVP testing: 2048, 3072, 4096, 6144, and 8192-bits. The CAVP certificate in table 2.5 indicates that the RSA key generating algorithm has been tested and validated for conformance to the methods in FIPS 186-5. The number of Miller-Rabin tests is consistent with the bit sizes of p and q from Table B.1 of FIPS 186-5.

2.7.6 RSA Signature Generation and Signature Verification

The module provides RSA signature generation and signature verification compliant with IG C.F. The module supports RSA modulus lengths greater than or equal to 2048 bits for both signature generation and signature verification. The RSA signature generation and signature verification implementations have been tested for all module lengths available in CAVP testing: 2048, 3072, and 4096 bits.

2.7.7 SHA-1 Use

SHA-1 is only approved when used in approved mode for message digest, message authentication and KDF (PBKDF). The use of SHA-1 for digital signature generation (e.g., ECDSA, RSA) or verification is non-approved.

2.7.8 SHA-3

The module provides SHA-3 hash functions compliant with IG C.C. Every implementation of each SHA-3 function was tested and validated on all the module's operating environments. SHAKE functions are not implemented. SHA-3 hash functions are not used as part of a higher-level algorithm.

2.7.9 Hash Algorithms

In compliance with IG C.B, every approved hash algorithm implementation was CAVP tested and validated on all the module's operational environments. Section 2.5 of this security policy contains a table of the CAVP certificates of the approved hash functions.

For the higher-level algorithms that use the approved hash functions - ECDSA SigGen, ECDSA SigVer, HMAC, KDA HKDF Sp800-56Cr1, KDF TLS (CVL), TLS v1.2 KDF RFC7627 (CVL), PBKDF2, RSA SigGen, RSA SigVer – every implemented combination for which CAVP testing exists was CAVP tested and validated on all the module's operational environments. Section 2.5 of this security policy contains a table of the CAVP certificates of these higher-level algorithms.

2.7.10 Authenticated Encryption / Authenticated Decryption

The module does not establish SSPs using an approved key transport scheme (KTS). However, it does offer approved authenticated algorithms that can be used by an external operator/application as part of an approved KTS.

2.7.11 Legacy Algorithms

The cryptographic module implements the following cryptographic algorithms for legacy use. Algorithms designated as "Legacy" can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M:

- ECDSA KeyVer (FIPS-186-4) with P-192.

2.8 RBG and Entropy

Cert Number	Vendor Name
E200	SUSE LLC

Table 11: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
SUSE Userspace Standalone	Non-Physical	SUSE Linux Enterprise Server 15 SP6 on AMD EPYCTM 7343; SUSE Linux Enterprise Server 15 SP6 on Ampere® Altra® Q80-30; SUSE Linux Enterprise	256 bits	256 bits	SHA3-256 (A5411)

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
CPU Time Jitter RNG		Server 15 SP6 on Intel® Xeon® Gold 5416S; SUSE Linux Enterprise Server 15 SP6 on IBM® TelumTM			

Table 12: Entropy Sources

The module employs a Deterministic Random Bit Generator (DRBG) based on [SP800- 90ARev1] for the generation of random value used in asymmetric keys, and for providing a RNG service to calling applications. The approved DRBG provided by the module is the CTR_DRBG with AES-256. The DRBG does not employ prediction resistance or a derivation function. The module uses an SP800-90B-compliant Entropy Source specified in the table above to seed the DRBG.

The DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy). Additionally, the DRBG is reseeded with a 256-bits long entropy input (corresponding to 256 bits of entropy).

2.9 Key Generation

In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys according to section 5.1 and 5.2 of [SP800-133rev2].

- For generating RSA and ECDSA keys, the module implements asymmetric cryptographic key generation (CKG) services compliant with [FIPS186-5].
- The public and private keys used in the EC Diffie-Hellman key agreement schemes are generated internally by the module using the ECDSA key generation method compliant with [FIPS186-5] and [SP800-56Arev3].
- The public and private keys used in the Diffie-Hellman key agreement scheme are also compliant with [SP800-56Arev3]. The module generates keys using safe primes defined in RFC7919 and RFC3526, as described in the next section.

Intermediate key generation values are not output from the module and are explicitly zeroized after processing the service.

Key Derivation

Additionally, the module supports the following key derivation methods:

- KDF TLS (CVL), compliant with SP800-135 Rev. 1: derivation of secret keys in the context of TLS 1.0/1.1,
- TLS v1.2 KDF RFC7627 (CVL), compliant with SP 800-135 Rev. 1: derivation of secret keys in the context of TLS 1.2,
- KDA HKDF SP 800-56Cr1, compliant with SP 800-56C Rev. 1: derivation of secret keys in the context of SP 800-56A Rev. 3 key agreement schemes,
- Password-based key derivation (PBKDF) compliant with option 1a of [SP800-132]. Keys derived from passwords or passphrases using this method can only be used in storage applications.

2.10 Key Establishment

Key Agreement

The module provides Diffie-Hellman and EC Diffie-Hellman shared secret computation compliant with SP800-56Arev3, in accordance with scenario 2 path (1) of IG D.F. The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS."

The EC Diffie-Hellman shared secret computation uses the Ephemeral Unified Model. The module supports EC Diffie-Hellman shared secret computation with P-256, P-384, and P-521 curves which have a security strength of 128, 192, and 256 bits.

The Diffie-Hellman shared secret computation uses the DH Ephemeral scheme. The module supports Diffie-Hellman shared secret computation with the MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, and ffdhe8192 groups which have a security strength of 112, 128, 152, 176, and 200 bits.

Additionally, the module provides Diffie-Hellman and EC Diffie-Hellman shared secret computation used as part of the TLS protocol key exchange in accordance with scenario 2 path (2) of IG D.F; that is, the shared secret computation (KAS-FFC-SSC and KAS-ECC-SSC) followed by key derivation using KDF TLS (CVL), TLS v1.2 KDF RFC7627 (CVL), or KDA HKDF SP 800-56Crev2. The Diffie-Hellman shared secret computation, EC Diffie-Hellman shared secret computation, KDF TLS (CVL), TLS v1.2 KDF RFC7627 (CVL), and KDA HKDF SP 800-56Crev2 have been CAVP tested.

2.11 Industry Protocols

The TLS protocol implementation provides both server and client sides. To operate in the approved mode, digital certificates used for server and client authentication shall comply with the restrictions of key size and message digest algorithms imposed by SP 800-131A Rev. 2.

No parts of the TLS protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	API input parameters, kernel I/O network or files on filesystem, TLS protocol input messages.
N/A	Data Output	API output parameters, kernel I/O network or files on filesystem, TLS protocol output messages.
N/A	Control Input	API function calls, API input parameters for control.
N/A	Status Output	API return codes, API output parameters for status output.

Table 13: Ports and Interfaces

All data output via data output interface is inhibited when the module is performing pre- operational self-test, conditional cryptographic algorithms self-tests, zeroization or when the module enters error state.

The module does not implement a control output interface.

The module does not output any control data to another cryptographic module.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not support authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 14: Roles

The module supports the Crypto Officer role only. This sole role is implicitly and always assumed by the operator of the module.

No support is provided for multiple concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Symmetric Encryption	Perform AES encryption	GNUTLS_FIPS140_OP_APPROVED	Key, Plaintext	Ciphertext	Symmetric Encryption with AES	Crypto Officer - AES key: W,E
Symmetric Decryption	Perform AES decryption	GNUTLS_FIPS140_OP_APPROVED	Key, Ciphertext	Plaintext	Symmetric Decryption with AES	Crypto Officer - AES key: W,E
Authenticated Encryption	Encrypt a plaintext	GNUTLS_FIPS140_OP_APPROVED	Key, Plaintext, IV	Ciphertext, MAC tag	Authenticated Encryption with AES	Crypto Officer - AES key: W,E
Authenticated Decryption	Decrypt a ciphertext	GNUTLS_FIPS140_OP_APPROVED	Key, Ciphertext, IV, MAC tag	Plaintext or fail	Authenticated Decryption with AES	Crypto Officer - AES key: W,E
Message Digest	Compute message digest	GNUTLS_FIPS140_OP_APPROVED	Message	Digest of the message	Message Digest with SHA	Crypto Officer
Random Number Generation	Generate random bitstrings	GNUTLS_FIPS140_OP_APPROVED	Number of bits	Random number	Random Number Generation with	Crypto Officer - Entropy Input: W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					CTR_DRBG	- DRBG seed: G,E - DRBG internal state (V value, key): G,W,E
Message Authentication Code (MAC) with HMAC	Compute HMAC	GNUTLS_FIPS140_OP_APPROVED	HMAC key, message	Message authentication code	Message Authentication Code (MAC) with HMAC	Crypto Officer - HMAC key: W,E
Message Authentication Code (MAC) with AES	Compute AES-base CMAC or GMAC	GNUTLS_FIPS140_OP_APPROVED	AES key, message	Message authentication code	Message Authentication Code (MAC) with AES	Crypto Officer - AES key: W,E
Shared Secret Computation with Diffie-Hellman	Compute a shared secret	GNUTLS_FIPS140_OP_APPROVED	Private key, public key from peer	Shared secret	Shared Secret Computation with Diffie-Hellman	Crypto Officer - Diffie-Hellman shared secret: G,R - Diffie-Hellman private key: W,E - Diffie-Hellman public key: W,E
Shared Secret Computation with EC Diffie-Hellman	Compute a shared secret	GNUTLS_FIPS140_OP_APPROVED	Private key, public key from peer	Shared secret	Shared Secret Computation with Diffie-Hellman	Crypto Officer - EC Diffie-Hellman shared secret: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- EC Diffie-Hellman private key: W,E - EC Diffie-Hellman public key: W,E
Digital Signature Generation with RSA	Generate RSA signature	GNUTLS_FIPS140_OP_APPROVED	Message, hash algorithm, private key	Digital signature	Digital Signature Generation with RSA	Crypto Officer - RSA private key: W,E
Digital Signature Generation with ECDSA	Generate ECDSA signature	GNUTLS_FIPS140_OP_APPROVED	Message, hash algorithm, private key	Digital signature	Digital Signature Generation with ECDSA	Crypto Officer - ECDSA private key: W,E
Digital Signature Verification with RSA	Verify RSA signature	GNUTLS_FIPS140_OP_APPROVED	Message, signature, hash algorithm, public key	Verification result	Digital Signature Verification with RSA	Crypto Officer - RSA public key: W,E
Digital Signature Verification with ECDSA	Verify ECDSA signature	GNUTLS_FIPS140_OP_APPROVED	Message, signature, hash algorithm, public key	Verification result	Digital Signature Verification with ECDSA	Crypto Officer - ECDSA public key: W,E
Public Key Verification with ECDSA	Verify ECDSA public key	GNUTLS_FIPS140_OP_APPROVED	Key	Return codes/log messages	Public Key Verification with ECDSA Public Key Verification with	Crypto Officer - ECDSA public key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ECDSA (Legacy)	
Key Pair Generation with RSA	Generate RSA key pairs	GNUTLS_FIPS140_OP_APPROVED	Key size	Key pair	Random Number Generation with CTR_DRBG Key Pair Generation with RSA	Crypto Officer - Module-generated RSA private key: G,R - Module-generated RSA public key: G,R - Intermediate key generation value: G,E,Z
Key Pair Generation with ECDSA	Generate ECDSA key pairs	GNUTLS_FIPS140_OP_APPROVED	Key size, enabled-curve	Key pair	Random Number Generation with CTR_DRBG Key Pair Generation with ECDSA	Crypto Officer - Module-generated ECDSA private key: G,R - Module-generated ECDSA public key: G,R - Module-generated EC Diffie-Hellman private key: G,R - Module-generated EC Diffie-Hellman public key: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Intermediate key generation value: G,E,Z
Key Pair Generation with Safe Primes	Generate DH key pairs	GNUTLS_FIPS140_OP_APPROVED	Key size	Key pair	Key Pair Generation with Safe Primes	Crypto Officer - Module-generated Diffie-Hellman private key: G,R - Module-generated Diffie-Hellman public key: G,R - Intermediate key generation value: G,E,Z
TLS Key Derivation	Perform key derivation using TLS KDF	GNUTLS_FIPS140_OP_APPROVED	TLS Pre-master Secret	TLS Derived Secret	Key Derivation with TLS 1.0, 1.1, 1.2 KDF	Crypto Officer - TLS Pre-master Secret: W,E - TLS Master Secret: G,E,Z - TLS Derived Secret: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
HKDF Key Derivation (derivation of HKDF Derived key)	Perform key derivation using HKDF	GNUTLS_FIPS140_OP_APPROVED	Shared Secret	HKDF Derived key	Key Derivation (as part of TLSv1.3) with KDA HKDF	Crypto Officer - Diffie-Hellman shared secret: W,E - EC Diffie-Hellman shared secret: W,E - HKDF Derived key: G,R
Key Derivation with PBKDF	Perform password-based key derivation	GNUTLS_FIPS140_OP_APPROVED	Password or passphrase	PBKDF Derived key	Key Derivation with PBKDF	Crypto Officer - PBKDF password or passphrase: W,E - PBKDF Derived key: G,R
Transport Layer Security (TLS) Network Protocol	Provide supported cipher suites (listed in Appendix A) in approved mode	GNUTLS_FIPS140_OP_APPROVED	Cipher-suites listed in Appendix A, Digital Certificate, Public and Private Keys, Application Data	Return codes and/or log messages, Application data	Symmetric Encryption with AES Symmetric Decryption with AES Authenticated Encryption with AES Authenticated Decryption with AES Authenticated Encryption in the	Crypto Officer - RSA public key: W,E - RSA private key: W,E - ECDSA public key: W,E - ECDSA private key: W,E - TLS Pre-master Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					context of TLS protocol Authenticated Decryption in the context of TLS protocol Message Digest with SHA Message Authentication Code (MAC) with HMAC Message Authentication Code (MAC) with AES Digital Signature Generation with RSA Digital Signature Verification with RSA Digital Signature Generation with ECDSA Digital Signature Verification with ECDSA Public Key Verification with	E,G - TLS Master Secret: E,G,Z - Module-generated Diffie-Hellman private key: E,G - Module-generated Diffie-Hellman public key: W,E,G,R - Module-generated EC Diffie-Hellman private key: E,G - Module-generated EC Diffie-Hellman public key: W,E,G,R - TLS Derived Secret: E,G - HKDF Derived key: E,G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ECDSA Public Key Verification with ECDSA (Legacy) TLS Handshake (KAS) Key Pair Generation with RSA Key Pair Generation with ECDSA Key Pair Generation with Safe Primes	
Self-tests	Perform self-tests	N/A	N/A	Result of self-test (pass/fail)	Symmetric Encryption with AES Symmetric Decryption with AES Authenticated Encryption with AES Authenticated Decryption with AES Authenticated Encryption in the context of TLS protocol Authenticated Decryption in the	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					context of TLS protocol Message Digest with SHA Random Number Generation with CTR_DRBG Message Authentication Code (MAC) with HMAC Message Authentication Code (MAC) with AES Digital Signature Generation with RSA Digital Signature Verification with RSA Digital Signature Generation with ECDSA Digital Signature Verification with ECDSA Public Key Verification with ECDSA	

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Public Key Verification with ECDSA (Legacy) Shared Secret Computation with EC Diffie-Hellman Shared Secret Computation with Diffie-Hellman Key Derivation with PBKDF Key Derivation with TLS 1.0, 1.1, 1.2 KDF Key Derivation (as part of TLSv1.3) with KDA HKDF TLS Handshake (KAS) Key Pair Generation with RSA Key Pair Generation with ECDSA Key Pair Generation	

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					with Safe Primes	
Show module name and version	Show module name and version	N/A	N/A	Name and version information	None	Crypto Officer
Show Status	Show module status	N/A	N/A	Return codes and/or log messages	None	Crypto Officer
Zeroization	Zeroize SSPs	N/A	Context containing SSPs	N/A	None	Crypto Officer - AES key: Z - HMAC key: Z - Module-generated RSA private key: Z - Module-generated RSA public key: Z - RSA private key: Z - RSA public key: Z - PBKDF password or passphrase: Z - PBKDF Derived key: Z - Module-generated ECDSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						private key: Z - Module-generated ECDSA public key: Z - ECDSA private key: Z - ECDSA public key: Z - Module-generated EC Diffie-Hellman private key: Z - Module-generated EC Diffie-Hellman public key: Z - EC Diffie-Hellman private key: Z - EC Diffie-Hellman public key: Z - Module-generated Diffie-Hellman private key: Z - Module-generated Diffie-Hellman

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						public key: Z - Diffie-Hellman private key: Z - Diffie-Hellman public key: Z - Diffie-Hellman shared secret: Z - EC Diffie-Hellman shared secret: Z - Entropy Input: Z - DRBG seed: Z - DRBG internal state (V value, key): Z - TLS Pre-master Secret: Z - HKDF Derived key: Z - TLS Master Secret: Z - TLS Derived Secret: Z

Table 15: Approved Services

The above table lists all approved services that can be used in the approved mode of operation.

For the above table, the convention below applies when specifying the access permissions (types) that the service has for each SSP.

- **Generate (G):** The module generates or derives the SSP.
- **Read (R):** The SSP is read from the module (e.g. the SSP is output).
- **Write (W):** The SSP is updated, imported, or written to the module.
- **Execute (E):** The module uses the SSP in performing a cryptographic operation.
- **Zeroize (Z):** The module zeroizes the SSP.
- **N/A:** The module does not access any SSP or key during its operation.

The service indicator is invoked by calling the function "gnutls_fips140_get_operation_state()" and it returns "GNUTLS_FIPS140_OP_APPROVED" or "GNUTLS_FIPS140_OP_NOT_APPROVED" depending on whether the API invoked corresponds to an approved or non-approved algorithm.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Symmetric key generation	Generate symmetric key other than AES and HMAC keys	DRBG when key length is less than 112 bits	CO
Symmetric encryption	Compute the cipher for encryption	Blowfish Camellia CAST ChaCha20 DES GOST RC2 RC4 Salsa20 Serpent Triple-DES Twofish	CO
Symmetric decryption	Compute the cipher for decryption	Blowfish Camellia CAST ChaCha20 DES GOST RC2 RC4 Salsa20 Serpent Triple-DES Twofish	CO

Name	Description	Algorithms	Role
Digital signature generation	Sign RSA, DSA, and ECDSA signatures	DSA ECDSA with curves not listed in Table "Approved Algorithms" or hash functions other than SHA2-224, SHA2-256, SHA2-384, SHA2-512 RSA (with keys smaller than 2048 bits and/or hash functions other than SHA2-224, SHA2-256, SHA2-384, SHA2-512)	CO
Digital signature verification	Verify RSA, DSA, and ECDSA signatures	DSA ECDSA with curves not listed in Table "Approved Algorithms" or hash functions other than SHA2-224, SHA2-256, SHA2-384, SHA2-512 RSA (with keys smaller than 2048 bits and/or hash functions other than SHA2-224, SHA2-256, SHA2-384, SHA2-512)	CO
Key generation	Generate RSA, DSA, and ECDSA key pairs	DSA ECDSA with curves not listed in Table "Approved Algorithms" RSA (with keys smaller than 2048 bits)	CO
Public key verification	Verify ECDSA public key	ECDSA with curves not listed in Table "Approved Algorithms"	CO
Message digest	Compute message digest	GOST MD2 MD4 MD5 RMD160 SM3 STREEBOG	CO
Message Authentication Code (MAC)	Compute HMAC	HMAC with keys smaller than 112-bit HMAC with GOST MD2 MD4 MD5 RMD160 STREEBOG UMAC	CO
Key encapsulation	Perform RSA key encapsulation	RSA (with any key sizes)	CO
Key unencapsulation	Perform RSA key unencapsulation	RSA (with any key sizes)	CO

Name	Description	Algorithms	Role
Shared Secret Computation with Diffie-Hellman	Perform DH key agreement	Diffie-Hellman with keys generated with domain parameters other than safe primes	CO
Shared Secret Computation with EC Diffie-Hellman	Perform ECDH key agreement	EC Diffie-Hellman with curves not listed in Table "Approved Algorithms"	CO
Key agreement	Perform DH (or ECDH) key agreement	Diffie-Hellman with keys generated with domain parameters other than safe primes EC Diffie-Hellman with curves not listed in Table "Approved Algorithms"	CO
Key Derivation with PBKDF	Perform password-based key derivation	PBKDF with non-approved message digest algorithms	CO
Transport Layer Security (TLS) Network Protocol	Provide non-supported cipher suites	Non-supported cipher suites (not listed in Appendix A)	CO
Random number generation	Generate random number	Yarrow	CO
Authenticated encryption	Perform authenticated encryption	ChaCha20 and Poly1305 AES-GCM (when not used in the context of the TLS protocol)	CO
Authenticated decryption	Perform authenticated decryption	ChaCha20 and Poly1305 AES-GCM (when not used in the context of the TLS protocol)	CO
Domain parameter generation	Generate domain parameter	DSA	CO

Table 16: Non-Approved Services

The table above lists the non-approved services in this module, the algorithms involved, the roles that can request the service, and the respective service indicator. In this table, CO specifies the Crypto Officer role.

4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

Each software component of the module has an associated HMAC-SHA2-256 integrity check value. The integrity of the module is verified by comparing the HMAC-SHA2-256 value calculated at run time for each software component of the module listed in section 2, with the HMAC value stored in each .hmac file corresponding to each software component, which was computed at build time. The HMAC key is embedded in the libgnutls shared library. If the integrity test fails the module enters the error state.

5.2 Initiate on Demand

The module provides the Self-Test service to perform self-tests on demand which includes the pre-operational test (i.e., integrity test) and the cryptographic algorithm self-tests (CASTs). The Self-tests service can be called on demand by invoking the gnutls_fips140_run_self_tests() function which will perform integrity tests and the cryptographic algorithms self-tests.

Additionally, the Self-test service can be invoked by powering-off and reloading the module. During the execution of the on-demand self-tests, services are not available, and no data output is possible.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The module operates in a modifiable operational environment per FIPS 140-3 level 1 specification: the module executes on a general-purpose operating system, which allows modification, loading, and execution of software that is not part of the validated module.

If properly installed, the operating system provides process isolation and memory protection mechanisms that ensure appropriate separation for memory access among the processes on the system. Each process has control over its own data and uncontrolled access to the data of other processes is prevented.

6.2 Configuration Settings and Restrictions

Instrumentation tools like the ptrace system call, gdb and strace, userspace live patching, as well as other tracing mechanisms offered by the Linux environment such as ftrace or systemtap, shall not be used in the operational environment. The use of any of these tools implies that the cryptographic module is running in a non-validated operational environment.

7 Physical Security

The module is comprised of software only and therefore this section is not applicable.

8 Non-Invasive Security

This module does not implement any non-invasive security mechanism and therefore this section is not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Temporary storage for SSPs used by the module as part of service execution. The module does not perform persistent storage of SSPs	Dynamic

Table 17: Storage Areas

The module does not perform persistent storage of SSPs. The SSPs are temporarily stored in the RAM in plaintext form. SSPs are provided to the module by the calling process and are destroyed when released by the appropriate zeroization function calls.

Symmetric keys, public and private keys are provided to the module by the calling application via API input parameters and are destroyed by the module when invoking the appropriate API function calls.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API input parameters (plaintext)	Calling application within TOEPP	Cryptographic module	Plaintext	Manual	Electronic	
API output parameters (plaintext)	Cryptographic module	Calling application within TOEPP	Plaintext	Manual	Electronic	

Table 18: SSP Input-Output Methods

SSPs are provided to the module via API input parameters in plaintext form and output via API output parameters in plaintext form within the physical perimeter of the operational environment. This is allowed by [FIPS140-3_IG] IG 9.5.A, according to the “CM Software to/from App via TOEPP Path” entry on the Key Establishment Table.

The module does not support entry or output of cryptographically protected SSPs.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroize Context	The memory occupied by SSPs is allocated by regular memory allocation	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable. The completion of the	By calling the appropriate zeroization functions: AES key: gnutls_cipher_deinit( ) AES key: gnutls_aead_cipher_ deinit() HMAC key: gnutls_hmac_deinit() RSA Public Key, RSA Private Key: gnutls_privkey_deinit ()

Zeroization Method	Description	Rationale	Operator Initiation
	operating system calls.	zeroization routine indicates that the zeroization procedure succeeded.	gnutls_x509_privkey _deinit() gnutls_rsa_params_d einit() ECDSA Public Key, ECDSA Private Key: gnutls_privkey_deinit () gnutls_x509_privkey _deinit() gnutls_rsa_params_d einit() Diffie-Hellman Public Key, Diffie-Hellman private key: gnutls_dh_params_d einit() TLS Pre-master Secret: gnutls_deinit() TLS Master Secret: gnutls_deinit() HKDF Derived key: gnutls_deinit() Diffie-Hellman Public Key, Diffie-Hellman private key: gnutls_pk_params_cl ear() EC Diffie-Hellman public key, EC Diffie-Hellman private key: gnutls_pk_params_cl ear() Diffie-Hellman Shared Secret: zeroize key() EC Diffie-Hellman Shared Secret: zeroize_key() All SSPs: gnutls_global_deinit()
Automatic	Automatically zeroized by the module when no longer needed	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable.	N/A
Reset	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed. Module power off indicates that the zeroization procedure succeeded.	Unloading and reloading the module

Table 19: SSP Zeroization Methods

All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	AES key used for encryption,	AES-XTS, AES-CCM, AES-GCM,	Symmetric key - CSP			Symmetric Encryption with AES

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	decryption, and computing MAC tags	AES-GMAC, AES-CMAC: 128, 256 bits; Other modes: 128, 192, 256 bits - AES-XTS, AES-CCM, AES-GCM, AES-GMAC, AES-CMAC: 128, 256 bits; Other modes: 128, 192, 256 bits				Symmetric Decryption with AES Authenticated Encryption with AES Authenticated Decryption with AES Message Authentication Code (MAC) with AES
HMAC key	HMAC key used for computing MAC tags	112 to 524288 bits - 112 to 256 bits	Symmetric key - CSP			Message Authentication Code (MAC) with HMAC
Module-generated RSA private key	RSA private key generated through asymmetric key generation	2048, 3072, 4096, 6144, 7680, 8192, 15360-bits - 112, 128, 149, 178, 192, 201, and 256 bits	Private key - CSP	Key Pair Generation with RSA		
Module-generated RSA public key	RSA public key generated through asymmetric key generation	2048, 3072, 4096, 6144, 7680, 8192, 15360-bits - 112, 128, 149, 178, 192, 201, and 256 bits	Public key - PSP	Key Pair Generation with RSA		
RSA private key	RSA private key used for digital	2048-16384 bits - 112-256 bits	Private key - CSP			Digital Signature

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	signature generation					Generation with RSA
RSA public key	RSA public key used for digital signature verification	2048-16384 bits - 112-256 bits	Public key - PSP			Digital Signature Verification with RSA
PBKDF password or passphrase	Password used to derive symmetric keys	14 characters minimum - 10^-14 minimum probability	Password - CSP			Key Derivation with PBKDF
PBKDF Derived key	Key derived from PBKDF password/passphrase during key derivation	128-256 bits - 128-256 bits	Derived key - CSP	Key Derivation with PBKDF		
Module-generated ECDSA private key	ECDSA private key generated through the asymmetric key generation	P-256, P-384, P-521 - 128, 192, 256 bits	Private key - CSP	Key Pair Generation with ECDSA		
Module-generated ECDSA public key	ECDSA private key generated through the asymmetric key generation	P-256, P-384, P-521 - 128, 192, 256 bits	Public key - PSP	Key Pair Generation with ECDSA		
ECDSA private key	ECDSA private key used for digital signature generation	P-256, P-384, P-521 - 128, 192, 256 bits	Private key - CSP			Digital Signature Generation with ECDSA
ECDSA public key	ECDSA public key used for	P-256, P-384, P-521 -	Public key - PSP			Public Key Verification with ECDSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	digital signature verification	128, 192, 256 bits				Public Key Verification with ECDSA (Legacy)
Module-generated EC Diffie-Hellman public key	EC Diffie-Hellman public key generated during asymmetric key generation	P-256, P-384, P-521 - 128, 192, 256 bits	Public key - PSP	Key Pair Generation with ECDSA		TLS Handshake (KAS)
Module-generated EC Diffie-Hellman private key	EC Diffie-Hellman private key generated during asymmetric key generation	P-256, P-384, P-521 - 128, 192, 256 bits	Private key - CSP	Key Pair Generation with ECDSA		TLS Handshake (KAS)
EC Diffie-Hellman public key	Public key used for Shared Secret Computation	P-256, P-384, P-521 - 128, 192, 256 bits	Public key - PSP			Shared Secret Computation with EC Diffie-Hellman
EC Diffie-Hellman private key	Private key used for Shared Secret Computation	P-256, P-384, P-521 - 128, 192, 256 bits	Private key - CSP			Shared Secret Computation with EC Diffie-Hellman
Module-generated Diffie-Hellman public key	Diffie-Hellman public key generated during Safe Primes Key Generation	2048, 3072, 4096, 6144, 8192 bits - 112, 128, 152, 176, 200 bits	Public key - PSP	Key Pair Generation with Safe Primes		TLS Handshake (KAS)
Module-generated Diffie-Hellman private key	Diffie-Hellman private key generated during Safe Primes Key Generation	2048, 3072, 4096, 6144, 8192 bits - 112, 128, 152, 176, 200 bits	Private key - CSP	Key Pair Generation with Safe Primes		TLS Handshake (KAS)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Diffie-Hellman public key	Public key used for Shared Secret Computation	2048, 3072, 4096, 6144, 8192 bits - 112, 128, 152, 176, 200 bits	Public key - PSP			Shared Secret Computation with Diffie-Hellman
Diffie-Hellman private key	Private key used for Shared Secret Computation	2048, 3072, 4096, 6144, 8192 bits - 112, 128, 152, 176, 200 bits	Private key - CSP			Shared Secret Computation with Diffie-Hellman
Diffie-Hellman shared secret	Shared secret generated by Diffie-Hellman	2048, 3072, 4096, 6144, 8192 bits - 112, 128, 152, 176, 200 bits	Shared Secret - CSP		Shared Secret Computation with Diffie-Hellman	
EC Diffie-Hellman shared secret	Shared secret generated by EC Diffie-Hellman	P-256, P-384, P-521 - 128, 192 256 bits	Shared Secret - CSP		Shared Secret Computation with EC Diffie-Hellman	
Entropy Input	Entropy input used to seed the DRBG	256-384 bits - 256-384 bits	Entropy Input - CSP			Random Number Generation with CTR_DRBG
DRBG seed	DRBG seed derived from entropy input	256-384 bits - 256-384 bits	Seed - CSP	Random Number Generation with CTR_DRBG		Random Number Generation with CTR_DRBG
DRBG internal state (V value, key)	Internal state of the CTR_DRBG (for IG D.L)	384 bits - 256 bits	Internal State - CSP	Random Number Generation with CTR_DRBG		Random Number Generation with CTR_DRBG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS Pre-master Secret	TLS Pre-master Secret used for deriving the TLS Master Secret	112 to 256 bits - 112 to 256 bits	Secret - CSP		Shared Secret Computation with EC Diffie-Hellman Shared Secret Computation with Diffie-Hellman	TLS Handshake (KAS)
TLS Master Secret	TLS Master Secret used for deriving the TLS Derived Secret	384 bits - 384 bits	Secret - CSP	Key Derivation with TLS 1.0, 1.1, 1.2 KDF		TLS Handshake (KAS)
TLS Derived Secret	Used as encryption key or MAC key	112-256 bits - 112-256 bits	Derived secret - CSP	Key Derivation with TLS 1.0, 1.1, 1.2 KDF		TLS Handshake (KAS)
HKDF Derived key	HKDF (used as part of TLS 1.3 protocol) derived key	128-256 bits - 128-256 bits	Derived secret - CSP	Key Derivation (as part of TLSv1.3) with KDA HKDF		TLS Handshake (KAS)
Intermediate key generation value	Temporary value generated during key generation services	256-15360 bits - 112-256 bits	Intermediate value - CSP	Key Pair Generation with RSA Key Pair Generation with ECDSA Key Pair Generation with Safe Primes		Key Pair Generation with RSA Key Pair Generation with ECDSA Key Pair Generation with Safe Primes

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	
HMAC key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	
Module-generated RSA private key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Module-generated RSA public key:Paired With Intermediate key generation value:Generated From
Module-generated RSA public key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Module-generated RSA private key:Paired With Intermediate key generation value:Generated From
RSA private key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	RSA public key:Paired With
RSA public key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	RSA private key:Paired With
PBKDF password or passphrase	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	PBKDF Derived key:Derived From
PBKDF Derived key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	PBKDF password or passphrase:Derived From
Module-generated ECDSA private key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Module-generated ECDSA public key:Paired With Intermediate key generation value:Generated From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Module-generated ECDSA public key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Module-generated ECDSA private key:Paired With Intermediate key generation value:Generated From
ECDSA private key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	ECDSA public key:Paired With
ECDSA public key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	ECDSA private key:Paired With
Module-generated EC Diffie-Hellman public key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Module-generated EC Diffie-Hellman private key:Paired With Intermediate key generation value:Generated From
Module-generated EC Diffie-Hellman private key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Module-generated EC Diffie-Hellman public key:Paired With Intermediate key generation value:Generated From
EC Diffie-Hellman public key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	EC Diffie-Hellman private key:Paired With
EC Diffie-Hellman private key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	EC Diffie-Hellman public key:Paired With
Module-generated Diffie-Hellman public key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Module-generated Diffie-Hellman private key:Paired With Intermediate key generation value:Generated From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Module-generated Diffie-Hellman private key	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Module-generated Diffie-Hellman public key:Paired With Intermediate key generation value:Generated From
Diffie-Hellman public key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Diffie-Hellman private key:Paired With
Diffie-Hellman private key	API input parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Diffie-Hellman public key:Paired With
Diffie-Hellman shared secret	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	Diffie-Hellman public key:Used With Diffie-Hellman private key:Used With
EC Diffie-Hellman shared secret	API output parameters (plaintext)	RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	EC Diffie-Hellman public key:Used With EC Diffie-Hellman private key:Used With
Entropy Input		RAM:Plaintext	From generation until DRBG Seed is created	Zeroize Context Automatic	DRBG seed:Derives
DRBG seed		RAM:Plaintext	While the DRBG is instantiated	Zeroize Context Automatic	Entropy Input:Derived From
DRBG internal state (V value, key)		RAM:Plaintext	While the module is operational	Zeroize Context Reset	DRBG seed:Used With
TLS Pre-master Secret		RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	TLS Master Secret:Derived From Module-generated Diffie-Hellman private key:Used With Module-generated Diffie-Hellman public key:Used With Module-generated EC

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Diffie-Hellman private key:Used With Module-generated EC Diffie-Hellman public key:Used With
TLS Master Secret		RAM:Plaintext	Until explicitly zeroized by operator	Zeroize Context Reset	TLS Pre-master Secret:Derived From TLS Derived Secret:Derived From
TLS Derived Secret	API output parameters (plaintext)	RAM:Plaintext	For the duration of the service	Zeroize Context Reset	TLS Master Secret:Derived From
HKDF Derived key	API output parameters (plaintext)	RAM:Plaintext	For the duration of the service	Zeroize Context Reset	Diffie-Hellman shared secret:Derived From EC Diffie-Hellman shared secret:Derived From
Intermediate key generation value		RAM:Plaintext	For the duration of the service	Automatic Zeroize Context Reset	Module-generated Diffie-Hellman private key:Generation Of Module-generated Diffie-Hellman public key:Generation Of Module-generated EC Diffie-Hellman private key:Generation Of Module-generated EC Diffie-Hellman public key:Generation Of Module-generated RSA private key:Generation Of Module-generated RSA public key:Generation Of

Table 21: SSP Table 2

9.5 Transitions

The SHA-1 algorithm as implemented by the module will be non-approved for all purposes, starting January 1, 2031.

10 Self-Tests

10.1 Pre-Operational Self-Tests

The module performs the following pre-operational tests: the integrity test of the shared libraries that comprise the module using HMAC-SHA2-256. The details of integrity test are provided in section 5.1.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A6363)	256-bit key	Integrity	SW/FW Integrity	Module becomes operational and services are available for use	MAC tag computation
HMAC-SHA2-256 (A6368)	256-bit key	Integrity	SW/FW Integrity	Module becomes operational and services are available for use	MAC tag computation
HMAC-SHA2-256 (A6372)	256-bit key	Integrity	SW/FW Integrity	Module becomes operational and services are available for use	MAC tag computation
HMAC-SHA2-256 (A6376)	256-bit key	Integrity	SW/FW Integrity	Module becomes operational and services are available for use	MAC tag computation

Table 22: Pre-Operational Self-Tests

The module performs the pre-operational self-test and CASTs automatically when the module is loaded into memory. Pre-operational self-test ensure that the module is not corrupted, and the CASTs ensure that the cryptographic algorithms work as expected. While the module is executing the self-tests, the module services are not available, and input and output are inhibited. The module is not available for use by the calling application until the pre-operational self-test and the CASTs are completed successfully. After the pre-operational test and the CASTs succeed, the module becomes operational. If any of the pre-operational test or any of the CASTs fail an error message is returned, and the module transitions to the error state. When the module is in the Error state, no data is output, and cryptographic operations are not allowed.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC - Encrypt (A6360)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CBC (A6361)	128, 256-bit key	KAT	CAST	Module becomes operational	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use		
AES-CBC (A6362)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CBC (A6363)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CBC (A6368)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CBC (A6372)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CBC (A6374)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CBC (A6375)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC - Decrypt (A6360)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-CBC - Decrypt (A6361)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-CBC - Decrypt (A6362)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-CBC - Decrypt (A6363)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-CBC - Decrypt (A6368)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-CBC - Decrypt (A6372)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-CBC - Decrypt (A6374)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC - Decrypt (A6375)	128, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-GCM - Encrypt (A6360)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-GCM - Encrypt (A6361)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-GCM - Encrypt (A6362)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-GCM - Encrypt (A6363)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-GCM - Encrypt (A6368)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-GCM - Encrypt (A6372)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Encrypt (A6374)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-GCM - Encrypt (A6375)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-GCM - Decrypt (A6360)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-GCM - Decrypt (A6361)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-GCM - Decrypt (A6362)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-GCM - Decrypt (A6363)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-GCM - Decrypt (A6368)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Decrypt (A6372)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-GCM - Decrypt (A6374)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-GCM - Decrypt (A6375)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-CFB8 - Encrypt (A6365)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CFB8 - Encrypt (A6366)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CFB8 - Encrypt (A6371)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-CFB8 - Decrypt (A6365)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CFB8 - Decrypt (A6366)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-CFB8 - Decrypt (A6371)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
AES-XTS Testing Revision 2.0 - Encrypt (A6369)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Module initialization
AES-XTS Testing Revision 2.0 - Decrypt (A6369)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Module initialization
SHA3-224 (A6364)	SHA3-224	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
SHA3-224 (A6370)	32-bit message	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
SHA3-256 (A6364)	32-bit message	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-256 (A6370)	32-bit message	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
SHA3-384 (A6364)	64-bit message	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
SHA3-384 (A6370)	64-bit message	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
SHA3-512 (A6364)	136-bit message	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
SHA3-512 (A6370)	136-bit message	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
HMAC-SHA-1 (A6363)	128-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A6368)	128-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 (A6372)	128-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A6376)	128-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A6363)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A6368)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A6372)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A6376)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A6363)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A6368)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A6372)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A6376)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A6363)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A6368)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A6372)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A6376)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A6363)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A6368)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A6372)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A6376)	160-bit key	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
AES-CMAC (A6360)	256-bit keys	KAT	CAST	Module becomes operational and services are available for use	MAC generation	Module initialization
AES-CMAC (A6363)	256-bit keys	KAT	CAST	Module becomes operational and services are available for use	MAC generation	Module initialization
AES-CMAC (A6368)	256-bit keys	KAT	CAST	Module becomes operational and services are available for use	MAC generation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CMAC (A6374)	256-bit keys	KAT	CAST	Module becomes operational and services are available for use	MAC generation	Module initialization
RSA SigGen (FIPS186-5) (A6368)	2048-bit key using SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Digital signature generation	Module initialization
RSA SigVer (FIPS186-5) (A6368)	2048-bit key using SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Digital signature verification	Module initialization
ECDSA SigGen (FIPS186-5) (A6368)	P-256 using SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Digital signature generation	Module initialization
ECDSA SigVer (FIPS186-5) (A6368)	P-256 using SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Digital signature verification	Module initialization
Counter DRBG (A6368)	256-bit keys without DF, without PR	KAT	CAST	Module becomes operational and services are available for use	KAT CTR_DRBG with AES with 256-bit keys without DF, without PR	Test runs at power-on before the integrity test (instantiate, generate and reseed functions)
Counter DRBG - Health Tests (A6368)	Health tests	Health tests according to section 11.3 of [SP800-90Ar1]	CAST	Module becomes operational and services are available for use	Health tests for Instantiate, Generate, and Reseed	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-FFC-SSC Sp800-56Ar3 (A6368)	ffdhe3072	KAT	CAST	Module becomes operational and services are available for use	Primitive "Z" Computation	Module initialization
KAS-ECC-SSC Sp800-56Ar3 (A6368)	P-256	KAT	CAST	Module becomes operational and services are available for use	Primitive "Z" Computation	Module initialization
TLS v1.2 KDF RFC7627 (A6368)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Industry-based TLS v1.2 KDF key derivation	Module initialization
KDF TLS (A6368)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	TLS KDF key derivation	Module initialization
PBKDF (A6368)	SHA-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational and services are available for use	Key Derivation with PBKDF	Module initialization
KDA HKDF Sp800-56Cr1 (A6367)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Key Derivation (as part of TLSv1.3) with KDA HKDF	Module initialization
ECDSA KeyGen (FIPS186-5) (A6368)	SHA-256 with the respective curve	PCT	PCT	Successful key pair generation	Signature generation and verification	Key Pair Generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA KeyGen (FIPS186-5) (A6368)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation and verification	Key Pair Generation
Safe Primes Key Generation (A6368)	N/A	PCT	PCT	Successful key pair generation	PCT according to section 5.6.2.1.4 of [SP800-56Arev3]	Key Pair Generation

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6363)	Integrity	SW/FW Integrity	On demand	Manual
HMAC-SHA2-256 (A6368)	Integrity	SW/FW Integrity	On demand	Manual
HMAC-SHA2-256 (A6372)	Integrity	SW/FW Integrity	On demand	Manual
HMAC-SHA2-256 (A6376)	Integrity	SW/FW Integrity	On demand	Manual

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC - Encrypt (A6360)	KAT	CAST	On demand	Manually
AES-CBC (A6361)	KAT	CAST	On demand	Manually
AES-CBC (A6362)	KAT	CAST	On demand	Manually
AES-CBC (A6363)	KAT	CAST	On demand	Manually
AES-CBC (A6368)	KAT	CAST	On demand	Manually
AES-CBC (A6372)	KAT	CAST	On demand	Manually
AES-CBC (A6374)	KAT	CAST	On demand	Manually
AES-CBC (A6375)	KAT	CAST	On demand	Manually
AES-CBC - Decrypt (A6360)	KAT	CAST	On demand	Manually
AES-CBC - Decrypt (A6361)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC - Decrypt (A6362)	KAT	CAST	On demand	Manually
AES-CBC - Decrypt (A6363)	KAT	CAST	On demand	Manually
AES-CBC - Decrypt (A6368)	KAT	CAST	On demand	Manually
AES-CBC - Decrypt (A6372)	KAT	CAST	On demand	Manually
AES-CBC - Decrypt (A6374)	KAT	CAST	On demand	Manually
AES-CBC - Decrypt (A6375)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A6360)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A6361)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A6362)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A6363)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A6368)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A6372)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A6374)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A6375)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A6360)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A6361)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A6362)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A6363)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM - Decrypt (A6368)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A6372)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A6374)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A6375)	KAT	CAST	On demand	Manually
AES-CFB8 - Encrypt (A6365)	KAT	CAST	On demand	Manually
AES-CFB8 - Encrypt (A6366)	KAT	CAST	On demand	Manually
AES-CFB8 - Encrypt (A6371)	KAT	CAST	On demand	Manually
AES-CFB8 - Decrypt (A6365)	KAT	CAST	On demand	Manually
AES-CFB8 - Decrypt (A6366)	KAT	CAST	On demand	Manually
AES-CFB8 - Decrypt (A6371)	KAT	CAST	On demand	Manually
AES-XTS Testing Revision 2.0 - Encrypt (A6369)	KAT	CAST	On demand	Manually
AES-XTS Testing Revision 2.0 - Decrypt (A6369)	KAT	CAST	On demand	Manually
SHA3-224 (A6364)	KAT	CAST	On demand	Manually
SHA3-224 (A6370)	KAT	CAST	On demand	Manually
SHA3-256 (A6364)	KAT	CAST	On demand	Manually
SHA3-256 (A6370)	KAT	CAST	On demand	Manually
SHA3-384 (A6364)	KAT	CAST	On demand	Manually
SHA3-384 (A6370)	KAT	CAST	On demand	Manually
SHA3-512 (A6364)	KAT	CAST	On demand	Manually
SHA3-512 (A6370)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6363)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A6368)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6372)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6376)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6363)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6368)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6372)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6376)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6363)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6368)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6372)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6376)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6363)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6368)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6372)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6376)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6363)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6368)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6372)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-512 (A6376)	KAT	CAST	On demand	Manually
AES-CMAC (A6360)	KAT	CAST	On demand	Manually
AES-CMAC (A6363)	KAT	CAST	On demand	Manually
AES-CMAC (A6368)	KAT	CAST	On demand	Manually
AES-CMAC (A6374)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6368)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6368)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6368)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6368)	KAT	CAST	On demand	Manually
Counter DRBG (A6368)	KAT	CAST	On demand	Manually
Counter DRBG - Health Tests (A6368)	Health tests according to section 11.3 of [SP800-90Ar1]	CAST	On demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A6368)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6368)	KAT	CAST	On demand	Manually
TLS v1.2 KDF RFC7627 (A6368)	KAT	CAST	On demand	Manually
KDF TLS (A6368)	KAT	CAST	On demand	Manually
PBKDF (A6368)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDA HKDF Sp800-56Cr1 (A6367)	KAT	CAST	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6368)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6368)	PCT	PCT	On demand	Manually
Safe Primes Key Generation (A6368)	PCT	PCT	On demand	Manually

Table 25: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	The module stops functioning and ends the application process	When the integrity test or KAT fail; When the KAT of DRBG fails during CASTs or when an error is returned from the Userspace Standalone Jitter RNG within the OE; When the newly generated RSA, ECDSA, Diffie-Hellman or EC Diffie-Hellman key pair fails the PCT; When the module is in error state and caller requests cryptographic operations	The module must be restarted and perform the pre-operational self-test and the CASTs to recover from these errors.	GNUTLS_E_SELF_TEST_ERROR (-400); GNUTLS_E_RANDOM_FAILED (-206); GNUTLS_E_PK_GENERATION_ERROR (-403); GNUTLS_E_LIB_IN_ERROR_STATE (-402)

Table 26: Error States

When the module fails any pre-operational self-test or conditional test, the module will return an error code to indicate the error and enters error state. Any further cryptographic operations and the data output via the data output interface are inhibited. The calling application can obtain the module state by calling the gnutls_fips140_get_operation_state() API function. The function returns GNUTLS_FIPS140_OP_ERROR if the module is in the Error state.

Self-test errors transition the module into an error state that keeps the module operational but prevents any cryptographic related operations. The module must be restarted and perform the pre-operational self-test and the CASTs to recover from these errors. If failures persist, the module must be re-installed.

10.5 Operator Initiation of Self-Tests

The operator can initiate the pre-operational integrity self-test and cryptographic algorithm self-tests by calling the Self-Test service (via the gnutls_fips140_run_self_tests() function) or by powering-off and reloading the module. The PCTs can be invoked on demand by requesting the Key Pair Generation service. During the execution of the pre-operational integrity self-test and cryptographic algorithm self-tests, services are not available, and no data output is possible.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Configuration of the Operating Environment

Before the SUSE Linux Enterprise GnuTLS Cryptographic Module RPM packages are installed, the SUSE Linux Enterprise SP6 system must operate in the FIPS validated configuration. This can be achieved by:

- Adding the fips=1 option to the kernel command line during the system installation. During the software selection stage, do not install any third-party software.
- Switching the system into the FIPS validated configuration after the installation. Execute the fips-mode-setup --enable command. Restart the system.

In both cases, the Crypto Officer must verify the system operates in the FIPS validated configuration by executing the fips-mode-setup --check command, which should output "FIPS mode is enabled."

If the module is not installed, initialized, and configured according to this section, the module is in a non-compliant state. If the module is in a non-compliant state, it can be placed into the compliant state by un-initializing and uninstalling the module and then installing, initializing, and configuring the module according to this section.

11.1.2 Delivery of the module

On the SuperMicro SuperChassis 825BTQC- R1K23LPB and Motherboard H12DSi-NT6 hardware platform with the AMD EPYC™ 7343 processor or the ASUS RS700-E11-RS4U hardware platform with the Intel® Xeon® Gold 5416S processor, the module is delivered through the following RPM packages:

- libgnutls30-3.8.3-150600.4.6.2.x86_64
- libnettle8-3.9.1-150600.3.2.1.x86_64
- libhogweed6-3.9.1-150600.3.2.1.x86_64
- libgmp10-6.1.2-4.9.1.x86_64

On the GIGABYTE R152-P30 hardware platform with the Ampere® Altra® Q80- 30 processor, the module is delivered through the following RPM packages:

- libgnutls30-3.8.3-150600.4.6.2.aarch64
- libnettle8-3.9.1-150600.3.2.1.aarch64
- libhogweed6-3.9.1-150600.3.2.1.aarch64
- libgmp10-6.1.2-4.9.1.aarch64

On the IBM z16 A01 hardware platform with the IBM® Telum™ processor, the module is delivered through the following RPM packages:

- libgnutls30-3.8.3-150600.4.6.2.s390x
- libnettle8-3.9.1-150600.3.2.1.s390x
- libhogweed6-3.9.1-150600.3.2.1.s390x
- libgmp10-6.1.2-4.9.1.s390x

11.2 Administrator Guidance

The binaries of the module are contained in the RPM packages for delivery, listed in section 11.1.2. The Crypto Officer shall follow section 11 to configure the operational environment and install the module to be operated as a FIPS 140-3 validated module.

The "Show module name and version" service returns the value “GnuTLS version 3.8.3-150600.4.6.2”, which matches the version included in the RPM package filenames, and map to version 1.2 of the cryptographic module.

11.3 Non-Administrator Guidance

The approved security functions are listed in section 2.6 of this security policy.

The logical interfaces available to the users of the cryptographic module are listed in section 3.1.

For the secure operation of the module, the operator must follow the instructions in section 11.1 of this security policy.

11.4 End of Life

For secure sanitization of the cryptographic module, the module needs first to be powered off, which will zeroize all keys and CSPs in volatile memory. Then, for actual deprecation, the module shall be upgraded to a newer version that is FIPS 140-3 validated.

The module does not possess persistent storage of SSPs, so further sanitization steps are not needed.

12 Mitigation of Other Attacks

The module does not offer mitigation of other attacks.

Appendix A. TLS Cipher Suites

The module supports the following cipher suites for the TLS protocol version 1.0, 1.1, 1.2 and 1.3, compliant with section 3.3.1 of [SP800-52rev2]. Each cipher suite defines the key exchange algorithm, the bulk encryption algorithm (including the symmetric key size) and the MAC algorithm.

Cipher Suite	ID	Reference
TLS_DH_RSA_WITH_AES_128_CBC_SHA	{ 0x00, 0x31 }	RFC3268
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	{ 0x00, 0x33 }	RFC3268
TLS_DH_RSA_WITH_AES_256_CBC_SHA	{ 0x00, 0x37 }	RFC3268
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	{ 0x00, 0x39 }	RFC3268
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	{ 0x00,0x3F }	RFC5246
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	{ 0x00,0x67 }	RFC5246
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	{ 0x00,0x69 }	RFC5246
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	{ 0x00,0x6B }	RFC5246
TLS_PSK_WITH_AES_128_CBC_SHA	{ 0x00, 0x8C }	RFC4279
TLS_PSK_WITH_AES_256_CBC_SHA	{ 0x00, 0x8D }	RFC4279
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	{ 0x00, 0x9E }	RFC5288
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	{ 0x00, 0x9F }	RFC5288
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	{ 0x00, 0xA0 }	RFC5288
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	{ 0x00, 0xA1 }	RFC5288
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	{ 0xC0, 0x04 }	RFC4492
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	{ 0xC0, 0x05 }	RFC4492
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	{ 0xC0, 0x09 }	RFC4492
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	{ 0xC0, 0x0A }	RFC4492
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	{ 0xC0, 0x0E }	RFC4492
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	{ 0xC0, 0x0F }	RFC4492
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	{ 0xC0, 0x13 }	RFC4492
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	{ 0xC0, 0x14 }	RFC4492
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	{ 0xC0, 0x23 }	RFC5289
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	{ 0xC0, 0x24 }	RFC5289
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	{ 0xC0, 0x25 }	RFC5289
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	{ 0xC0, 0x26 }	RFC5289
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	{ 0xC0, 0x27 }	RFC5289
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	{ 0xC0, 0x28 }	RFC5289

Cipher Suite	ID	Reference
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	{ 0xC0, 0x29 }	RFC5289
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	{ 0xC0, 0x2A }	RFC5289
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	{ 0xC0, 0x2B }	RFC5289
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	{ 0xC0, 0x2C }	RFC5289
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	{ 0xC0, 0x2D }	RFC5289
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	{ 0xC0, 0x2E }	RFC5289
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	{ 0xC0, 0x2F }	RFC5289
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	{ 0xC0, 0x30 }	RFC5289
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	{ 0xC0, 0x31 }	RFC5289
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	{ 0xC0, 0x32 }	RFC5289
TLS_DHE_RSA_WITH_AES_128_CCM	{ 0xC0, 0x9E }	RFC6655
TLS_DHE_RSA_WITH_AES_256_CCM	{ 0xC0, 0x9F }	RFC6655
TLS_DHE_RSA_WITH_AES_128_CCM_8	{ 0xC0, 0xA2 }	RFC6655
TLS_DHE_RSA_WITH_AES_256_CCM_8	{ 0xC0, 0xA3 }	RFC6655
TLS_AES_128_GCM_SHA256	{ 0x13, 0x01 }	RFC8446
TLS_AES_256_GCM_SHA384	{ 0x13, 0x02 }	RFC8446
TLS_AES_128_CCM_SHA256	{ 0x13, 0x04 }	RFC8446
TLS_AES_128_CCM_8_SHA256	{ 0x13, 0x05 }	RFC8446

Appendix B. Glossary and abbreviations

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CPACF	CP Assist for Cryptographic Functions
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DF	Derivation Function
DSA	Digital Signature Algorithm
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
GMAC	Galois Counter Mode Message Authentication Code
HMAC	Hash Message Authentication Code
KAS	Key Agreement Scheme
KAT	Known Answer Test
KW	AES Key Wrap
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
PAA	Processor Algorithm Acceleration
PAI	Processor Algorithm Implementation
PBKDF2	Password-based Key Derivation Function v2

PKCS	Public-Key Cryptography Standards
PCT	Pairwise Consistency Test
PR	Prediction Resistance
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
AES	Advanced Encryption Standard
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CKG	Cryptographic Key Generation
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
HKDF	HMAC-based Key Derivation Function
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange
KAS	Key Agreement Scheme
KAT	Known Answer Test
KTS	Key Transport Scheme
KW	Key Wrap

MAC	Message Authentication Code
NIST	National Institute of Science and Technology
PAA	Processor Algorithm Acceleration
PAI	Processor Algorithm Implementation
PCT	Pair-wise Consistency Test
PBKDF2	Password-based Key Derivation Function v2
PKCS	Public-Key Cryptography Standards
PSS	Probabilistic Signature Scheme
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSP	Sensitive Security Parameter
TLS	Transport Layer Security

Appendix C. References

FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
FIPS 140-3 IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** April, 18 2025 https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips 140-3/FIPS 140-3 IG.pdf
FIPS 140-3 Management Manual	**FIPS 140-3 Cryptographic Module Validation Program Management Manual** December 2024 https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips 140-3/FIPS-140-3-CMVP Management Manual.pdf
FIPS 180-4	**Secure Hash Standard (SHS)** August 2015 https://doi.org/10.6028/NIST.FIPS.180-4
FIPS 186-4	**Digital Signature Standard (DSS)** July 2013 https://doi.org/10.6028/NIST.FIPS.186-4
FIPS 186-5	**Digital Signature Standard (DSS)** February 2023 https://doi.org/10.6028/NIST.FIPS.186-5
FIPS 197	**Advanced Encryption Standard** May 2023 https://doi.org/10.6028/NIST.FIPS.197-upd1
FIPS 198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 https://doi.org/10.6028/NIST.FIPS.198-1
FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://doi.org/10.6028/NIST.FIPS.202
PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2** November 2016 https://www.rfc-editor.org/rfc/rfc8017.txt

RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) May 2003 https://www.ietf.org/rfc/rfc3526.txt
RFC 5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS August 2008 https://www.ietf.org/rfc/rfc5288.txt
RFC 7919	Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS) August 2016 https://www.ietf.org/rfc/rfc7919.txt
RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3 August 2018 https://www.ietf.org/rfc/rfc8446.txt
RFC 7627	Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension) September 2015 https://www.ietf.org/rfc/rfc7627.txt
SP 800-38A	Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001 https://doi.org/10.6028/NIST.SP.800-38A
SP 800-38A Addendum	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode October 2010 https://doi.org/10.6028/NIST.SP.800-38A-Add
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005 https://doi.org/10.6028/NIST.SP.800-38B
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC November 2007 https://doi.org/10.6028/NIST.SP.800-38A
SP 800-52 Rev. 2	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations August 2019 https://doi.org/10.6028/NIST.SP.800-52r2

SP 800-56A Rev. 3	**Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** April 2018 https://doi.org/10.6028/NIST.SP.800-56Ar3
SP 800-56C Rev. 2	**Recommendation for Key-Derivation Methods in Key-Establishment Schemes** August 2020 https://doi.org/10.6028/NIST.SP.800-56Cr2
SP 800-90A Rev. 1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 https://doi.org/10.6028/NIST.SP.800-90Ar1
SP 800-90B	**Recommendation for the Entropy Sources Used for Random Bit Generation** January 2018 https://doi.org/10.6028/NIST.SP.800-90B
SP 800-132	**Recommendation for Password-Based Key Derivation - Part 1: Storage Applications** December 2010 https://doi.org/10.6028/NIST.SP.800-132
SP 800-133 Rev. 2	**Recommendation for Cryptographic Key Generation** June 2020 https://doi.org/10.6028/NIST.SP.800-133r2
SP 800-135 Rev. 1	**Recommendation for Existing Application-Specific Key Derivation Functions** December 2011 https://doi.org/10.6028/NIST.SP.800-135r1