SUSE, LLC

SUSE Linux Enterprise OpenSSL Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Version 1.4

Last update: 2026-07-15

Prepared by:

atsec information security corporation

4516 Seton Center Parkway, Suite 250

Austin, TX 78759

www.atsec.com

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 Table of Contents

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Tables

List of Figures

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 4.4 of the SUSE Linux Enterprise OpenSSL 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 a Security Level 1 software module. It has a one-to-one mapping to SP 800-140B starting with section B.2.1 named "General" that maps to section 1 in this document and ending with section B.2.12 named "Mitigation of other attacks" that maps to section 12 in this document.

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	1
	Overall Level	1

Table 1: Security Levels

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The SUSE Linux Enterprise OpenSSL Cryptographic Module (hereafter referred to as "the module") is a software library that provides a C language application program interface (API) for use by other applications that require cryptographic functionality. The module operates on a general-purpose computer.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The software block diagram below shows the cryptographic boundary of the module, and its interfaces with the operational environment.

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.

Figure 1 shows a block diagram that represents the design of the module when the module is operational and providing services to other user space applications. In this diagram, the physical perimeter of the operational environment is the general-purpose computer on which the module is installed. The cryptographic boundary is represented by the libssl and libcrypto shared libraries and their respective integrity check files.

The "Data/Control Input" and "Data/Status Output" arrows indicate the flow of data between the cryptographic module and its operator application, through the logical interfaces defined in Section 3.

Other components are only included in the diagram for informational purposes. They are not included in the cryptographic boundary (and therefore not part of the module's validation). For example, the kernel is responsible for managing system calls issued by the module itself, as well as other applications using the module for cryptographic services.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

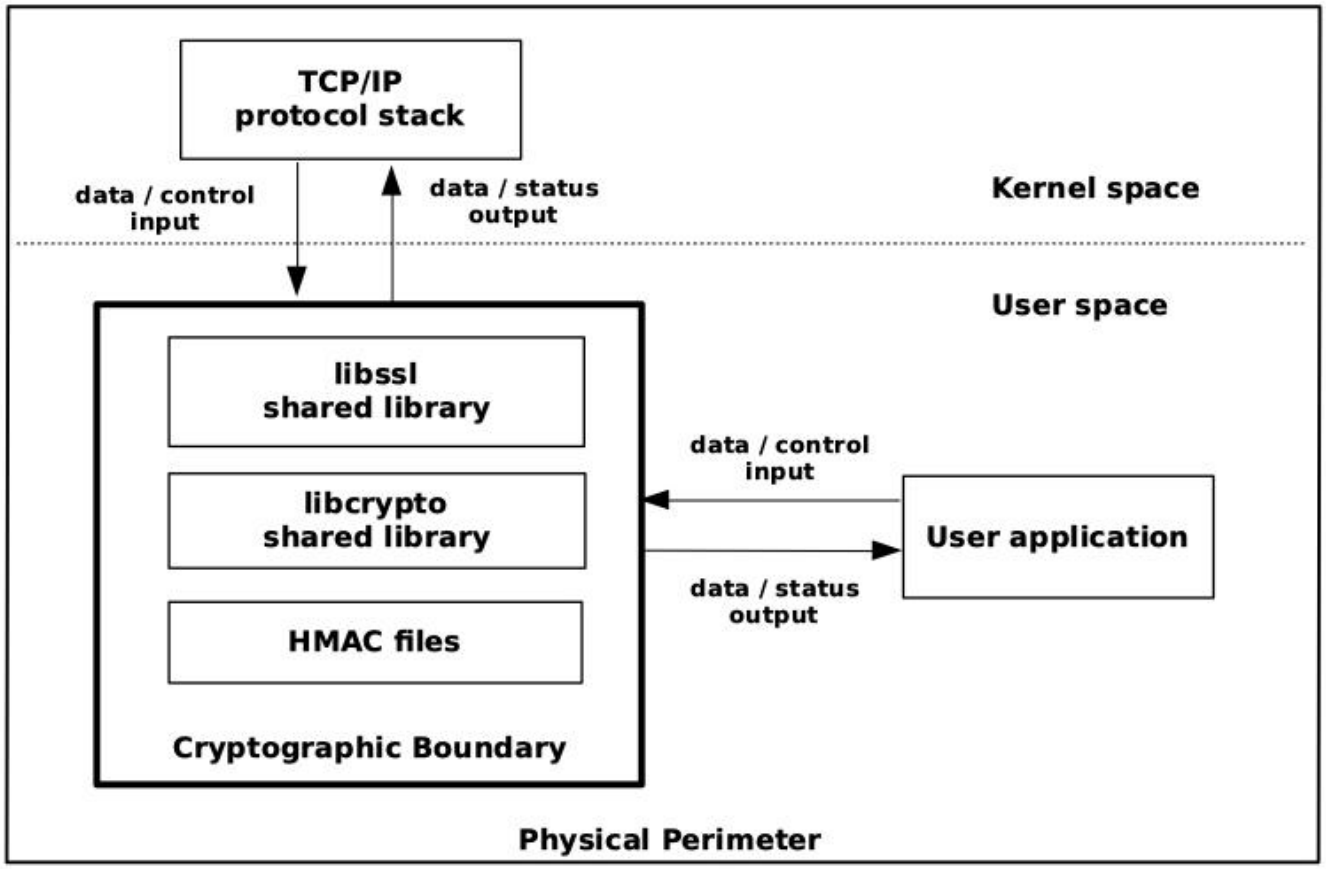

Figure 1 - Cryptographic boundary

2.2 Tested and Vendor Affirmed Module Version and Identification

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
libcrypto.so.1.1, libssl.so.1.1, .libcrypto.so.1.1.hmac, and .libssl.so.1.1.hmac on SUSE Linux Enterprise Server 15 SP4	4.4	N/A	HMAC-SHA2-256

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Package or File Name	Software/ Firmware Version	Features	Integrity Test
and Intel® Xeon® Silver 4215R or AMD EPYC (TM) 7371			
libcrypto.so.1.1 (32-bit), libssl.so.1.1 (32-bit), .libcrypto.so.1.1.hmac, and .libssl.so.1.1.hmac on SUSE Linux Enterprise Server 15 SP4 and Intel® Xeon® Silver 4215R	4.4	N/A	HMAC-SHA2-256
libcrypto.so.1.1, libssl.so.1.1, .libcrypto.so.1.1.hmac, and .libssl.so.1.1.hmac on SUSE Linux Enterprise Server 15 SP4 and ARM Ampere® Altra® Q80-30	4.4	N/A	HMAC-SHA2-256
libcrypto.so.1.1, libssl.so.1.1, .libcrypto.so.1.1.hmac, and .libssl.so.1.1.hmac on SUSE Linux Enterprise Server 15 SP4 and IBM z15	4.4	N/A	HMAC-SHA2-256
libcrypto.so.1.1, libssl.so.1.1, .libcrypto.so.1.1.hmac, and .libssl.so.1.1.hmac on SUSE Linux Enterprise Server 15 SP4 on PowerVM (VIOS 3.1.4.00) and IBM Power10	4.4	N/A	HMAC-SHA2-256

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

The above table lists the software components of the cryptographic module, which defines its cryptographic boundary.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
SUSE Linux Enterprise Server 15 SP4	Supermicro Super Server SYS-6019P-WTR	Intel® Xeon® Silver 4215R	Yes	N/A	4.4
SUSE Linux Enterprise Server 15 SP4	GIGABYTE R181-Z90-00	AMD EPYC (TM) 7371	Yes	N/A	4.4
SUSE Linux Enterprise Server 15 SP4	GIGABYTE G242-P32-QZ	ARM Ampere® Altra® Q80-30	Yes	N/A	4.4
SUSE Linux Enterprise Server 15 SP4	IBM z/15	IBM z15	Yes	N/A	4.4
SUSE Linux Enterprise Server 15 SP4	IBM Power E1080 (9080-HEX)	IBM Power10	Yes	PowerVM (VIOS 3.1.4.00)	4.4
SUSE Linux Enterprise Server 15 SP4	Supermicro Super Server SYS-6019P-WTR	Intel® Xeon® Silver 4215R	No	N/A	4.4
SUSE Linux Enterprise Server 15 SP4	GIGABYTE R181-Z90-00	AMD EPYC (TM) 7371	No	N/A	4.4
SUSE Linux Enterprise Server 15 SP4	GIGABYTE G242-P32-QZ	ARM Ampere® Altra® Q80-30	No	N/A	4.4
SUSE Linux Enterprise Server 15 SP4	IBM z/15	IBM z15	No	N/A	4.4
SUSE Linux Enterprise Server 15 SP4	IBM Power E1080 (9080-HEX)	IBM Power10	No	PowerVM (VIOS 3.1.4.00)	4.4

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

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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

Operating System	Hardware Platform
SUSE Linux Enterprise Server 15SP4	IBM LinuxONE III LT1 [IBM z15]
SUSE Linux Enterprise Micro 5.3	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Micro 5.3	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]
SUSE Linux Enterprise Micro 5.3	GIGABYTE G242-P32-QZ [ARM Ampere® Altra® Q80-30]
SUSE Linux Enterprise Micro 5.3	IBM z/15 [IBM z15]
SUSE Linux Enterprise Micro 5.3	IBM LinuxONE III LT1 [IBM z15]
SUSE Linux Enterprise Server for SAP 15SP4	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Server for SAP 15SP4	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]
SUSE Linux Enterprise Server for SAP 15SP4 on PowerVM (VIOS 3.1.4.00)	IBM Power E1080 (9080-HEX) [IBM Power10]
SUSE Linux Enterprise Base Container Image 15SP4	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Base Container Image 15SP4	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]
SUSE Linux Enterprise Base Container Image 15SP4	GIGABYTE G242-P32-QZ [ARM Ampere® Altra® Q80-30]
SUSE Linux Enterprise Base Container Image 15SP4	IBM z/15 [IBM z15]
SUSE Linux Enterprise Base Container Image 15SP4	IBM LinuxONE III LT1 [IBM z15]
SUSE Linux Enterprise Base Container Image 15SP4 on PowerVM (VIOS 3.1.4.00)	IBM Power E1080 (9080-HEX) [IBM Power10]
SUSE Linux Enterprise Desktop 15SP4	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Operating System	Hardware Platform
SUSE Linux Enterprise Desktop 15SP4	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]
SUSE Linux Enterprise Real Time 15SP4	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Real Time 15SP4	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]
SUSE Linux Enterprise Server 15SP4 (32-bit)	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]
SUSE Linux Enterprise Server for SAP 15SP4 (32-bit)	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Server for SAP 15SP4 (32-bit)	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]
SUSE Linux Enterprise Desktop 15SP4 (32-bit)	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Desktop 15SP4 (32-bit)	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]
SUSE Linux Enterprise Real Time 15SP4 (32-bit)	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Real Time 15SP4 (32-bit)	GIGABYTE R181-Z90-00 [AMD EPYC (TM) 7371]

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

The SUSE Linux Enterprise Server operating system is used as the basis of other products. Compliance is maintained for SUSE products whenever the binary is found unchanged per the vendor affirmation from SUSE based on the allowance FIPS 140-3 Management Manual, 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 excluded from the requirements of the FIPS 140-3 standard.

2.4 Modes of Operation

Modes List and Description:

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Mode Name	Description	Type	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service
Non-approved mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Equivalent to the indicator of the requested service

Table 5: Modes List and Description

After passing all pre-operational self-tests and cryptographic algorithm self-tests executed on start-up, the module automatically transitions to the approved mode. No operator intervention is required to reach this point. The module operates in the approved mode of operation by default and can only transition into the non-approved mode by calling one of the non-approved services listed in the Non-Approved Services table of the Security Policy.

In the operational state, the module accepts service requests from calling applications through its logical interfaces. At any point in the operational state, a calling application can end its process, causing the module to end its operation.

Mode Change Instructions and Status:

The module automatically switches between the approved and non-approved modes depending on the services requested by the operator. The status indicator of the mode of operation is equivalent to the indicator of the service that was requested.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 256 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CFB1	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
AES-CFB128	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 8-524288 Increment 8	SP 800-38B
AES-CTR	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-ECB	A3136, A3137, A3138, A3140, A3141, A3142, A3143, A3149, A3150, A3154, A3157, A3158, A3160, A3162, A3163, A3165, A3166, A3167, A3169, A3170, A3171, A3172	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A3151, A3152, A3153, A3155, A3159, A3176, A3177, A3178, A3179, A3180, A3181, A3182, A3183, A3184, A3190, A3194, A3195, A3196, A3197, A3198, A3199, A3200, A3201, A3204, A3205, A3206	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96, IV Length: 96, 128 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 128, 256, 120, 0, AAD Length: 64, 96	SP 800-38D
AES-KW	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256	SP 800-38F

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Payload Length - Payload Length: 128-4096 Increment 128	
AES-KWP	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 8-4096 Increment 8	SP 800-38F
AES-OFB	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
Counter DRBG	A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167	Prediction Resistance - No, Yes Supports Reseed - No Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No, Yes Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 128, Entropy Input: 192, Entropy Input: 256, Entropy Input: 320, Entropy Input: 384 Nonce - Nonce: 128, Nonce: 64, Nonce: 96 Personalization String Length - Personalization String Length: 0 Returned Bits - 1024, 512	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigGen (FIPS186-4)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	MAC - MAC: 160 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3147, A3156, A3161, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A3144, A3145, A3146, A3148, A3173, A3174, A3175	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A3144, A3145, A3146, A3148, A3173, A3174, A3175	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-384	A3144, A3145, A3146, A3148, A3173, A3174, A3175	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A3144, A3145, A3146, A3148, A3173, A3174, A3175	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A3207, A3211	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	A3139, A3168	Fixed Info Pattern - uPartyInfo||vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-3072 Increment 8 HMAC Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-56C Rev. 2
KDF SSH (CVL)	A3140, A3141, A3142, A3143, A3149, A3157, A3169, A3170, A3171, A3172	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF TLS (CVL)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	TLS Version - v1.0/1.1	SP 800-135 Rev. 1
PBKDF	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Iteration Count - Iteration Count: 10-1000 Increment 1 HMAC Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512 Password Length - Password Length: 8-128 Increment 1	SP 800-132

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-4096 Increment 8	
PBKDF	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Iteration Count - Iteration Count: 10-1000 Increment 1 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Password Length - Password Length: 8-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-4)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Key Generation Mode - B.3.3 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Random Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA SigVer (FIPS186-4)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
Safe Primes Key Generation	A3207, A3211	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
Safe Primes Key Verification	A3207, A3211	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
SHA-1	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A3147, A3156, A3161, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-224	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-256	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-384	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-512	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHAKE-128	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Supports Bit-Oriented Messages - No Supports Empty Message - Yes Supports Bit-Oriented Output - No Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A3144, A3145, A3146, A3148, A3173, A3174, A3175	Supports Bit-Oriented Messages - No Supports Empty Message - Yes Supports Bit-Oriented Output - No Output Length - Output Length: 16-65536 Increment 8	FIPS 202

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
TLS v1.2 KDF RFC7627 (CVL)	A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210	Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	SP 800-133 Rev. 2 Section 4 Example 1 with V=0

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

This module does not implement non-approved algorithms that are allowed in the approved mode of operation.

Non-Approved, Allowed Algorithms with No Security Claimed:

The table below lists the non-approved algorithms that are allowed in the approved mode of operation with no security claimed. These algorithms are used by the approved services listed in Section 4.3.

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

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

Non-Approved, Not Allowed Algorithms:

The table below lists non-approved algorithms that are not allowed in the approved mode of operation. These algorithms are used by the non-approved services listed in Section 4.4.

Name	Use and Function
AES(GCM) with external IV	Authenticated Symmetric encryption

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Use and Function
ARIA	Symmetric encryption; Symmetric decryption
Blake2	Message digest
Blowfish	Symmetric encryption; Symmetric decryption
Camellia	Symmetric encryption; Symmetric decryption
CAST	Symmetric encryption; Symmetric decryption
CAST5	Symmetric encryption; Symmetric decryption
ChaCha20	Symmetric encryption; Symmetric decryption
DES	Symmetric encryption; Symmetric decryption
Chacha20 and Poly1305	Authenticated encryption; Authenticated decryption
CMAC with Triple-DES	Message authentication code (MAC)
Diffie-Hellman with keys generated with domain parameters other than safe primes	Key agreement; Shared secret computation
DSA with any key sizes	Key pair generation; Domain parameter generation, Digital signature generation; Digital signature verification
EC Diffie-Hellman with P-192 curve, K curves, B curves and non-NIST curves	Key agreement; Shared secret computation
ECDSA with P-192 curve, K curves, B curves and non-NIST curves	Key pair generation; Key validation; Digital signature generation; Digital signature verification
GHASH	Message digest
Gost	Message digest

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Use and Function
HKDF	Key derivation as a standalone service
HMAC with less than 112-bit keys	Message authentication Code (MAC)
KDF SSH using Triple-DES	Key derivation
MD4	Message digest
MD5	Message digest
MDC2	Message digest
Multiblock ciphers using AES in CBC mode with 128- and 256-bit keys and HMAC SHA-1 and SHA-256 (available only in Intel processors with AES-NI capability)	Authenticated encryption; Authenticated decryption
PBKDF with non-approved message digest algorithms or input parameters not meeting requirements stated in Section 2.7.3	Key derivation
RC2	Symmetric encryption; Symmetric decryption
RC4	Symmetric encryption; Symmetric decryption
RMD160	Message digest
RSA with keys smaller than 2048 bits	Key pair generation; Domain parameter verification; Digital signature generation
RSA with keys smaller than 1024 bits	Digital signature verification
RSA encryption and decryption with any key sizes	Key encapsulation
SEED	Symmetric encryption; Symmetric decryption
SHA-1	Digital signature generation
SipHash	Message authentication code (MAC)
SM3	Message digest
SM4	Symmetric encryption; Symmetric decryption

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Use and Function
Triple-DES	Symmetric encryption; Symmetric decryption

Table 9: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric Encryption	BC-UnAuth	Symmetric Encryption		AES-CBC: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-CFB1: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-CFB128: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-CFB8: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-CTR: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137,

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A3158) AES-OFB: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-ECB: (A3171, A3162, A3150, A3143, A3169, A3142, A3140, A3157, A3170, A3154, A3166, A3141, A3163, A3138, A3136, A3165, A3160, A3149, A3167, A3172, A3137, A3158) AES-XTS Testing Revision 2.0: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158)
Symmetric Decryption	BC-UnAuth	Symmetric Decryption		AES-CBC: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-CFB1: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-CFB128: (A3162, A3150, A3154, A3166,

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-CFB8: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-CTR: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-OFB: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-ECB: (A3171, A3162, A3150, A3143, A3169, A3142, A3140, A3157, A3170, A3154, A3166, A3141, A3163, A3138, A3136, A3165, A3160, A3149, A3167, A3172, A3137, A3158) AES-XTS Testing Revision 2.0: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158)

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
Authenticated Symmetric Encryption	BC-Auth	Authenticated Symmetric Encryption		AES-CCM: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-GCM: (A3199, A3206, A3190, A3183, A3196, A3181, A3153, A3151, A3205, A3179, A3182, A3201, A3204, A3152, A3176, A3194, A3155, A3197, A3180, A3159, A3198, A3184, A3195, A3177, A3200, A3178) AES-CBC: (A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167) HMAC-SHA2-256: (A3147, A3156, A3161, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210) HMAC-SHA2-384: (A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210)
Authenticated Symmetric Decryption	BC-Auth	Authenticated Symmetric Decryption		AES-CCM: (A3162, A3150, A3154, A3166, A3163,

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-GCM: (A3199, A3206, A3190, A3183, A3196, A3181, A3153, A3151, A3205, A3179, A3182, A3201, A3204, A3152, A3176, A3194, A3155, A3197, A3180, A3159, A3198, A3184, A3195, A3177, A3200, A3178) AES-CBC: (A3136, A3137, A3138, A3150, A3154, A3158, A3160, A3162, A3163, A3165, A3166, A3167) HMAC-SHA2-256: (A3147, A3156, A3161, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210) HMAC-SHA2-384: (A3147, A3156, A3185, A3186, A3187, A3188, A3193, A3202, A3203, A3210)
Key Wrapping	BC-Auth	Key Wrapping (as a standalone service)		AES-KW: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158)

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				AES-KWP: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158)
Key Unwrapping	BC-Auth	Key Unwrapping (as a standalone service)		AES-KW: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) AES-KWP: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158)
Message Authentication Code (MAC)	MAC	Message Authentication Code (MAC)		AES-CMAC: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158) HMAC-SHA-1: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) HMAC-SHA2-224: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) HMAC-SHA2-256: (A3147, A3188, A3202, A3203, A3161, A3156,

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A3187, A3193, A3210, A3186, A3185) HMAC-SHA2-384: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) HMAC-SHA2-512: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) HMAC-SHA3-224: (A3144, A3145, A3148, A3175, A3146, A3173, A3174) HMAC-SHA3-256: (A3144, A3145, A3148, A3175, A3146, A3173, A3174) HMAC-SHA3-384: (A3144, A3145, A3148, A3175, A3146, A3173, A3174) HMAC-SHA3-512: (A3144, A3145, A3148, A3175, A3146, A3173, A3174)
Random Number Generation	DRBG	Random Number Generation		Counter DRBG: (A3162, A3150, A3154, A3166, A3163, A3138, A3136, A3165, A3160, A3167, A3137, A3158)

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
Key Pair Generation	AsymKeyPair-KeyGen CKG	Key Pair Generation	RSA Key Sizes:RSA key sizes other than 2048, 3072, and 4096 are not CAVP tested, but are approved as per IG C.F.	ECDSA KeyGen (FIPS186-4): (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) RSA KeyGen (FIPS186-4): (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) Safe Primes Key Generation: (A3207, A3211) CKG: ()
Key Pair Verification	AsymKeyPair-KeyVer	Key Pair Verification		ECDSA KeyVer (FIPS186-4): (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) Safe Primes Key Verification: (A3207, A3211)
Signature Generation	DigSig-SigGen	Digital signature generation	RSA Key Sizes:RSA key sizes other than 2048, 3072, and 4096 are not CAVP tested, but are approved as per IG C.F.	ECDSA SigGen (FIPS186-4): (A3147, A3188, A3144, A3145, A3148, A3202, A3203, A3156, A3175, A3146, A3173, A3187, A3193, A3210, A3186, A3185, A3174) RSA SigGen (FIPS186-4): (A3147, A3188, A3202, A3203,

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A3156, A3187, A3193, A3210, A3186, A3185)
Signature Verification	DigSig-SigVer	Digital signature verification	RSA Key Sizes:RSA key sizes other than 1024, 2048, 3072, and 4096 are not CAVP tested, but are approved as per IG C.F.	ECDSA SigVer (FIPS186-4): (A3147, A3188, A3144, A3145, A3148, A3202, A3203, A3156, A3175, A3146, A3173, A3187, A3193, A3210, A3186, A3185, A3174) RSA SigVer (FIPS186-4): (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185)
EC Diffie-Hellman shared secret computation	KAS-SSC	EC Diffie-Hellman shared secret computation		KAS-ECC-SSC Sp800-56Ar3: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185)
Diffie-Hellman shared secret computation	KAS-SSC	Diffie-Hellman shared secret computation		KAS-FFC-SSC Sp800-56Ar3: (A3211, A3207)
EC Diffie-Hellman KAS	KAS-Full	EC Diffie-Hellman KAS in the context of TLS	IG:IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL and KDA (separately tested) Caveat:Key establishment	KAS-ECC-SSC Sp800-56Ar3: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) ECDSA KeyGen (FIPS186-4): (A3147, A3156, A3185, A3186,

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
			methodology provides between 112 and 256 bits of security strength	A3187, A3188, A3193, A3202, A3203, A3210) KDA HKDF Sp800-56Cr1: (A3139, A3168) KDF TLS: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) TLS v1.2 KDF RFC7627: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185)
Diffie-Hellman KAS	KAS-Full	Diffie-Hellman KAS in the context of TLS	IG:IG D.F Scenario 2, path (2), split 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 200 bits of security strength	Safe Primes Key Generation: (A3207, A3211) KAS-FFC-SSC Sp800-56Ar3: (A3207, A3211) KDA HKDF Sp800-56Cr1: (A3139, A3168) KDF TLS: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) TLS v1.2 KDF RFC7627: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185)

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
Key Derivation with HKDF	KAS-56CKDF	Key derivation for TLS v1.3 used in the TLS protocol service		KDA HKDF Sp800-56Cr1: (A3139, A3168)
Key Derivation with TLS	KAS-135KDF	Key Derivation using TLS v1.2, v1.3		KDF TLS: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) TLS v1.2 KDF RFC7627: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185)
Key Derivation with SSH KDF	KAS-135KDF	Key Derivation using SSH KDF		KDF SSH: (A3171, A3143, A3169, A3142, A3140, A3157, A3170, A3141, A3149, A3172)
Key Derivation with PBKDF	PBKDF	Key Derivation using PBKDF		PBKDF: (A3147, A3188, A3144, A3145, A3148, A3202, A3203, A3156, A3175, A3146, A3173, A3187, A3193, A3210, A3186, A3185, A3174)
Message Digest	SHA XOF	Message Digest		SHA-1: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) SHA2-224: (A3147, A3188, A3202, A3203, A3156,

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A3187, A3193, A3210, A3186, A3185) SHA2-256: (A3147, A3188, A3202, A3203, A3161, A3156, A3187, A3193, A3210, A3186, A3185) SHA2-384: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) SHA2-512: (A3147, A3188, A3202, A3203, A3156, A3187, A3193, A3210, A3186, A3185) SHA3-224: (A3144, A3145, A3148, A3175, A3146, A3173, A3174) SHA3-256: (A3144, A3145, A3148, A3175, A3146, A3173, A3174) SHA3-384: (A3144, A3145, A3148, A3175, A3146, A3173, A3174) SHA3-512: (A3144, A3145, A3148, A3175, A3146, A3173, A3174) SHAKE-128: (A3144, A3145, A3148, A3175, A3146, A3173, A3174) SHAKE-256: (A3144, A3145, A3148, A3175,

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A3146, A3173, A3174)

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 SP 800-38E. The length of a single data unit encrypted or decrypted with AES-XTS 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 the service APIs.

AES-XTS keys (i.e., Key_1 and Key_2) entered into the module shall be generated and/or established independently according to NIST SP 800-133rev2, Section 6.3. for an approved use of AES-XTS.

2.7.2 AES GCM IV

The AES GCM IV generation is in compliance with RFC 5288 and shall only be used for the TLS protocol version 1.2 to be compliant with FIPS 140-3 IG C.H, provision 1 (“TLS protocol IV generation”); in addition, the module is compliant with Section 3.3.1 of SP 800-52 Rev. 2.

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 of 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.

When a GCM IV is used for decryption, the responsibility for the IV generation lies with the party that performs the AES GCM encryption.

2.7.3 Key Derivation using SP 800-132 PBKDF

The module provides password-based key derivation (PBKDF2), compliant with SP 800-132. The module supports option 1a from Section 5.4 of SP 800-132, in which the Master Key (MK) or a segment of it is used directly as the Data Protection Key (DPK).

In accordance to SP 800-132 and FIPS 140-3 IG D.N, the following requirements are met:

- Derived keys shall be used only for storage applications, and shall not be used for any other purposes. The length of the MK or DPK is 112 bits or more.
- Passwords or passphrases, used as an input for the PBKDF2, shall not be used as cryptographic keys.
- The minimum length of the password or passphrase accepted by the module is 20 characters. The probability of guessing the value, assuming a worst-case scenario of all digits, is estimated to be at most

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10^{-20}. Combined with the minimum iteration count as described below, this provides an acceptable trade-off between user experience and security against brute-force attacks.

- A portion of the salt shall be generated randomly using the SP 800-90A Rev. 1 DRBG provided by the module. The minimum length required is 128 bits.
- 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 accepted by the module is 1000.

If any of these requirements are not met, the requested service is non-approved (see Section 4.4).

2.7.4 SP 800-56A Rev. 3 Assurances

To comply with the assurances found in Section 5.6.2 of SP 800-56A Rev. 3, the operator must use the module in the context of the TLS or SSH protocols. Additionally, the module's approved key pair generation service (see Approved Services table in Section 4.3) must be used to generate ephemeral Diffie-Hellman or EC Diffie-Hellman key pairs, or the key pairs must be obtained from another FIPS-validated module. As part of this service, the module will internally perform the full public key validation of the generated public key.

The module's shared secret computation service will internally perform the full public key validation of the peer public key, complying with Sections 5.6.2.2.1 and 5.6.2.2.2 of SP 800-56A Rev. 3.

2.7.5 RSA Signatures

The module supports RSA with any even moduli size between 2048 and 16384 bits. Moduli lengths other than 2048, 3072, and 4096 bits cannot be tested by CAVP but are approved for RSA key generation, signature generation, and signature verification as per IG C.F.

2.7.6 Key Transport

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.

2.7.7 Key Agreement

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.

2.8 RBG and Entropy

The module employs a Deterministic Random Bit Generator (DRBG) based on SP 800-90A Rev. 1 for the creation of seeds for asymmetric keys, random numbers for security functions (e.g. ECDSA signature generation), and server and client random numbers for the TLS protocol. In addition, the module provides a Random Number Generation service to calling applications.

The DRBG supports the CTR_DRBG mechanism. The DRBG is initialized during module initialization; the module loads by default the DRBG using the CTR_DRBG mechanism with AES-256, with derivation function, and without prediction resistance. A different DRBG mechanism can be chosen through an API function call.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

The module uses an SP 800-90B-compliant entropy source specified in the following tables. This entropy source is located within the physical perimeter, but outside of the cryptographic boundary of the module. The module obtains 384 bits of entropy to seed the DRBG and 256 bits to reseed it, sufficient to provide a DRBG with 256 bits of security strength.

The operational environment on the ESV certificate is identical to the operational environment listed in this document. There are no maintenance requirements for the entropy source.

Cert Number	Vendor Name
E22	SUSE
E28	SUSE
E29	SUSE
E30	SUSE

Table 11: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Standalone Userspace CPU Time Jitter RNG version 3.4.0	Non-Physical	SUSE Linux Enterprise Server 15 SP4 on Intel® Xeon® Silver 4215R, SUSE Linux Enterprise Server 15 SP4 on AMD EPYC (TM) 7371, SUSE Linux Enterprise Server 15 SP4 on ARM Ampere® Altra® Q80-30, SUSE Linux Enterprise Server 15 SP4 on IBM z15, SUSE Linux Enterprise Server 15 SP4 on PowerVM (VIOS 3.1.4.00) on IBM Power10	256 bits	Full entropy	SHA3-256 (A3034, A3036)

Table 12: Entropy Sources

2.9 Key Generation

The module implements asymmetric key pair generation compliant with SP 800-133 Rev. 2. When random values are required, they are obtained from the SP 800-90A Rev. 1 approved DRBG, compliant with Section 4 of SP 800-133 Rev. 2 (without XOR). The following methods are implemented:

- Safe primes key pair generation: compliant with SP 800-133 Rev. 2, Section 5.2
- RSA key pair generation: compliant with SP 800-133 Rev. 2, Section 5.1
- ECC (ECDH and ECDSA) key pair generation: compliant with SP 800-133 Rev. 2, Section 5.1

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

The key pair generation methods implemented for each of the services mentioned above have been CAVP tested and are described in Section 2.6.

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

Additionally, the module implements the following key derivation methods according to SP 800-135 Rev. 1:

- KDF for the TLS protocol used as pseudo-random functions (PRF) for TLS v1.2;
- KDA HKDF for the TLS protocol, used as pseudo-random function (PRF) for TLS v1.3;
- KDA HKDF as standalone KDF.
- SSH KDF for the SSHv2 protocol.

The module also supports password-based key derivation (PBKDF). The implementation is compliant with option 1a of SP 800-132.

2.10 Key Establishment

The module provides Diffie-Hellman and EC Diffie-Hellman shared secret computation compliant with SP 800-56A Rev. 3, in accordance with scenario 2 (1) of FIPS 140-3 IG D.F.

The module also provides Diffie-Hellman and EC Diffie-Hellman key agreement schemes compliant with SP 800-56A Rev. 3 and used as part of the TLS protocol key exchange in accordance with scenario 2 (2) of FIPS 140-3 IG D.F; that is, the shared secret computation (KAS-FFC-SSC and KAS-ECC-SSC) followed by the derivation of the keying material using SP 800-135 Rev. 1 KDF or the KDA HKDF compliant to SP 800-56C Rev. 2 for version 1.3 of the TLS protocol.

2.11 SHA-1 Use

SHA-1 is only approved when used in approved modes for message digest, HMAC, PBKDF, KDF SSH and RSA/ECDSA Digital Signature Verification.

2.12 Industry Protocols

The module supports cipher suites for the TLS protocol versions 1.0, 1.1, 1.2, and 1.3 compliant with Section 3.3.1 of SP 800-52 Rev. 2. Each cipher suite defines the key exchange algorithm, the bulk encryption algorithm (including the symmetric key size), and the MAC algorithm. All cipher suites supported by the module can be found in Appendix A.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

As a software-only module, the module does not have physical ports. The operator can only interact with the module through the API provided by the module. Thus, the physical ports are interpreted to be the physical ports of the hardware platform on which the module runs. The following table shows the logical interfaces implemented in the module.

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

The logical interfaces are the APIs through which applications may request service. These logical interfaces are logically separated from each other by the API design. All data output via the data output interface is inhibited when the module is performing pre-operational test or zeroization or when the module enters the error state.

The module does not implement a control output interface.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4 Roles, Services, and Authentication

4.1 Authentication Methods

This module does not support authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	Crypto Officer	None

Table 14: Roles

The Crypto Officer role is implicitly and always assumed by the operator of the module. The module does not support multiple concurrent operators.

4.3 Approved Services

The table below lists the approved services. For each service, the table lists the associated cryptographic algorithm(s), the role to perform the service, the cryptographic keys or SSPs involved, and their access type(s). No support of intermediate key generation is provided. The following convention is used to specify access rights to an SSP:

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

The details of the approved cryptographic algorithms including the CAVP certificate numbers can be found in Section 2.5.

The “Indicator” column shows the service indicator API functions that must be used to verify the service indicator for each of the services. A value of 1 indicates that the service is approved, and 0 indicates that the service is non-approved.

Additionally there is a separate indicator used for the following services.

- The API function used to determine the indicator for the “TLS network protocol” service returns the cipher suite established for the TLS session. If the returned cipher suite ID belongs to one of the cipher suites listed in Appendix A, then the service is approved, otherwise, it is non-approved.

For more information, see the “FIPS server level indicator” man pages.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Symmetric encryption	Perform AES encryption	fips_sli_is_approved_EVP_CIPHER_CTX returns 1	Plaintext, AES key, IV	Ciphertext	Symmetric Encryption	Crypto Officer - AES key: W,E
Authenticated symmetric encryption	Perform AES encryption	fips_sli_is_approved_EVP_CIPHER_CTX returns 1	Plaintext, AES key, IV	Ciphertext, MAC tag	Authenticated Symmetric Encryption	Crypto Officer - AES key: W,E
Symmetric decryption	Perform AES decryption	fips_sli_is_approved_EVP_CIPHER_CTX returns 1	Ciphertext, AES key, IV	Plaintext	Symmetric Decryption	Crypto Officer - AES key: W,E
Authenticated symmetric decryption	Perform AES decryption	fips_sli_is_approved_EVP_CIPHER_CTX returns 1	Ciphertext, AES key, IV, MAC tag	Plaintext or Fail	Authenticated Symmetric Decryption	Crypto Officer - AES key: W,E
RSA key pair generation	Generate RSA key pairs	fips_sli_is_approved_EVP_PKEY_CTX returns 1	Modulus size	RSA Key Pair	Key Pair Generation	Crypto Officer - Module-generated RSA public key: G,R - Module-generated RSA private key: G,R - Intermediate Key Generation Value: G,E,Z
ECDSA key pair generation	Generate ECDSA key pairs	fips_sli_is_approved_EVP_PKEY_CTX returns 1	EC Domain Parameters	ECDSA Key Pair	Key Pair Generation	Crypto Officer - Module-generated ECDSA public key: G,R - Module-

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						generated ECDSA private key: G,R - Intermediate Key Generation Value: G,E,Z
RSA digital signature generation	Sign using RSA	fips_sli_is_approved_EVP_PKEY_CTX returns 1	Message, RSA private key	Signature	Signature Generation	Crypto Officer - RSA private key: W,E
ECDSA digital signature generation	Sign using ECDSA	fips_sli_is_approved_EVP_PKEY_CTX returns 1	Message, ECDSA private key	Signature	Key Pair Generation	Crypto Officer - ECDSA private key: W,E
RSA digital signature verification	Verify RSA signatures	fips_sli_is_approved_EVP_PKEY_CTX returns 1	Message, RSA public key, Signature	Pass or Fail	Signature Verification	Crypto Officer - RSA public key: W,E
ECDSA digital signature verification	Verify ECDSA signatures	fips_sli_is_approved_EVP_PKEY_CTX returns 1	Message, ECDSA public key, Signature	Pass or Fail	Signature Verification	Crypto Officer - ECDSA public key: W,E
Key validation	Validate ECDSA public key	fips_sli_is_approved_EVP_PKEY_CTX returns 1	ECDSA public key	Pass or Fail	Key Pair Verification	Crypto Officer - ECDSA public key: W,E
Random number	Generate random	fips_sli_is_approved_EVP_PKEY_CTX returns 1	Output length	Random bytes	Random Number	Crypto Officer - DRBG internal state (V, key): G,E

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
generation	bitstrings				Generation	- Entropy input: W,E,Z - DRBG seed: G,E,Z
Message digest	Compute SHA hashes	fips_sli_SHA*_is_approved returns 1	Message	Message digest	Message Digest	Crypto Officer
Message authentication code (HMAC)	Compute HMAC	fips_sli_HMAC_is_approved returns 1	Message, HMAC key	MAC	Message Authentication Code (MAC)	Crypto Officer - HMAC key: W,E
Message authentication code (CMAC)	Compute an AES-based CMAC	fips_sli_is_approved_CMAC_CTX returns 1	Message, AES key	MAC	Message Authentication Code (MAC)	Crypto Officer - AES key: W,E
Key wrapping	Perform AES-based key wrapping	fips_sli_is_approved_EVP_CIPHER_CTX returns 1	Key to be wrapped, AES key wrapping key	Wrapped key	Key Wrapping	Crypto Officer - AES key: W,E
Key unwrapping	Perform AES-based key unwrapping	fips_sli_is_approved_EVP_CIPHER_CTX returns 1	Key to be unwrapped, AES key wrapping key	Unwrapped key	Key Unwrapping	Crypto Officer - AES key: W,E
DH shared secret computation	Diffie-Hellman shared secret computation	fips_sli_is_approved_EVP_PKEY_CTX returns 1	DH private key, DH public key	DH shared secret	Diffie-Hellman shared secret computation	Crypto Officer - Diffie-Hellman private key: W,E - Diffie-Hellman

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			from peer			public key: W,E - Diffie-Hellman shared secret: G,R
ECDH shared secret computation	EC Diffie-Hellman shared secret computation	fips_sli_is_approved_EVP_PKEY_CTX returns 1	ECDH private key, ECDH public key from peer	ECDH shared secret	EC Diffie-Hellman shared secret computation	Crypto Officer - EC Diffie-Hellman private key: W,E - EC Diffie-Hellman public key: W,E - EC Diffie-Hellman shared secret: G,R
Diffie-Hellman key generation using safe primes	Perform Diffie-Hellman key generation with safe primes	fips_sli_is_approved_EVP_PKEY_CTX returns 1	DH group	DH key pair	Key Pair Generation	Crypto Officer - Module-generated Diffie-Hellman public key: G,R - Module-generated Diffie-Hellman private key: G,R - Intermediate Key Generation Value: G,E,Z
Diffie-Hellman key verification using	Perform Diffie-Hellman key verification with	fips_sli_is_approved_EVP_PKEY_CTX returns 1	DH key pair, DH group	Pass or Fail	Key Pair Verification	Crypto Officer - Diffie-Hellman public key: W,E - Diffie-

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
safe primes	safe primes					Hellman private key: W,E
Key derivation (TLS/SSH)	Perform TLS 1.2, TLS 1.3, or SSH key derivation	fips_sli_is_approved_EVP_KDF_CTX returns 1	Shared secret	TLS 1.2, TLS 1.3, or SSH derived key	Key Derivation with HKDF Key Derivation with TLS Key Derivation with SSH KDF	Crypto Officer - EC Diffie-Hellman shared secret: W,E - Diffie-Hellman shared secret: W,E - TLS Derived key: G,R - SSH Derived key: G,R - TLS pre-master secret: W,E - TLS master secret: G,W,E
Key derivation (password)	Perform password-based key derivation	fips_sli_PKCS5_PBKDF2_HMAC_is_approved returns 1	Password	PBKDF derived key	Key Derivation with PBKDF	Crypto Officer - Password/passphrase: W,E - PBKDF Derived key: G,R
Transport Layer Security (TLS) network protocol	Provide supported cipher suites in the approved mode of operation	SSL_CIPHER_get_protocol_id or SSL_get_current_cipher returns a two-byte ID matching an approved cipher suite	Cipher suite listed in Appendix A, Digital Certificate, Public and Private Keys, Applica	Return codes and/or log messages, Application Data	Signature Generation Signature Verification EC Diffie-Hellman KAS Diffie-Hellman KAS	Crypto Officer - RSA public key: W,E - ECDSA public key: W,E - TLS pre-master secret: G,E - TLS master secret: G,E - TLS Derived key: G,E - RSA private

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			tion Data			key: W,E - ECDSA private key: W,E - Diffie-Hellman public key: W,E - Diffie-Hellman private key: W,E - KAS Domain Parameters: E
Show status	Show module status	Implicit (always approved)	None	Module status	None	Crypto Officer
Zeroization	Zeroize SSPs	Implicit (always approved)	None	None	None	Crypto Officer - AES key: Z - HMAC key: Z - Module-generated RSA public key: Z - Module-generated RSA private key: Z - RSA public key: Z - RSA private key: Z - Module-generated ECDSA public key: Z - Module-generated ECDSA private key: Z - ECDSA public key: Z

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Derived key: Z - SSH Derived key: Z - PBKDF Derived key: Z - Entropy input: Z - DRBG seed: Z - DRBG internal state (V, key): Z - TLS pre-master secret: Z - TLS master secret: Z
Self-tests	Perform self-tests	Implicit (always approved)	None	Pass or Fail	Symmetric Encryption Symmetric Decryption Authenticated Symmetric Encryption Authenticated Symmetric Decryption Key Wrapping Key Unwrapping	Crypto Officer

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Message Authentication Code (MAC) Random Number Generation Key Pair Generation Key Pair Verification Signature Generation Signature Verification EC Diffie-Hellman shared secret computation Diffie-Hellman shared secret computation Key Derivation with HKDF Key Derivation with PBKDF Key Derivation with SSH KDF	

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Key Derivation with TLS Message Digest	
Show module name and version	Show module name and version	Implicit (always approved)	None	Module name/version	None	Crypto Officer

Table 15: Approved Services

4.4 Non-Approved Services

The below table lists the non-approved services. The details of the non-approved cryptographic algorithms available in non-approved mode can be found in Section 2.5.

Name	Description	Algorithms	Role
AES(GCM) with external IV	Authenticated Symmetric encryption	AES(GCM) with external IV	CO
ARIA	Symmetric encryption; Symmetric decryption	ARIA	CO
Blowfish	Symmetric encryption; Symmetric decryption	Blowfish	CO
Camellia	Symmetric encryption; Symmetric decryption	Camellia	CO
CAST	Symmetric encryption; Symmetric decryption	CAST	CO
CAST5	Symmetric encryption; Symmetric decryption	CAST5	CO
ChaCha20	Symmetric encryption; Symmetric decryption	ChaCha20	CO

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Algorithms	Role
DES	Symmetric encryption; Symmetric decryption	DES	CO
RC4	Symmetric encryption; Symmetric decryption	RC4	CO
RC2	Symmetric encryption; Symmetric decryption	RC2	CO
SEED	Symmetric encryption; Symmetric decryption	SEED	CO
Triple-DES	Symmetric encryption; Symmetric decryption	Triple-DES	CO
SM4	Symmetric encryption; Symmetric decryption	SM4	CO
Chacha20 and Poly1305	Authenticated symmetric encryption; Authenticated symmetric decryption	Chacha20 and Poly1305	CO
Multiblock ciphers using AES in CBC mode with 128- and 256-bit keys and HMAC SHA-1 and SHA-256 (available only in Intel processors with AES-NI capability)	Authenticated symmetric encryption; Authenticated symmetric decryption	Multiblock ciphers using AES in CBC mode with 128- and 256-bit keys and HMAC SHA-1 and SHA-256 (available only in Intel processors with AES-NI capability)	CO
Blake2	Message digest	Blake2	CO
GHASH	Message digest	GHASH	CO
Gost	Message digest	Gost	CO
MD4	Message digest	MD4	CO
MD5	Message digest	MD5	CO
MDC2	Message digest	MDC2	CO
RMD160	Message digest	RMD160	CO
SM3	Message digest	SM3	CO

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Algorithms	Role
CMAC with Triple-DES	Message authentication code (MAC)	CMAC with Triple-DES	CO
HMAC with less than 112-bit keys	Message authentication Code (MAC)	HMAC with less than 112-bit keys	CO
SipHash	Message authentication code (MAC)	SipHash	CO
KDF SSH using Triple-DES	Key derivation	KDF SSH using Triple-DES	CO
PBKDF with non-approved message digest algorithms or input parameters not meeting requirements stated in Section 2.7.3	Key derivation	PBKDF with non-approved message digest algorithms or input parameters not meeting requirements stated in Section 2.7.3	CO
HKDF	Key derivation as a standalone service	HKDF	CO
Diffie-Hellman with keys generated with domain parameters other than safe primes	Key agreement; Shared secret computation	Diffie-Hellman with keys generated with domain parameters other than safe primes	CO
EC Diffie-Hellman with P-192 curve, K curves, B curves and non-NIST curves	Key agreement; Shared secret computation	EC Diffie-Hellman with P-192 curve, K curves, B curves and non-NIST curves	CO
DSA with any key sizes	Key pair generation; Domain parameter generation, Digital signature generation; Digital signature verification	DSA with any key sizes	CO
RSA with keys smaller than 2048 bits	Key pair generation; Domain parameter verification; Digital signature generation	RSA with keys smaller than 2048 bits	CO
ECDSA with P-192 curve, K curves, B curves and non-NIST curves (Key pair generation/validation)	Key pair generation; Key validation	ECDSA with P-192 curve, K curves, B curves and non-NIST curves	CO

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Algorithms	Role
RSA encryption and decryption with any key sizes	Key encapsulation	RSA encryption and decryption with any key sizes	CO
ECDSA with P-192 curve, K curves, B curves and non-NIST curves (Signature generation/verification)	Digital signature generation; Digital signature verification	ECDSA with P-192 curve, K curves, B curves and non-NIST curves	CO
RSA with keys smaller than 1024 bits	Digital signature verification	RSA with keys smaller than 1024 bits	CO
SHA-1	Digital signature generation	SHA-1	CO

Table 16: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not support the loading of external software or firmware.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified by comparing an HMAC-SHA2-256 value calculated at run time with the HMAC-SHA2-256 value stored in the .hmac file that was computed at build time for each software component of the module. If the HMAC values do not match, the test fails and the module enters the error state. The MAC key is hardcoded in the module.

5.2 Initiate on Demand

Integrity tests are performed as part of the pre-operational self-tests, which are executed when the module is initialized. The integrity test may be invoked on-demand by unloading and subsequently re-initializing the module.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

Any SSPs contained within the module are protected by the process isolation and memory separation mechanisms, and only the module has control over these SSPs.

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

The module shall be installed as stated in Section 11.1.

Instrumentation tools like the ptrace system call, gdb and strace utilities, 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-tested operational environment.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

7 Physical Security

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

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

8 Non-Invasive Security

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

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9 Sensitive Security Parameters Management

9.1 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.

Storage Area Name	Description	Persistence Type
RAM	Temporary storage for SSPs used by the module as part of service execution.	Dynamic

Table 17: Storage Areas

9.2 SSP Input-Output Methods

The module does not support manual SSP entry or intermediate SSP generation output. The 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 FIPS 140-3 IG 9.5.A, according to the "CM Software to/from App via TOEPP Path" entry in the Key Establishment Table.

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

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Wipe and Free memory block allocated	Zeroizes the SSPs contained within the cipher handle.	Memory occupied by SSPs is overwritten with zeroes and then it is released, which renders the SSP values irretrievable. The completion of the	By calling the cipher related zeroization API functions: EVP_CIPHER_CTX_free/ EVP_CIPHER_reset for AES keys, HMAC_CTX_free for HMAC keys, RSA_free for RSA keys, EC_KEY_free for ECDSA and ECDH keys/shared secrets, DH_free for DH keys/shared secrets, EVP_PKEY_free for

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Zeroization Method	Description	Rationale	Operator Initiation
		zeroization routine indicates that the zeroization procedure succeeded.	passwords and derived keys, FIPS_drbg_free for DRBG SSPs, SSL_free/SSL_clear for TLS secrets
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
Module Reset	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	By unloading and reloading the module

Table 19: SSP Zeroization Methods

The memory occupied by SSPs is allocated by regular memory allocation operating system calls. The application that is acting as the CO is responsible for calling the appropriate zeroization functions provided in the module's API and listed in Section 4.3. Calling the SSL_free() and SSL_clear() will zeroize the SSPs stored in the TLS protocol internal state and also invoke the corresponding API functions listed in Section 4.3 to zeroize SSPs. The zeroization functions overwrite the memory occupied by SSPs with “zeros” and deallocate the memory with the regular memory deallocation operating system call. The completion of a zeroization routine(s) will indicate that a zeroization procedure succeeded.

9.4 SSPs

The following tables summarize the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	AES key	128, 192, 256 bits - 128, 192, 256 bits	Symmetric key - CSP			Symmetric Encryption Symmetric Decryption Authenticated Symmetric Encryption Authenticat

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						ed Symmetric Decryption Key Wrapping Key Unwrapping Message Authentication Code (MAC)
HMAC key	HMAC key	112 to 524288 bits - 112 to 256 bits	Symmetric key - CSP			Message Authentication Code (MAC)
Module-generated RSA public key	Module-generated RSA public key	2048 to 16384 bits - 112 to 256 bits	Public key - PSP	Key Pair Generation		
Module-generated RSA private key	Module-generated RSA private key	2048 to 16384 bits - 112 to 256 bits	Private key - CSP	Key Pair Generation		
RSA public key	RSA public key	1024 to 16384 bits - 80 to 256 bits	Public key - PSP			Signature Verification
RSA private key	RSA private key	2048 to 16384 bits - 112 to 256 bits	Private key - CSP			Signature Generation
Module-generated ECDSA public key	Module-generated ECDSA public key	P-224, P-256, P-384, P-521 bits - 112, 128, 192, 256 bits	Public key - PSP	Key Pair Generation		
Module-generated	Module-generated	P-224, P-256, P-384, P-521 bits - 112,	Private key - CSP	Key Pair Generation		

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ECDSA private key	ECDSA private key	128, 192, 256 bits				
ECDSA public key	ECDSA public key	P-224, P-256, P-384, P-521 bits - 112, 128, 192, 256 bits	Public key - PSP			Key Pair Verification Signature Verification
ECDSA private key	ECDSA private key	P-224, P-256, P-384, P-521 bits - 112, 128, 192, 256 bits	Private key - CSP			Key Pair Verification Signature Verification
Module-generated EC Diffie-Hellman public key	Module-generated EC Diffie-Hellman public key	P-224, P-256, P-384, P-521 bits - 112, 128, 192, 256 bits	Public key - PSP	Key Pair Generation		
Module-generated EC Diffie-Hellman private key	Module-generated EC Diffie-Hellman private key	P-224, P-256, P-384, P-521 bits - 112, 128, 192, 256 bits	Private key - CSP	Key Pair Generation		
EC Diffie-Hellman public key	EC Diffie-Hellman public key	P-224, P-256, P-384, P-521 bits - 112, 128, 192, 256 bits	Public key - PSP			Key Pair Verification EC Diffie-Hellman shared secret computation EC Diffie-Hellman KAS
EC Diffie-Hellman private key	EC Diffie-Hellman private key	P-224, P-256, P-384, P-521 bits - 112, 128, 192, 256 bits	Private key - CSP			Key Pair Verification EC Diffie-Hellman shared secret computation EC Diffie-

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Hellman KAS
Module-generated Diffie-Hellman public key	Module-generated Diffie-Hellman public key	MODP-2048, ffdhe2048, MODP-3072, ffdhe3072, MODP-4096, ffdhe4096, MODP-6144, ffdhe6144, MODP-8192, ffdhe8192 - 112, 128, 149, 172, 200 bits	Public key - PSP	Key Pair Generation		
Module-generated Diffie-Hellman private key	Module-generated Diffie-Hellman private key	MODP-2048, ffdhe2048, MODP-3072, ffdhe3072, MODP-4096, ffdhe4096, MODP-6144, ffdhe6144, MODP-8192, ffdhe8192 - 112, 128, 149, 172, 200 bits	Private key - CSP	Key Pair Generation		
Diffie-Hellman public key	Diffie-Hellman public key	MODP-2048, ffdhe2048, MODP-3072, ffdhe3072, MODP-4096, ffdhe4096, MODP-6144, ffdhe6144, MODP-8192, ffdhe8192 - 112, 128, 149, 172, 200 bits	Public key - PSP			Key Pair Verification Diffie-Hellman shared secret computation Diffie-Hellman KAS
Diffie-Hellman private key	Diffie-Hellman private key	MODP-2048, ffdhe2048, MODP-3072,	Private key - CSP			Key Pair Verification Diffie-

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		ffdhe3072, MODP-4096, ffdhe4096, MODP-6144, ffdhe6144, MODP-8192, ffdhe8192 - 112, 128, 149, 172, 200 bits				Hellman shared secret computation Diffie-Hellman KAS
EC Diffie-Hellman shared secret	EC Diffie-Hellman shared secret	P-224, P-256, P-384, P-512 - 112, 128, 192, 256 bits	Shared secret - CSP		EC Diffie-Hellman shared secret computation	Key Derivation with HKDF Key Derivation with SSH KDF
Diffie-Hellman shared secret	Diffie-Hellman shared secret	MODP-2048, ffdhe2048, MODP-3072, ffdhe3072, MODP-4096, ffdhe4096, MODP-6144, ffdhe6144, MODP-8192, ffdhe8192 - 112, 128, 149, 172, 200 bits	Shared secret - CSP		Diffie-Hellman shared secret computation	Key Derivation with HKDF Key Derivation with SSH KDF
Password/passphrase	Password/passphrase	8-128 bytes - N/A	Password - CSP			Key Derivation with PBKDF
TLS Derived key	TLS Derived key	112-256 bits - 112-256 bits	Symmetric key - CSP	Key Derivation with HKDF Key Derivation with TLS	EC Diffie-Hellman KAS Diffie-Hellman KAS	

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH Derived key	SSH Derived key	112-256 bits - 112-256 bits	Symmetric key - CSP	Key Derivation with SSH KDF		
PBKDF Derived key	PBKDF Derived key	128-4096 bits - 112-256 bits	Symmetric key - CSP	Key Derivation with PBKDF		
Entropy input	Entropy input (IG D.L compliant)	192-384 bits - 192-384 bits	Entropy Input - CSP	Random Number Generation		Random Number Generation
DRBG seed	DRBG seed (IG D.L compliant)	256, 320, 384 bits - 128, 192, 256 bits	Seed - CSP	Random Number Generation		Random Number Generation
DRBG internal state (V, key)	DRBG internal state (V, key) (IG D.L compliant)	256, 320, 384 bits - 128, 192, 256 bits	Internal state - CSP	Random Number Generation		Random Number Generation
TLS pre-master secret	TLS pre-master secret	DH: MODP-2048/ffdhe2048 to MODP-8192/ffdhe-8192; ECDH: P-224, P-256, P-384, P-521 bits - DH: 112 to 200 bits; ECDH: 112, 128, 192, 256 bits	Shared secret - CSP			Key Derivation with HKDF Key Derivation with TLS
TLS master secret	TLS master secret	384 bits - 112-256 bits	Master secret - CSP	Key Derivation with HKDF Key Derivation		Key Derivation with HKDF Key Derivation with TLS

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
				n with TLS		
KAS Domain Parameters	SP 800-56Arev3 domain parameters used for KAS	DH: MODP-2048/ffdhe2048 to MODP-8192/ffdhe8192; ECDH: P-224, P-256, P-384, P-521 - N/A	Domain parameters - PSP			EC Diffie-Hellman KAS Diffie-Hellman KAS
Intermediate Key Generation Value	Intermediate key pair generation value generated during key generation and key derivation services (SP 800-133 Rev. 2 Section 4, 5.1, and 5.2)	112-16384 bits - 112-256 bits	Intermediate value - CSP	Key Pair Generation		Key Pair Generation

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	API input parameters	RAM:Plaintext	From service invocation to service completion	Module Reset Wipe and Free memory block allocated	
HMAC key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Module-generated RSA public key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module-generated RSA private key:Paired With
Module-generated RSA private key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module-generated RSA public key:Paired With
RSA public key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	RSA private key:Paired With
RSA private key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	RSA public key:Paired With
Module-generated ECDSA public key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module-generated ECDSA private key:Paired With
Module-generated ECDSA private key	API output parameters	RAM:Plaintext	From service invocation to service	Wipe and Free memory block	Module-generated ECDSA public key:Paired With

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			completion	allocated Module Reset	
ECDSA public key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	ECDSA private key:Paired With
ECDSA private key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	ECDSA public key:Paired With
Module-generated EC Diffie-Hellman public key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module-generated EC Diffie-Hellman private key:Paired With
Module-generated EC Diffie-Hellman private key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module-generated EC Diffie-Hellman public key:Paired With
EC Diffie-Hellman public key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	EC Diffie-Hellman private key:Paired With EC Diffie-Hellman shared secret:Establishes

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
EC Diffie-Hellman private key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	EC Diffie-Hellman public key:Paired With EC Diffie-Hellman shared secret:Establishes
Module-generated Diffie-Hellman public key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module-generated Diffie-Hellman private key:Paired With
Module-generated Diffie-Hellman private key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module-generated Diffie-Hellman public key:Paired With
Diffie-Hellman public key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Diffie-Hellman private key:Paired With Diffie-Hellman shared secret:Establishes
Diffie-Hellman private key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Diffie-Hellman public key:Paired With Diffie-Hellman shared secret:Establishes
EC Diffie-Hellman shared secret	API input parameters API	RAM:Plaintext	From service invocation to service	Wipe and Free memory block	EC Diffie-Hellman public key:Established by EC Diffie-Hellman private

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	output parameters		completion	allocated Module Reset	key:Established by SSH Derived key:Derives
Diffie-Hellman shared secret	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Diffie-Hellman public key:Established by Diffie-Hellman private key:Established by SSH Derived key:Derives
Password/passphrase	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	PBKDF Derived key:Derives
TLS Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	TLS master secret:Derived From
SSH Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	EC Diffie-Hellman shared secret:Derived From Diffie-Hellman shared secret:Derived From
PBKDF Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Password/passphrase:Derived From

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Entropy input		RAM:Plaintext	From service invocation to service completion	Automatic Module Reset	DRBG seed:Derives
DRBG seed		RAM:Plaintext	From service invocation to service completion	Automatic Module Reset	Entropy input:Derived From DRBG internal state (V, key):Derives
DRBG internal state (V, key)		RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	DRBG seed:Derived From
TLS pre-master secret	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	TLS master secret:Derives
TLS master secret		RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Automatic Module Reset	TLS Derived key:Derives TLS pre-master secret:Derived From
KAS Domain Parameters		RAM:Plaintext	From service invocation to service	Wipe and Free memory block allocated	

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			completion	Automatic Module Reset	
Intermediate Key Generation Value		RAM:Plaintext	From service invocation to service completion	Automatic	Module-generated RSA public key:Derived From Module-generated RSA private key:Derived From Module-generated ECDSA public key:Derived From Module-generated ECDSA private key:Derived From Module-generated EC Diffie-Hellman public key:Derived From Module-generated EC Diffie-Hellman private key:Derived From Module-generated Diffie-Hellman public key:Derived From Module-generated Diffie-Hellman private key:Derived From

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.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests

10.1 Pre-Operational Self-Tests

The pre-operational software integrity tests are performed automatically when the module is initialized, before the module transitions into the operational state. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the tests are successfully completed. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

A CAST is performed on each algorithm used in the Pre-operational Self-Tests prior to their execution.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A3147)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3156)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3161)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3185)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3186)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3187)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3188)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3193)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3202)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3203)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A
HMAC-SHA2-256 (A3210)	SHA2-256	MAC tag verification	SW/FW Integrity	Module becomes operational	N/A

Table 22: Pre-Operational Self-Tests

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10.2 Conditional Self-Tests

Data output through the data output interface is inhibited during the conditional self-tests. The module does not return control to the calling application until the tests are completed. If any of these tests fails, the module transitions to the error state as described in Section 10.4.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3171) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3162) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3150) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3143) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3169) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3142) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3140) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3157) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3170) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3154) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3166) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3141) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3163) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3138) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3136) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3165) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3160) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3149) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3167) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3172) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3137) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3158) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3171) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3162) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3150) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3143) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3169) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3142) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3140) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3157) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3170) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3154) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3166) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3141) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3163) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3138) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3136) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3165) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3160) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3149) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3167) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3172) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3137) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3158) - Decryption	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A3162) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3150) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3154) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3166) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3163) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3138) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3136) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3165) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3160) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A3167) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3137) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3158) - Encryption	192-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3162) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3150) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3154) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3166) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3163) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3138) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A3136) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3165) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3160) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3167) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3137) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3158) - Decryption	192-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3199) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3206) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3190) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3183) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3196) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3181) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3153) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3151) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3205) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3179) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3182) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3201) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3204) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3152) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3176) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3194) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3155) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3197) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3180) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3159) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3198) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3184) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3195) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3177) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3200) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3178) - Encryption	256-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3199) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3206) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3190) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3183) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3196) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3181) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3153) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3151) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3205) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3179) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3182) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3201) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3204) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3152) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3176) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3194) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3155) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3197) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3180) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3159) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3198) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3184) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3195) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3177) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3200) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3178) - Decryption	256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3163) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3137) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3136) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3162) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (A3138) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3154) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3158) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3166) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3167) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3165) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3160) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (A3150) - Encryption	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3163) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3137) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3136) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3162) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3138) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3154) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (A3158) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3166) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3167) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3165) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3160) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3150) - Decryption	128/256-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CMAC (A3162) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3150) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
AES-CMAC (A3154) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3166) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3163) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3138) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3136) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3165) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3160) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3167) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CMAC (A3137) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3158) - Encryption	128/192/256-bit key, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
Counter DRBG (A3162)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3150)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3154)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3166)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3163)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3138)	256-bit key, with/without df, with/without	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	prediction resistance					
Counter DRBG (A3136)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3165)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3160)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3167)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3137)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A3158)	256-bit key, with/without df, with/without prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A3211) - KAT	MODP-2048, ffdhe2048	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-FFC-SSC Sp800-56Ar3 (A3207) - KAT	MODP-2048, ffdhe2048	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3147)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3188)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3202)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3203)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3156)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3187)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3193)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3210)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-ECC-SSC Sp800-56Ar3 (A3186)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3185)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3147)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3188)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3144)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3145)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3148)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3202)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3203)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen (FIPS186-4) (A3156)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3175)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3146)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3173)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3187)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3193)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3210)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3186)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3185)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen (FIPS186-4) (A3174)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3147)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3188)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3144)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3145)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3148)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3202)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3203)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3156)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4) (A3175)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3146)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3173)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3187)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3193)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3210)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3186)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3185)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3174)	P-256 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 (A3147)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3188)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3202)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3203)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3156)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3187)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3193)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3210)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3186)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 (A3185)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3147)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3188)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3202)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3203)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3156)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3187)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3193)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3210)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A3186)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3185)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3147)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3188)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3202)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3203)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3161)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3156)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3187)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A3193)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3210)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3186)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3185)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3147)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3188)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3202)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3203)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3156)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 (A3187)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3193)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3210)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3186)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3185)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3147)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3188)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3202)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3203)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A3156)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3187)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3193)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3210)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3186)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3185)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3144)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3145)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3148)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-224 (A3175)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3146)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3173)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3174)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3144)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3145)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3148)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3175)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3146)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-256 (A3173)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3174)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3144)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3145)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3148)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3175)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3146)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3173)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3174)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-512 (A3144)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3145)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3148)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3175)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3146)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3173)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3174)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
PBKDF (A3147)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3188)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
PBKDF (A3144)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3145)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3148)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3202)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3203)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3156)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3175)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3146)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3173)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
PBKDF (A3187)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3193)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3210)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3186)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3185)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3174)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3147) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3188) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3202) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-4) (A3203) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3156) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3187) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3193) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3210) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3186) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3185) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3147) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3188) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-4) (A3202) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3203) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3156) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3187) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3193) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3210) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3186) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3185) - PKCS#1 v1.5	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3147) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-4) (A3188) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3202) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3203) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3156) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3187) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3193) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3210) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3186) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3185) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-4) (A3147) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3188) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3202) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3203) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3156) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3187) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3193) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3210) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3186) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-4) (A3185) - PSS	PSS with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
SHA-1 (A3147)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3188)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3202)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3203)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3156)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3187)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3193)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3210)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A3186)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3185)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3147)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3188)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3202)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3203)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3156)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3187)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3193)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-224 (A3210)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3186)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3185)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3147)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3188)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3202)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3203)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3161)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3156)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A3187)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3193)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3210)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3186)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3185)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3147)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3188)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3202)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3203)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-384 (A3156)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3187)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3193)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3210)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3186)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3185)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3147)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3188)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3202)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-512 (A3203)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3156)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3187)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3193)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3210)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3186)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3185)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3144)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3145)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-256 (A3148)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3175)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3146)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3173)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3174)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3144)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3145)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3148)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3175)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-512 (A3146)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3173)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3174)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-128 (A3144)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-128 (A3145)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-128 (A3148)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-128 (A3175)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-128 (A3146)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-128 (A3173)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHAKE-128 (A3174)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-256 (A3144)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-256 (A3145)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-256 (A3148)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-256 (A3175)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-256 (A3146)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-256 (A3173)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHAKE-256 (A3174)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
KDF SSH (A3171)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SSH (A3143)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3169)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3142)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3140)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3157)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3170)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3141)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3149)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3172)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TLS v1.2 KDF RFC7627 (A3147)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3188)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3202)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3203)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3156)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3187)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3193)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3210)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3186)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TLS v1.2 KDF RFC7627 (A3185)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
KDA HKDF Sp800-56Cr1 (A3139)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Test runs at power-on before the integrity test
KDA HKDF Sp800-56Cr1 (A3168)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Test runs at power-on before the integrity test
RSA KeyGen (FIPS186-4) (A3147)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3188)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3202)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3203)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3156)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3187)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3193)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA KeyGen (FIPS186-4) (A3210)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3186)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3185)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3147)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3188)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3202)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3203)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3156)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3187)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA KeyGen (FIPS186-4) (A3193)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3210)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3186)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3185)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
KAS-FFC-SSC Sp800-56Ar3 (A3211) - PCT	N/A	PCT	PCT	Module becomes operational	PCT according to SP 800-56A Rev. 3, Section 5.6.2.1.4	Key pair generation
KAS-FFC-SSC Sp800-56Ar3 (A3207) - PCT	N/A	PCT	PCT	Module becomes operational	PCT according to SP 800-56A Rev. 3, Section 5.6.2.1.4	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 (A3147)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3156)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3161)	MAC tag verification	SW/FW Integrity	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3185)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3186)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3187)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3188)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3193)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3202)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3203)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3210)	MAC tag verification	SW/FW Integrity	On Demand	Manually

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3171) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3162) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3150) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3143) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3169) - Encryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3142) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3140) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3157) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3170) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3154) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3166) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3141) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3163) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3138) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3136) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3165) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3160) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3149) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3167) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3172) - Encryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3137) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3158) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3171) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3162) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3150) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3143) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3169) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3142) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3140) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3157) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3170) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3154) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3166) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3141) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3163) - Decryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3138) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3136) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3165) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3160) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3149) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3167) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3172) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3137) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3158) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3162) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3150) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3154) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3166) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3163) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3138) - Encryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM (A3136) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3165) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3160) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3167) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3137) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3158) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3162) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3150) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3154) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3166) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3163) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3138) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3136) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3165) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3160) - Decryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM (A3167) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3137) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3158) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3199) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3206) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3190) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3183) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3196) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3181) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3153) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3151) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3205) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3179) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3182) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3201) - Encryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3204) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3152) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3176) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3194) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3155) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3197) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3180) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3159) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3198) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3184) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3195) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3177) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3200) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3178) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3199) - Decryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3206) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3190) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3183) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3196) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3181) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3153) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3151) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3205) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3179) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3182) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3201) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3204) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3152) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3176) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3194) - Decryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3155) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3197) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3180) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3159) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3198) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3184) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3195) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3177) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3200) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3178) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3163) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3137) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3136) - Encryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0 (A3162) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3138) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3154) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3158) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3166) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3167) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3165) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3160) - Encryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3150) - Encryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0 (A3163) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3137) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3136) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3162) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3138) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3154) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3158) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3166) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3167) - Decryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0 (A3165) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3160) - Decryption	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3150) - Decryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3162) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3150) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3154) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3166) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3163) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3138) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3136) - Encryption	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CMAC (A3165) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3160) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3167) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3137) - Encryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3158) - Encryption	KAT	CAST	On Demand	Manually
Counter DRBG (A3162)	KAT	CAST	On Demand	Manually
Counter DRBG (A3150)	KAT	CAST	On Demand	Manually
Counter DRBG (A3154)	KAT	CAST	On Demand	Manually
Counter DRBG (A3166)	KAT	CAST	On Demand	Manually
Counter DRBG (A3163)	KAT	CAST	On Demand	Manually
Counter DRBG (A3138)	KAT	CAST	On Demand	Manually
Counter DRBG (A3136)	KAT	CAST	On Demand	Manually
Counter DRBG (A3165)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A3160)	KAT	CAST	On Demand	Manually
Counter DRBG (A3167)	KAT	CAST	On Demand	Manually
Counter DRBG (A3137)	KAT	CAST	On Demand	Manually
Counter DRBG (A3158)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3211) - KAT	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3207) - KAT	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3147)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3188)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3202)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3203)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3156)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3187)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC Sp800-56Ar3 (A3193)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3210)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3186)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3185)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3147)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3188)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3144)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3145)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3148)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3202)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3203)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-4) (A3156)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3175)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3146)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3173)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3187)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3193)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3210)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3186)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3185)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3174)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3147)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A3188)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3144)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3145)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3148)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3202)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3203)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3156)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3175)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3146)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3173)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3187)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A3193)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3210)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3186)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3185)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3174)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3147)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3188)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3202)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3203)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3156)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3187)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3193)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3210)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A3186)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3185)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3147)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3188)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3202)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3203)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3156)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3187)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3193)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3210)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3186)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3185)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3147)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3188)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3202)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3203)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3161)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3156)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3187)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3193)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3210)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3186)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3185)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3147)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3188)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3202)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3203)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3156)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3187)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3193)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-384 (A3210)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3186)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3185)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3147)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3188)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3202)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3203)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3156)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3187)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3193)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3210)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3186)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3185)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3144)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3145)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA3-224 (A3148)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3175)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3146)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3173)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3174)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3144)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3145)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3148)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3175)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3146)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3173)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3174)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3144)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3145)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3148)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA3-384 (A3175)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3146)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3173)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3174)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3144)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3145)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3148)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3175)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3146)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3173)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3174)	KAT	CAST	On Demand	Manually
PBKDF (A3147)	KAT	CAST	On Demand	Manually
PBKDF (A3188)	KAT	CAST	On Demand	Manually
PBKDF (A3144)	KAT	CAST	On Demand	Manually
PBKDF (A3145)	KAT	CAST	On Demand	Manually
PBKDF (A3148)	KAT	CAST	On Demand	Manually
PBKDF (A3202)	KAT	CAST	On Demand	Manually
PBKDF (A3203)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
PBKDF (A3156)	KAT	CAST	On Demand	Manually
PBKDF (A3175)	KAT	CAST	On Demand	Manually
PBKDF (A3146)	KAT	CAST	On Demand	Manually
PBKDF (A3173)	KAT	CAST	On Demand	Manually
PBKDF (A3187)	KAT	CAST	On Demand	Manually
PBKDF (A3193)	KAT	CAST	On Demand	Manually
PBKDF (A3210)	KAT	CAST	On Demand	Manually
PBKDF (A3186)	KAT	CAST	On Demand	Manually
PBKDF (A3185)	KAT	CAST	On Demand	Manually
PBKDF (A3174)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3147) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3188) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3202) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3203) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3156) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-4) (A3187) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3193) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3210) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3186) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3185) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3147) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3188) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3202) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3203) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A3156) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3187) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3193) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3210) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3186) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3185) - PKCS#1 v1.5	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3147) - PSS	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3188) - PSS	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3202) - PSS	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3203) - PSS	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-4) (A3156) - PSS	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3187) - PSS	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3193) - PSS	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3210) - PSS	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3186) - PSS	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3185) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3147) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3188) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3202) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3203) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3156) - PSS	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A3187) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3193) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3210) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3186) - PSS	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3185) - PSS	KAT	CAST	On Demand	Manually
SHA-1 (A3147)	KAT	CAST	On Demand	Manually
SHA-1 (A3188)	KAT	CAST	On Demand	Manually
SHA-1 (A3202)	KAT	CAST	On Demand	Manually
SHA-1 (A3203)	KAT	CAST	On Demand	Manually
SHA-1 (A3156)	KAT	CAST	On Demand	Manually
SHA-1 (A3187)	KAT	CAST	On Demand	Manually
SHA-1 (A3193)	KAT	CAST	On Demand	Manually
SHA-1 (A3210)	KAT	CAST	On Demand	Manually
SHA-1 (A3186)	KAT	CAST	On Demand	Manually
SHA-1 (A3185)	KAT	CAST	On Demand	Manually
SHA2-224 (A3147)	KAT	CAST	On Demand	Manually
SHA2-224 (A3188)	KAT	CAST	On Demand	Manually
SHA2-224 (A3202)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-224 (A3203)	KAT	CAST	On Demand	Manually
SHA2-224 (A3156)	KAT	CAST	On Demand	Manually
SHA2-224 (A3187)	KAT	CAST	On Demand	Manually
SHA2-224 (A3193)	KAT	CAST	On Demand	Manually
SHA2-224 (A3210)	KAT	CAST	On Demand	Manually
SHA2-224 (A3186)	KAT	CAST	On Demand	Manually
SHA2-224 (A3185)	KAT	CAST	On Demand	Manually
SHA2-256 (A3147)	KAT	CAST	On Demand	Manually
SHA2-256 (A3188)	KAT	CAST	On Demand	Manually
SHA2-256 (A3202)	KAT	CAST	On Demand	Manually
SHA2-256 (A3203)	KAT	CAST	On Demand	Manually
SHA2-256 (A3161)	KAT	CAST	On Demand	Manually
SHA2-256 (A3156)	KAT	CAST	On Demand	Manually
SHA2-256 (A3187)	KAT	CAST	On Demand	Manually
SHA2-256 (A3193)	KAT	CAST	On Demand	Manually
SHA2-256 (A3210)	KAT	CAST	On Demand	Manually
SHA2-256 (A3186)	KAT	CAST	On Demand	Manually
SHA2-256 (A3185)	KAT	CAST	On Demand	Manually
SHA2-384 (A3147)	KAT	CAST	On Demand	Manually
SHA2-384 (A3188)	KAT	CAST	On Demand	Manually
SHA2-384 (A3202)	KAT	CAST	On Demand	Manually
SHA2-384 (A3203)	KAT	CAST	On Demand	Manually
SHA2-384 (A3156)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-384 (A3187)	KAT	CAST	On Demand	Manually
SHA2-384 (A3193)	KAT	CAST	On Demand	Manually
SHA2-384 (A3210)	KAT	CAST	On Demand	Manually
SHA2-384 (A3186)	KAT	CAST	On Demand	Manually
SHA2-384 (A3185)	KAT	CAST	On Demand	Manually
SHA2-512 (A3147)	KAT	CAST	On Demand	Manually
SHA2-512 (A3188)	KAT	CAST	On Demand	Manually
SHA2-512 (A3202)	KAT	CAST	On Demand	Manually
SHA2-512 (A3203)	KAT	CAST	On Demand	Manually
SHA2-512 (A3156)	KAT	CAST	On Demand	Manually
SHA2-512 (A3187)	KAT	CAST	On Demand	Manually
SHA2-512 (A3193)	KAT	CAST	On Demand	Manually
SHA2-512 (A3210)	KAT	CAST	On Demand	Manually
SHA2-512 (A3186)	KAT	CAST	On Demand	Manually
SHA2-512 (A3185)	KAT	CAST	On Demand	Manually
SHA3-256 (A3144)	KAT	CAST	On Demand	Manually
SHA3-256 (A3145)	KAT	CAST	On Demand	Manually
SHA3-256 (A3148)	KAT	CAST	On Demand	Manually
SHA3-256 (A3175)	KAT	CAST	On Demand	Manually
SHA3-256 (A3146)	KAT	CAST	On Demand	Manually
SHA3-256 (A3173)	KAT	CAST	On Demand	Manually
SHA3-256 (A3174)	KAT	CAST	On Demand	Manually
SHA3-512 (A3144)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-512 (A3145)	KAT	CAST	On Demand	Manually
SHA3-512 (A3148)	KAT	CAST	On Demand	Manually
SHA3-512 (A3175)	KAT	CAST	On Demand	Manually
SHA3-512 (A3146)	KAT	CAST	On Demand	Manually
SHA3-512 (A3173)	KAT	CAST	On Demand	Manually
SHA3-512 (A3174)	KAT	CAST	On Demand	Manually
SHAKE-128 (A3144)	KAT	CAST	On Demand	Manually
SHAKE-128 (A3145)	KAT	CAST	On Demand	Manually
SHAKE-128 (A3148)	KAT	CAST	On Demand	Manually
SHAKE-128 (A3175)	KAT	CAST	On Demand	Manually
SHAKE-128 (A3146)	KAT	CAST	On Demand	Manually
SHAKE-128 (A3173)	KAT	CAST	On Demand	Manually
SHAKE-128 (A3174)	KAT	CAST	On Demand	Manually
SHAKE-256 (A3144)	KAT	CAST	On Demand	Manually
SHAKE-256 (A3145)	KAT	CAST	On Demand	Manually
SHAKE-256 (A3148)	KAT	CAST	On Demand	Manually
SHAKE-256 (A3175)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHAKE-256 (A3146)	KAT	CAST	On Demand	Manually
SHAKE-256 (A3173)	KAT	CAST	On Demand	Manually
SHAKE-256 (A3174)	KAT	CAST	On Demand	Manually
KDF SSH (A3171)	KAT	CAST	On Demand	Manually
KDF SSH (A3143)	KAT	CAST	On Demand	Manually
KDF SSH (A3169)	KAT	CAST	On Demand	Manually
KDF SSH (A3142)	KAT	CAST	On Demand	Manually
KDF SSH (A3140)	KAT	CAST	On Demand	Manually
KDF SSH (A3157)	KAT	CAST	On Demand	Manually
KDF SSH (A3170)	KAT	CAST	On Demand	Manually
KDF SSH (A3141)	KAT	CAST	On Demand	Manually
KDF SSH (A3149)	KAT	CAST	On Demand	Manually
KDF SSH (A3172)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3147)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3188)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3202)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3203)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3156)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3187)	KAT	CAST	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
TLS v1.2 KDF RFC7627 (A3193)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3210)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3186)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3185)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A3139)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A3168)	KAT	CAST	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3147)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3188)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3202)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3203)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3156)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3187)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3193)	PCT	PCT	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA KeyGen (FIPS186-4) (A3210)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3186)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3185)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3147)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3188)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3202)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3203)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3156)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3187)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3193)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3210)	PCT	PCT	On Demand	Manually

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-4) (A3186)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3185)	PCT	PCT	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3211) - PCT	PCT	PCT	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3207) - PCT	PCT	PCT	On Demand	Manually

Table 25: Conditional Periodic Information

10.4 Error States

When the module fails the pre-operational self-test or any conditional test, the module returns an error code to indicate the error and enters the “Abort” error state, showing the following message to stderr: “OpenSSL internal error, assertion failed: FATAL FIPS SELFTEST FAILURE” and stops functioning. The only way to recover from this error is to restart the application. If the failure persists, the module must be reinstalled.

When a PCT fails during conditional tests, the module returns an error code to indicate the error and enters the “Error” error state. Any further cryptographic operation is inhibited. The calling application can obtain the module state by requesting the “Show status” service by calling the FIPS_selftest_failed() API function. The function returns 1 if the module is in the “Error” state, 0 if the module is in the Operational state.

Some cryptographic services cannot handle the return value of the “Error” state, and when the module is in that state and receives a service request, shows an error message and transitions to the “Abort” state, showing the following message to stderr: “OpenSSL internal error, assertion failed: FATAL FIPS SELFTEST FAILURE” and stops functioning. The only way to recover from this error is to restart the application.

The following table shows the error codes and the corresponding condition:

Name	Description	Conditions	Recovery Method	Indicator
Abort	Module abort: the module immediately stops functioning and ends the	Integrity test failure Any CAST failure Module is in error state and one of the following cryptographic services is	Module reinitialization	Message to stderr: "OpenSSL internal error, assertion failed: FATAL

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Conditions	Recovery Method	Indicator
	application process.	invoked: Message Digest, Encryption/Decryption, Diffie-Hellman		FIPS SELFTEST FAILURE". Module does not load.
Error	Module error: an error has occured, but the module has not yet reset.	Any PCT failure Module is in error state and a cryptographic service other than the following is invoked: Message Digest, Encryption/Decryption, Diffie-Hellman	Module reinitialization	FIPS_selftest_failed() returns 1. The module returns an error code and stops functioning. Any cryptographic operation is inhibited.

Table 26: Error States

In the “Error” state, errors are reported through the regular ERR interface of the modules and can be queried by functions such as ERR_get_error(). See the OpenSSL man pages for the function description.

10.5 Operator Initiation of Self-Tests

Both conditional and pre-operational self-tests can be executed on-demand by unloading and subsequently re-initializing the module, or by calling the OSSL_PROVIDER_self_test function. The pair-wise consistency tests can be invoked on demand by requesting the key pair generation service.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Module Installation

The Crypto Officer can install the RPM packages containing the module as listed in Section 2.2 using the zypper tool as follows:

```
# zypper install libopenssl1_1
# zypper install libopenssl1_1-hmac
```

If the use of certified 32-bit Openssl libraries on Intel x86 is required, then use the following to install the 32bit libraries and hmac packages:

```
# zypper install libopenssl1_1-32bit
# zypper install libopenssl1_1-hmac-32bit
```

The integrity of the RPM package is automatically verified during the installation, and the Crypto Officer shall not install the RPM package if there is any integrity error.

11.1.2 Operating Environment Configuration

The operating environment needs to be configured to support the approved mode of operation, so the following steps shall be performed with the root privilege:

1. Install the dracut-fips RPM package:

```
# zypper install dracut-fips
```

2. Recreate the INITRAMFS image:

```
# dracut -f
```

3. After regenerating the initrd, the Crypto Officer has to append the following parameter in the /etc/default/grub configuration file in the GRUB_CMDLINE_LINUX_DEFAULT line:

```
fips=1
```

4. After editing the configuration file, please run the following command to change the setting in the boot loader:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

If /boot or /boot/efi resides on a separate partition, the kernel parameter boot=<partition of /boot or /boot/efi> must be supplied. The partition can be identified with the command "df /boot" or "df /boot/efi" respectively. For example:

```
# df /boot
Filesystem     1K-blocks     Used     Available     Use%     Mounted on
/dev/sda1      233191        30454    190296        14%                  /boot
```

The partition of /boot is located on /dev/sda1 in this example. Therefore, the following string needs to be appended in the aforementioned grub file:

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

"boot=/dev/sda1"

5. Reboot to apply these settings.

Now, the operating environment is configured to support the approved mode of operation. The Crypto Officer should check the existence of the file /proc/sys/crypto/fips_enabled, and verify it contains a numeric value “1”. If the file does not exist or does not contain “1”, the operating environment is not configured to support the approved mode of operation and the module will not operate as a FIPS validated module properly.

11.1.3 Module Installation for Vendor Affirmed Platforms

The following table includes the information on module installation process for the vendor affirmed platforms that are listed in Section 2.2.

Product	Link
SUSE Linux Enterprise Micro 5.3	https://documentation.suse.com/sle-micro/5.3/single-html/SLE-Micro-security/#sec-fips-slemicro-install
SUSE Linux Enterprise Server for SAP 15SP4	https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-security.html
SUSE Linux Enterprise Base Container Image 15SP4	https://documentation.suse.com/smart/linux/html/concept-bci/index.html
SUSE Linux Enterprise Desktop 15SP4	https://documentation.suse.com/sled/15-SP4/html/SLED-all/book-security.html
SUSE Linux Enterprise Real Time 15SP4	https://documentation.suse.com/sle-rt/15-SP4

Table 27 - Installation for Vendor Affirmed Platforms

Note: Per section 7.9 in the FIPS 140-3 Management Manual, the Cryptographic Module Validation Program (CMVP) makes no statement as to the correct operation of the module or the security strengths of the generated keys when this module is ported and executed in an operational environment not listed on the validation certificate.

11.2 Administrator Guidance

The binaries of the module are contained in the RPM packages for delivery. The Crypto Officer shall follow section 11.1.1 and 11.1.2 to configure the operational environment and install the module to be operated as a FIPS 140-3 validated module.

Section 2.2 lists the RPM packages that contain the FIPS validated module and the OE directory where the components are installed. The "Show module name and version" service returns the value "OpenSSL 1.1.11 24 Aug 2021 SUSE release 150400.7.81.1”, which matches the version included in the RPM package filenames.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11.2.1 Environment Variables

OPENSSL_ENFORCE_MODULUS_BITS

Setting the environment variable OPENSSL_ENFORCE_MODULUS_BITS can restrict the module to only generate the acceptable key sizes of RSA. If the environment variable is set, the module enforces the generation of keys of 2048 bits or more.

Notice that even if this environment variable is not set, the module will provide the corresponding value of the service indicator depending on the size of the key generated.

11.3 Non-Administrator Guidances

No non-administrator guidance is provided.

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.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

12.1 Attack List

The module implements blinding against RSA timing attacks.

RSA is vulnerable to timing attacks. In a setup where attackers can measure the time of RSA decryption or signature operations, blinding must be used to protect the RSA operation from that attack.

The module provides the API functions RSA_blinding_on() and RSA_blinding_off() to turn the blinding on and off for RSA. When the blinding is on, the module generates a random value to form a blinding factor in the RSA key before the RSA key is used in the RSA cryptographic operations.

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix A. TLS Cipher Suites

The module supports the following cipher suites for the TLS protocol versions 1.2 and 1.3 compliant with section 3.3.1 of SP 800-52 Rev. 2. 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 }	RFC 3268
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	{ 0x00, 0x33 }	RFC 3268
TLS_DH_RSA_WITH_AES_256_CBC_SHA	{ 0x00, 0x37 }	RFC 3268
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	{ 0x00, 0x39 }	RFC 3268
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	{ 0x00,0x3F }	RFC 5246
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	{ 0x00,0x67 }	RFC 5246
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	{ 0x00,0x69 }	RFC 5246
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	{ 0x00,0x6B }	RFC 5246
TLS_PSK_WITH_AES_128_CBC_SHA	{ 0x00, 0x8C }	RFC 4279
TLS_PSK_WITH_AES_256_CBC_SHA	{ 0x00, 0x8D }	RFC 4279
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	{ 0x00, 0x9E }	RFC 5288
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	{ 0x00, 0x9F }	RFC 5288
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	{ 0x00, 0xA0 }	RFC 5288
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	{ 0x00, 0xA1 }	RFC 5288
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	{ 0xC0, 0x04 }	RFC 4492
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	{ 0xC0, 0x05 }	RFC 4492
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	{ 0xC0, 0x09 }	RFC 4492
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	{ 0xC0, 0x0A }	RFC 4492
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	{ 0xC0, 0x0E }	RFC 4492
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	{ 0xC0, 0x0F }	RFC 4492
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	{ 0xC0, 0x13 }	RFC 4492
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	{ 0xC0, 0x14 }	RFC 4492
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	{ 0xC0, 0x23 }	RFC 5289

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Cipher Suite	ID	Reference
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	{ 0xC0, 0x24 }	RFC 5289
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	{ 0xC0, 0x25 }	RFC 5289
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	{ 0xC0, 0x26 }	RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	{ 0xC0, 0x27 }	RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	{ 0xC0, 0x28 }	RFC 5289
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	{ 0xC0, 0x29 }	RFC 5289
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	{ 0xC0, 0x2A }	RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	{ 0xC0, 0x2B }	RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	{ 0xC0, 0x2C }	RFC 5289
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	{ 0xC0, 0x2D }	RFC 5289
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	{ 0xC0, 0x2E }	RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	{ 0xC0, 0x2F }	RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	{ 0xC0, 0x30 }	RFC 5289
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	{ 0xC0, 0x31 }	RFC 5289
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	{ 0xC0, 0x32 }	RFC 5289
TLS_DHE_RSA_WITH_AES_128_CCM	{ 0xC0, 0x9E }	RFC 6655
TLS_DHE_RSA_WITH_AES_256_CCM	{ 0xC0, 0x9F }	RFC 6655
TLS_DHE_RSA_WITH_AES_128_CCM_8	{ 0xC0, 0xA2 }	RFC 6655
TLS_DHE_RSA_WITH_AES_256_CCM_8	{ 0xC0, 0xA3 }	RFC 6655
TLS_AES_128_GCM_SHA256	{ 0x13, 0x01 }	RFC 8446
TLS_AES_256_GCM_SHA384	{ 0x13, 0x02 }	RFC 8446
TLS_AES_128_CCM_SHA256	{ 0x13, 0x04 }	RFC 8446
TLS_AES_128_CCM_8_SHA256	{ 0x13, 0x05 }	RFC 8446

Table 28 - TLS Cipher Suites

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix B. Glossary and Abbreviations

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
CAST	Cryptographic Algorithm Self-Tests
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CPACF	Central Processor Assist for Cryptographic Function
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
FSM	Finite State Model
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
ISA	Instruction Set Architecture
KAS	Key Agreement Schema
KAT	Known Answer Test
KW	AES Key Wrap
KWP	AES Key Wrap with Padding
MAC	Message Authentication Code
NDF	No Derivation Function
NIST	National Institute of Science and Technology

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

OFB	Output Feedback
PAA	Processor Algorithm Acceleration
PAI	Processor Algorithm Implementation
PR	Prediction Resistance
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell
SSP	Sensitive Security Parameter
TDES	Triple-DES
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix C. References

FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
FIPS 140-3 IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** October 2024 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 140-3 MM	**FIPS 140-3 Cryptographic Module Validation Program Management Manual** May 2025 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual
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 800-38B	**Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://doi.org/10.6028/NIST.SP.800-38B
SP 800-38C	**Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality** May 2004 https://doi.org/10.6028/NIST.SP.800-38C
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.800-38D
SP 800-38E	**Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality of Storage Devices** January 2010 https://doi.org/10.6028/NIST.SP.800-38E
SP 800-38F	**Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** December 2012 https://doi.org/10.6028/NIST.SP.800-38F
FIPS 180-4	**Secure Hash Standard (SHS)** August 2015 https://doi.org/10.6028/NIST.FIPS.180-4

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://doi.org/10.6028/NIST.FIPS.202
FIPS 198-1	**The Keyed-Hash Message Authentication Code (HMAC)** July 2008 https://doi.org/10.6028/NIST.FIPS.198-1
FIPS 186-4	**Digital Signature Standard (DSS)** July 2013 https://doi.org/10.6028/NIST.FIPS.186-4
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 800-56A 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 800-135 Rev. 1	**Recommendation for Existing Application-Specific Key Derivation Functions** December 2011 https://doi.org/10.6028/NIST.SP.800-135r1
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 800-133 Rev. 2	**Recommendation for Cryptographic Key Generation** June 2020 https://doi.org/10.6028/NIST.SP.800-133r2
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

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** February 2003 https://www.ietf.org/rfc/rfc3447.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 4253	**The Secure Shell (SSH) Transport Layer Protocol** June 2006 https://www.ietf.org/rfc/rfc4253.txt
RFC 5288	**AES Galois Counter Mode (GCM) Cipher Suites for TLS** August 2008 https://www.ietf.org/rfc/rfc5288.txt
RFC 6668	**SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol** July 2012 https://www.ietf.org/rfc/rfc6668.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

© 2026 SUSE, LLC / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.