

SUSE LLC

SUSE Linux Enterprise Kernel Crypto API Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Version 1.4

Last update: 2026-07-31

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

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 9
2.4 Modes of Operation 9
2.5 Algorithms 10
2.6 Security Function Implementations 15
2.7 Algorithm Specific Information 20
2.7.1 AES XTS 20
2.7.2 AES GCM IV 20
2.7.3 SP 800-56A Rev. 3 Assurances 20
2.7.4 Key Transport 20
2.7.5 Key Agreement 21
2.7.6 SHA-1 Usage 21
2.8 RBG and Entropy 21
2.9 Key Generation 22
2.10 Key Establishment 22
2.11 Industry Protocols 22
3 Cryptographic Module Interfaces 23
3.1 Ports and Interfaces 23
4 Roles, Services, and Authentication 24
4.1 Authentication Methods 24
4.2 Roles 24
4.3 Approved Services 24
4.4 Non-Approved Services 31
4.5 External Software/Firmware Loaded 31
5 Software/Firmware Security 32
5.1 Integrity Techniques 32
5.2 Initiate on Demand 32
6 Operational Environment 33
6.1 Operational Environment Type and Requirements 33
6.2 Configuration Settings and Restrictions 33
7 Physical Security 34
8 Non-Invasive Security 35
9 Sensitive Security Parameters Management 36
9.1 Storage Areas 36
9.2 SSP Input-Output Methods 36
9.3 SSP Zeroization Methods 36
9.4 SSPs 37
9.5 Transitions 42
10 Self-Tests 43
10.1 Pre-Operational Self-Tests 43
10.2 Conditional Self-Tests 44

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

10.3 Periodic Self-Test Information 103
10.4 Error States 132
10.5 Operator Initiation of Self-Tests 132
11 Life-Cycle Assurance 133
11.1 Installation, Initialization, and Startup Procedures 133
11.1.1 Module Installation 133
11.1.2 Operating Environment Configuration 133
11.1.3 Module Installation for Vendor Affirmed Platforms 134
11.2 Administrator Guidance 134
11.3 Non-Administrator Guidances 134
11.4 End of Life 134
12 Mitigation of Other Attacks 135
12.1 Attack List 135
Appendix A. Glossary and Abbreviations 136
Appendix B. References 138

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

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 7
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 8
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 9
Table 5: Modes List and Description 9
Table 6: Approved Algorithms 14
Table 7: Non-Approved, Not Allowed Algorithms 15
Table 8: Security Function Implementations 20
Table 9: Entropy Certificates 21
Table 10: Entropy Sources 21
Table 11: Ports and Interfaces 23
Table 12: Roles 24
Table 13: Approved Services 31
Table 14: Non-Approved Services 31
Table 15: Storage Areas 36
Table 16: SSP Input-Output Methods 36
Table 17: SSP Zeroization Methods 36
Table 18: SSP Table 1 40
Table 19: SSP Table 2 42
Table 20: Pre-Operational Self-Tests 44
Table 21: Conditional Self-Tests 103
Table 22: Pre-Operational Periodic Information 103
Table 23: Conditional Periodic Information 132
Table 24: Error States 132
Table 25 - Installation for Vendor Affirmed Platforms 134
Table 26 – RPM packages 134

List of Figures

Figure 1 - Cryptographic boundary 6

© 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 versions 3.3 and 3.4 of the SUSE Linux Enterprise Kernel Crypto API 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	N/A
	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 Kernel Crypto API 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 static kernel binary, kernel object files, the fipscheck application, and the corresponding HMAC files for integrity. Note that the kernel object files do not have associated HMAC 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).

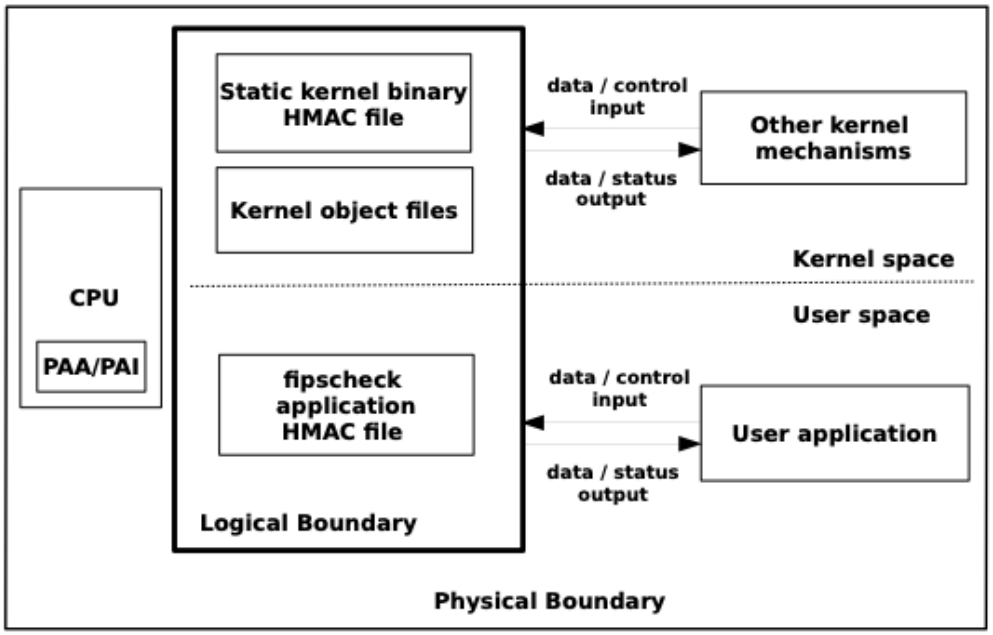


Figure 1 - Cryptographic boundary

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

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
/boot/vmlinuz-5.14.21-150400.24.46-default, /boot/.vmlinuz-5.14.21-150400.24.46-default.hmac, /lib/modules/5.14.21-150400.24.46-default/kernel/crypto/*.ko, /lib/modules/5.14.21-150400.24.46-default/kernel/arch/x86/crypto/*.ko, /usr/lib64/libkcapi/fipscheck, /usr/lib64/libkcapi/fipscheck.hmac on SUSE Linux Enterprise Server 15 SP4 and Intel® Xeon® Silver 4215R or AMD EPYC(TM) 7371	3.3	N/A	HMAC-SHA2-256 (static kernel binary, fipscheck application), RSA SigVer with 2048-bit key (kernel object files)
/boot/vmlinuz-5.14.21-150400.15.11-rt, /boot/.vmlinuz-5.14.21-150400.15.11-rt.hmac, /lib/modules/5.14.21-150400.15.11-rt/kernel/crypto/*.ko, /lib/modules/5.14.21-150400.15.11-rt/kernel/arch/x86/crypto/*.ko, /usr/lib64/libkcapi/fipscheck, /usr/lib64/libkcapi/fipscheck.hmac on SUSE Linux Enterprise Server 15 SP4 and Intel® Xeon® Silver 4215R or AMD EPYC(TM) 7371	3.4	N/A	HMAC-SHA2-256 (static kernel binary, fipscheck application), RSA SigVer with 2048-bit key (kernel object files)
/boot/Image-5.14.21-150400.24.46-default, /boot/.Image-5.14.21-150400.24.46-default.hmac, /lib/modules/5.14.21-150400.24.46-default/kernel/crypto/*.ko, /lib/modules/5.14.21-150400.24.46-default/kernel/arch/arm64/crypto/*.ko, /usr/lib64/libkcapi/fipscheck, /usr/lib64/libkcapi/fipscheck.hmac on SUSE Linux Enterprise Server 15 SP4 and ARM Ampere® Altra® Q80-30	3.3	N/A	HMAC-SHA2-256 (static kernel binary, fipscheck application), RSA SigVer with 2048-bit key (kernel object files)
/boot/vmlinuz-5.14.21-150400.24.46-default, /boot/.vmlinuz-5.14.21-150400.24.46-default.hmac, /lib/modules/5.14.21-150400.24.46-default/kernel/crypto/*.ko, /lib/modules/5.14.21-150400.24.46-default/kernel/arch/powerpc/crypto/*.ko, /usr/lib64/libkcapi/fipscheck, /usr/lib64/libkcapi/fipscheck.hmac on SUSE Linux Enterprise Server 15 SP4 on PowerVM (VIOS 3.1.4.00) and Power10	3.3	N/A	HMAC-SHA2-256 (static kernel binary, fipscheck application), RSA SigVer with 2048-bit key (kernel object files)
/boot/image-5.14.21-150400.24.46-default, /boot/.image-5.14.21-150400.24.46-default.hmac, /lib/modules/5.14.21-150400.24.46-default/kernel/crypto/*.ko, /lib/modules/5.14.21-150400.24.46-default/kernel/arch/s390/crypto/*.ko, /usr/lib64/libkcapi/fipscheck, /usr/lib64/libkcapi/fipscheck.hmac on SUSE Linux Enterprise Server 15 SP4 and z15	3.3	N/A	HMAC-SHA2-256 (static kernel binary, fipscheck application), RSA SigVer with 2048-bit key (kernel object files)

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

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

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

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	3.3 3.4
SUSE Linux Enterprise Server 15 SP4	GIGABYTE R181-Z90-00	AMD EPYC(TM) 7371	Yes	N/A	3.3 3.4
SUSE Linux Enterprise Server 15 SP4	GIGABYTE G242-P32-QZ	ARM Ampere® Altra® Q80-30	Yes	N/A	3.3
SUSE Linux Enterprise Server 15 SP4	IBM z/15	IBM z15	Yes	N/A	3.3
SUSE Linux Enterprise Server 15 SP4	IBM Power E1080 (9080-HEX)	IBM Power10	Yes	PowerVM (VIOS 3.1.4.00)	3.3
SUSE Linux Enterprise Server 15 SP4	Supermicro Super Server SYS-6019P-WTR	Intel® Xeon® Silver 4215R	No	N/A	3.3 3.4
SUSE Linux Enterprise Server 15 SP4	GIGABYTE R181-Z90-00	AMD EPYC(TM) 7371	No	N/A	3.3 3.4
SUSE Linux Enterprise Server 15 SP4	GIGABYTE G242-P32-QZ	ARM Ampere® Altra® Q80-30	No	N/A	3.3
SUSE Linux Enterprise Server 15 SP4	IBM z/15	IBM z15	No	N/A	3.3
SUSE Linux Enterprise Server 15 SP4	IBM Power E1080 (9080-HEX)	IBM Power10	No	PowerVM (VIOS 3.1.4.00)	3.3

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

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

Operating System	Hardware Platform
SUSE Linux Enterprise Server 15SP4 [Version 3.3]	IBM LinuxONE III LT1 [IBM z15]
SUSE Linux Enterprise Micro 5.3 [Versions 3.3 and 3.4]	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 Micro 5.3 [Versions 3.3 and 3.4]	GIGABYTE R181-Z90-00 [AMD EPYC(TM) 7371]
SUSE Linux Enterprise Micro 5.3 [Version 3.3]	GIGABYTE G242-P32-QZ [ARM Ampere® Altra® Q80-30]
SUSE Linux Enterprise Micro 5.3 [Version 3.3]	IBM z/15 [IBM z15]
SUSE Linux Enterprise Micro 5.3 [Version 3.3]	IBM LinuxONE III LT1 [IBM z15]
SUSE Linux Enterprise Server for SAP 15SP4 [Version 3.3]	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Server for SAP 15SP4 [Version 3.3]	GIGABYTE R181-Z90-00 [AMD EPYC(TM) 7371]
SUSE Linux Enterprise Server for SAP 15SP4 on PowerVM (VIOS 3.1.4.00) [Version 3.3]	IBM Power E1080 (9080-HEX) [IBM Power10]
SUSE Linux Enterprise Desktop 15SP4 [Version 3.3]	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Desktop 15SP4 [Version 3.3]	GIGABYTE R181-Z90-00 [AMD EPYC(TM) 7371]
SUSE Linux Enterprise Real Time 15SP4 [Version 3.4]	Supermicro Super Server SYS-6019P-WTR [Intel® Xeon® Silver 4215R]
SUSE Linux Enterprise Real Time 15SP4 [Version 3.4]	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:

Mode Name	Description	Types of Services	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-

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

approved mode by calling one of the non-approved services listed in the Non-Approved Services table in Section 4.3 of this 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	A3045, A3053, A3061, A3064, A3075, A3078, A3090, A3098, A3106, A3109, A3125, A3128, A3131	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3050, A3059, A3070, A3084, A3095, A3104, A3115, A3128	Direction - decrypt, encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128-65536 Increment 8	SP 800-38A
AES-CCM	A3045, A3053, A3064, A3075, A3078, A3090, A3098, A3109, A3125, A3128	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CFB128	A3048, A3057, A3068, A3082, A3093, A3102, A3113, A3128	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3045, A3053, A3064, A3075, A3078, A3090, A3098, A3109, A3125, A3128	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	A3045, A3053, A3061, A3064, A3075, A3078, A3090, A3098, A3106, A3109, A3125, A3128, A3131	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	A3043, A3044, A3045, A3051, A3052, A3053, A3055, A3056, A3061, A3062,	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
	A3063, A3064, A3065, A3066, A3075, A3076, A3077, A3078, A3079, A3080, A3088, A3089, A3090, A3096, A3097, A3098, A3100, A3101, A3106, A3107, A3108, A3109, A3110, A3111, A3125, A3128, A3129, A3130, A3131		
AES-GCM	A3045, A3053, A3064, A3075, A3078, A3090, A3098, A3109, A3128	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.2 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128-65536 Increment 128 AAD Length - AAD Length: 128, 256, 120, 0	SP 800-38D
AES-GCM	A3051, A3055, A3062, A3065, A3076, A3079, A3096, A3100, A3107, A3110, A3129	Direction - Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 64, 96	SP 800-38D
AES-GCM	A3052, A3056, A3061, A3063, A3066, A3077, A3080, A3097, A3101, A3106, A3108, A3111, A3130	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.2 Key Length - 128, 192, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 64, 96	SP 800-38D
AES-KW	A3046, A3054, A3067, A3081, A3091, A3099, A3112, A3128	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 128	SP 800-38F
AES-OFB	A3049, A3058, A3069, A3083, A3094, A3103, A3114, A3128	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3045, A3053, A3061, A3064, A3075, A3078, A3090, A3098, A3106, A3109, A3125, A3128, A3131	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex	SP 800-38E

© 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
		Data Unit Length Matches Payload Length - Yes	
Counter DRBG	A3043, A3044, A3045, A3051, A3052, A3053, A3055, A3056, A3061, A3062, A3063, A3064, A3065, A3066, A3075, A3076, A3077, A3078, A3079, A3080, A3088, A3089, A3090, A3096, A3097, A3098, A3100, A3101, A3106, A3107, A3108, A3109, A3110, A3111, A3128, A3129, A3130	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 128, Entropy Input: 192, Entropy Input: 256 Nonce - Nonce: 128, Nonce: 64 Personalization String Length - Personalization String Length: 0 Returned Bits - 1024, 4096, 512	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A3044, A3089	Curve - P-256, P-384 Secret Generation Mode - Testing Candidates	FIPS 186-4
Hash DRBG	A3043, A3044, A3045, A3051, A3052, A3053, A3055, A3056, A3061, A3062, A3063, A3064, A3065, A3066, A3071, A3072, A3073, A3076, A3077, A3078, A3079, A3080, A3088, A3089, A3090, A3096, A3097, A3098, A3100, A3101, A3106, A3107, A3108, A3109, A3110, A3111, A3116, A3117, A3118, A3129, A3130	Prediction Resistance - No, Yes Supports Reseed - No Mode - SHA-1, SHA2-256, SHA2-384, SHA2-512 Entropy Input - Entropy Input: 160, Entropy Input: 256 Nonce - Nonce: 160, Nonce: 256 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 320, 384	SP 800-90A Rev. 1
HMAC DRBG	A3043, A3044, A3045, A3051, A3052, A3053, A3055, A3056, A3061, A3062, A3063, A3064, A3065, A3066, A3071, A3072, A3073, A3076, A3077, A3078, A3079, A3080, A3088, A3089, A3090, A3096, A3097, A3098, A3100, A3101, A3106, A3107, A3108, A3109, A3110, A3111, A3116, A3117, A3118, A3129, A3130	Prediction Resistance - No, Yes Supports Reseed - No Mode - SHA-1, SHA2-256, SHA2-384, SHA2-512 Entropy Input - Entropy Input: 160, Entropy Input: 256 Nonce - Nonce: 160, Nonce: 256 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 320, 384	SP 800-90A Rev. 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-SHA-1	A3043, A3044, A3045, A3071, A3072, A3073, A3074, A3078, A3086, A3087, A3088, A3089, A3090, A3116, A3117, A3118, A3119, A3125	MAC - MAC: 160 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3043, A3044, A3045, A3071, A3072, A3073, A3074, A3078, A3087, A3088, A3089, A3090, A3116, A3117, A3118, A3119, A3125, A3131, A3132	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3043, A3044, A3045, A3071, A3072, A3073, A3074, A3078, A3087, A3088, A3089, A3090, A3116, A3117, A3118, A3119, A3125, A3131, A3132	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3043, A3044, A3045, A3071, A3072, A3073, A3078, A3088, A3089, A3090, A3116, A3117, A3118, A3127, A3132	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3043, A3044, A3045, A3071, A3072, A3073, A3078, A3088, A3089, A3090, A3116, A3117, A3118, A3127, A3132	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A3047, A3085, A3092, A3126	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A3047, A3085, A3092, A3126	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A3047, A3085, A3092, A3126	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A3047, A3085, A3092, A3126	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3044, A3089	Domain Parameter Generation Methods - P-256, P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A3043, A3088	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
RSA SigVer (FIPS186-4)	A3045, A3071, A3072, A3073, A3078, A3090, A3116, A3117, A3118	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096 Hash Pair -	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
		Hash Algorithm - SHA-1 Public Exponent Mode - Random	
Safe Primes Key Generation	A3043, A3088	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
SHA-1	A3043, A3044, A3045, A3071, A3072, A3073, A3074, A3078, A3086, A3087, A3088, A3089, A3090, A3116, A3117, A3118, A3119, A3125	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A3043, A3044, A3045, A3071, A3072, A3073, A3074, A3078, A3087, A3088, A3089, A3090, A3116, A3117, A3118, A3119, A3125, A3131, A3132	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A3043, A3044, A3045, A3071, A3072, A3073, A3074, A3078, A3087, A3088, A3089, A3090, A3116, A3117, A3118, A3119, A3125, A3131, A3132	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A3043, A3044, A3045, A3071, A3072, A3073, A3078, A3088, A3089, A3090, A3116, A3117, A3118, A3127, A3132	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A3043, A3044, A3045, A3071, A3072, A3073, A3078, A3088, A3089, A3090, A3116, A3117, A3118, A3127, A3132	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA3-224	A3047, A3085, A3092, A3126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-256	A3047, A3085, A3092, A3126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-384	A3047, A3085, A3092, A3126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-512	A3047, A3085, A3092, A3126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

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.

N/A for this module.

© 2026 SUSE, LLC / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

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	Symmetric encryption
AES-GMAC	Message authentication code (MAC)
RSA	RSA encryption primitive; RSA decryption primitive; RSA signature generation primitive; RSA signature verification primitive
ECDSA	ECDSA signature verification primitive

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric encryption	BC-UnAuth	Symmetric encryption		AES-CBC: (A3128, A3053, A3078, A3064, A3061, A3075, A3131, A3125, A3098, A3090, A3106, A3109, A3045) AES-CBC-CS3: (A3128, A3050, A3095, A3084, A3104, A3070, A3115, A3059) AES-CFB128: (A3093, A3128, A3057, A3068, A3048, A3082, A3102, A3113) AES-CTR: (A3128, A3053, A3078, A3064, A3061, A3075, A3131, A3125, A3098, A3090, A3106, A3109, A3045) AES-ECB: (A3128, A3053, A3080, A3051, A3078, A3062, A3096, A3052, A3064, A3063, A3100, A3079, A3066, A3089, A3065, A3061, A3076, A3043, A3097, A3075, A3088, A3044, A3129, A3131, A3125, A3111, A3110, A3107, A3077, A3108, A3098, A3090, A3055, A3130, A3101, A3106, A3056, A3109, A3045) AES-OFB: (A3058, A3128, A3094, A3114, A3083, A3069, A3049, A3103) AES-XTS Testing Revision 2.0: (A3128, A3053, A3078, A3064, A3061, A3075, A3131, A3125,

© 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
				A3098, A3090, A3106, A3109, A3045)
Symmetric decryption	BC-UnAuth	Symmetric decryption		AES-CBC: (A3128, A3053, A3078, A3064, A3061, A3075, A3131, A3125, A3098, A3090, A3106, A3109, A3045) AES-CBC-CS3: (A3128, A3050, A3095, A3084, A3104, A3070, A3115, A3059) AES-CFB128: (A3093, A3128, A3057, A3068, A3048, A3082, A3102, A3113) AES-CTR: (A3128, A3053, A3078, A3064, A3061, A3075, A3131, A3125, A3098, A3090, A3106, A3109, A3045) AES-ECB: (A3128, A3053, A3080, A3051, A3078, A3062, A3096, A3052, A3064, A3063, A3100, A3079, A3066, A3089, A3065, A3061, A3076, A3043, A3097, A3075, A3088, A3044, A3129, A3131, A3125, A3111, A3110, A3107, A3077, A3108, A3098, A3090, A3055, A3130, A3101, A3106, A3056, A3109, A3045) AES-OFB: (A3058, A3128, A3094, A3114, A3083, A3069, A3049, A3103) AES-XTS Testing Revision 2.0: (A3128, A3053, A3078, A3064, A3061, A3075, A3131, A3125, A3098, A3090, A3106, A3109, A3045)
Authenticated symmetric encryption	BC-Auth	Authenticated symmetric encryption		AES-CCM: (A3128, A3053, A3078, A3064, A3075, A3125, A3098, A3090, A3109, A3045) AES-GCM: (A3128, A3053, A3080, A3051, A3078, A3062, A3096, A3052, A3064, A3063, A3100, A3079, A3066, A3065, A3061, A3076, A3097, A3075, A3129, A3111, A3110, A3107, A3077, A3108, A3098, A3090, A3055, A3130, A3101, A3106, A3056, A3109, A3045)

© 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 decryption	BC-Auth	Authenticated symmetric decryption		AES-CCM: (A3128, A3053, A3078, A3064, A3075, A3125, A3098, A3090, A3109, A3045) AES-GCM: (A3128, A3053, A3080, A3051, A3078, A3062, A3096, A3052, A3064, A3063, A3100, A3079, A3066, A3065, A3061, A3076, A3097, A3075, A3129, A3111, A3110, A3107, A3077, A3108, A3098, A3090, A3055, A3130, A3101, A3106, A3056, A3109, A3045)
Message authentication code (MAC)	MAC	Message authentication code (MAC)		AES-CMAC: (A3128, A3053, A3078, A3064, A3075, A3125, A3098, A3090, A3109, A3045) HMAC-SHA-1: (A3078, A3119, A3086, A3117, A3087, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3125, A3073, A3090, A3072, A3074, A3045) HMAC-SHA2-224: (A3132, A3078, A3119, A3117, A3087, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3131, A3125, A3073, A3090, A3072, A3074, A3045) HMAC-SHA2-256: (A3132, A3078, A3119, A3117, A3087, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3131, A3125, A3073, A3090, A3072, A3074, A3045) HMAC-SHA2-384: (A3132, A3078, A3127, A3117, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3073, A3090, A3072, A3045) HMAC-SHA2-512: (A3132, A3078, A3127, A3117, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3073, A3090, A3072, A3045) HMAC-SHA3-224: (A3085, A3092, A3126, A3047) HMAC-SHA3-256: (A3085, A3092, A3126, A3047) HMAC-SHA3-384: (A3085,

© 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
				A3092, A3126, A3047) HMAC-SHA3-512: (A3085, A3092, A3126, A3047)
Key wrapping	BC-Auth	Key wrapping		AES-KW: (A3128, A3067, A3099, A3112, A3091, A3054, A3081, A3046)
Key unwrapping	BC-Auth	Key unwrapping		AES-KW: (A3128, A3067, A3099, A3112, A3091, A3054, A3081, A3046)
Deterministic random bit generation	DRBG	Deterministic random bit generation		Counter DRBG: (A3128, A3053, A3080, A3051, A3078, A3062, A3096, A3052, A3064, A3063, A3100, A3079, A3066, A3089, A3065, A3061, A3076, A3043, A3097, A3075, A3088, A3044, A3129, A3111, A3110, A3107, A3077, A3108, A3098, A3090, A3055, A3130, A3101, A3106, A3056, A3109, A3045) Hash DRBG: (A3053, A3080, A3051, A3078, A3062, A3096, A3052, A3117, A3064, A3063, A3100, A3079, A3066, A3118, A3089, A3065, A3061, A3071, A3076, A3043, A3097, A3116, A3088, A3044, A3129, A3111, A3110, A3107, A3073, A3077, A3108, A3098, A3090, A3055, A3130, A3101, A3106, A3072, A3056, A3109, A3045) HMAC DRBG: (A3053, A3080, A3051, A3078, A3062, A3096, A3052, A3117, A3064, A3063, A3100, A3079, A3066, A3118, A3089, A3065, A3061, A3071, A3076, A3043, A3097, A3116, A3088, A3044, A3129, A3111, A3110, A3107, A3073, A3077, A3108, A3098, A3090, A3055, A3130, A3101, A3106, A3072, A3056, A3109, A3045)
EC Diffie-Hellman key generation	AsymKeyPair-KeyGen	EC Diffie-Hellman key generation		ECDSA KeyGen (FIPS186-4): (A3089, A3044)
Safe Primes key generation	AsymKeyPair-KeyGen	Safe Primes key generation		Safe Primes Key Generation: (A3043, A3088)

© 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
EC Diffie-Hellman shared secret computation	KAS-SSC	EC Diffie-Hellman shared secret computation		KAS-ECC-SSC Sp800-56Ar3: (A3089, A3044)
Diffie-Hellman shared secret computation	KAS-SSC	Diffie-Hellman shared secret computation		KAS-FFC-SSC Sp800-56Ar3: (A3043, A3088)
Digital signature verification	DigSig-SigVer	Digital signature verification	Hash:SHA2-224, SHA2-256, SHA2-384, SHA2-512	RSA SigVer (FIPS186-4): (A3078, A3117, A3118, A3071, A3116, A3073, A3090, A3072, A3045)
Digital signature verification (Legacy Use)	DigSig-SigVer	Digital signature verification for legacy use	Hash:SHA-1	RSA SigVer (FIPS186-4): (A3078, A3117, A3118, A3071, A3116, A3073, A3090, A3072, A3045)
Message digest	SHA	Message digest		SHA3-224: (A3085, A3092, A3126, A3047) SHA3-256: (A3085, A3092, A3126, A3047) SHA3-384: (A3085, A3092, A3126, A3047) SHA3-512: (A3085, A3092, A3126, A3047) SHA-1: (A3078, A3119, A3086, A3117, A3087, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3125, A3073, A3090, A3072, A3074, A3045) SHA2-224: (A3132, A3078, A3119, A3117, A3087, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3131, A3125, A3073, A3090, A3072, A3074, A3045) SHA2-256: (A3132, A3078, A3119, A3117, A3087, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3131, A3125, A3073, A3090, A3072, A3074, A3045) SHA2-384: (A3132, A3078, A3127, A3117, A3118, A3089, A3071, A3043, A3116, A3088, A3044, A3073, A3090, A3072, A3045) SHA2-512: (A3132, A3078, A3127, A3117, A3118, A3089, A3071, A3043, A3116, A3088,

© 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
				A3044, A3073, A3090, A3072, A3045)

Table 8: 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 4106 and shall only be used for the IPsec stack of the kernel to be compliant with FIPS 140-3 IG C.H, Scenario 1 b. Any other usage of GCM encryption is considered as non-approved.
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 IPsec protocol 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 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 Diffie-Hellman and Elliptic Curve Diffie-Hellman shared secret computation services in the context of IETF protocols. Additionally, the module's approved key pair generation service 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.

2.7.4 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.

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

2.7.5 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.

2.7.6 SHA-1 Usage

SHA-1 is only approved when used in approved modes for message digest, HMAC, Hash DRBG, and HMAC DRBG.

2.8 RBG and Entropy

The module employs a Deterministic Random Bit Generator (DRBG) based on SP 800-90A Rev. 1 for random number generation. The DRBG supports the Hash_DRBG, HMAC_DRBG, and CTR_DRBG mechanisms. These DRBG mechanisms are self-tested in accordance with Section 11.3 of SP 800-90A Rev. 1.

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 performs APT and RCT health tests on the entropy source at startup and during normal operation as required by Section 4 of SP 800-90B. The module obtains 337 bits (version 3.3) or 342 bits (version 3.4) of entropy to seed, and 224 bits (version 3.3) or 228 bits (version 3.4) of entropy to reseed. As the reseeding entropy string does not provide a full 256 bits of entropy, the module generates SSPs (e.g., keys) whose strengths are modified by available entropy.
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
E19	SUSE LLC
E20	SUSE LLC

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Kernel CPU Time Jitter RNG	Non-Physical	SUSE Linux Enterprise Server 15 SP4 on ARM Ampere® Altra® Q80-30, AMD EPYC(TM) 7371, IBM z15, Intel® Xeon® Silver 4215R, or IBM Power10	64 bits	56.22 bits	N/A
Kernel-RT CPU Time Jitter RNG	Non-Physical	SUSE Linux Enterprise Server 15 SP4 on AMD EPYC(TM) 7371, or Intel® Xeon® Silver 4215R	64 bits	57.07 bits	N/A

Table 10: Entropy Sources

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

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

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.

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. 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).

2.11 Industry Protocols

The module supports AES-GCM for use in the IPsec-v3 protocol.

© 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 from kernel system calls
N/A	Data Output	API output parameters from kernel system calls
N/A	Control Input	API function calls, API input parameters from kernel system calls, kernel command line
N/A	Status Output	API return values, kernel logs

Table 11: 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 self-tests, conditional self-tests, 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 12: 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.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Symmetric encryption	Perform AES encryption	crypto_skcipher_setkey returns 0	Key, plaintext	Ciphertext	Symmetric encryption	Crypto Officer - AES key: W,E
Symmetric decryption	Perform AES decryption	crypto_skcipher_setkey returns 0	Key, ciphertext	Plaintext	Symmetric decryption	Crypto Officer - AES key: W,E
Authenticated symmetric encryption	Perform authenticated AES encryption	crypto_aead_setkey returns 0 (CCM), crypto_tfm_get_flags has the CRYPTO_TFM_FIPS_COMPLIANCE flag set (GCM)	Key, plaintext	Ciphertext	Authenticated symmetric encryption	Crypto Officer - AES key: W,E
Authenticated symmetric decryption	Perform authenticated AES	crypto_aead_setkey returns 0 (CCM), crypto_tfm_get_flags has the	Key, ciphertext	Plaintext	Authenticated symmetric decryption	Crypto Officer - AES key: W,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
	decryption	CRYPTO_TFM_FIPS_COMPLIANCE flag set (GCM)				
Random number generation	Generate random numbers	crypto_rng_get_bytes returns 0	Number of bits	Random number	Deterministic random bit generation	Crypto Officer - Entropy input: G,E - DRBG seed: W,E,Z - DRBG internal state (V, C or key): G,E,Z
Message digest	Compute SHA hashes	crypto_shash_init returns 0	Message	Digest of the message	Message digest	Crypto Officer
Message authentication code (MAC)	Compute HMAC or AES-based CMAC	crypto_shash_init returns 0 (HMAC), crypto_cmac_digest_init returns 0 (CMAC)	Message, key	Message authentication code	Message authentication code (MAC)	Crypto Officer - HMAC key: W,E
Encrypt-then-MAC operation	Perform AES encryption then compute MAC	crypto_shash_init returns 0	Message, AES Key, HMAC key	Authenticated message	Symmetric encryption Message authentication code (MAC)	Crypto Officer - AES key: W,E - HMAC key: W,E
Key wrapping	Perform AES-based key wrapping	crypto_skcipher_setkey returns 0	Key wrapping key, key to be wrapped	Wrapped key	Key wrapping	Crypto Officer - AES key: W,E
Key wrapping (separate encrypt and MAC)	Perform AES-based key wrapping and HMAC	crypto_skcipher_setkey returns 0; crypto_shash_init returns 0	Key wrapping key, key to be wrapped	Wrapped key	Symmetric encryption Message authentication code (MAC)	Crypto Officer - AES key: W,E
Key unwrapping	Perform AES-based key unwrapping	crypto_skcipher_setkey returns 0	Wrapped key, key unwrapping key	Unwrapped key	Key unwrapping	Crypto Officer - AES key: W,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
Key unwrapping (separate decrypt and MAC)	Perform AES-based key unwrapping and HMAC	crypto_skcipher_setkey returns 0; crypto_shash_init returns 0	Wrapped key, key unwrapping key	Unwrapped key	Symmetric decryption Message authentication code (MAC)	Crypto Officer - AES key: W,E
EC Diffie-Hellman shared secret computation	Perform ECDH shared secret computation	crypto_kpp_compute_shared_secret returns 0	Private key, public key from peer	Shared secret	EC Diffie-Hellman shared secret computation	Crypto Officer - EC Diffie-Hellman public key: W,E - EC Diffie-Hellman private key: W,E - EC Diffie-Hellman shared secret: G,R
EC Diffie-Hellman key generation	Perform ECDH key generation	crypto_kpp_set_secret and crypto_kpp_generate_public_key return 0	Domain parameters	Generated key	EC Diffie-Hellman key generation	Crypto Officer - Module-generated EC Diffie-Hellman public key: G,R - Module-generated EC Diffie-Hellman private key: G,R
Diffie-Hellman shared secret	Perform DH shared secret	crypto_kpp_compute_shared_secret returns 0	Private key, public key from peer	Shared secret	Diffie-Hellman shared secret	Crypto Officer - 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
computation	computation				computation	public key: W,E - Diffie-Hellman private key: W,E - Diffie-Hellman shared secret: G,R
Diffie-Hellman key generation using safe primes	Perform DH key generation	crypto_kpp_set_secret and crypto_kpp_generate_public_key return 0	Domain parameters	Generated key	Safe Primes key generation	Crypto Officer - Module-generated Diffie-Hellman public key: G,R - Module-generated Diffie-Hellman private key: G,R
Error detection code	Detect, report, correct memory errors with crc32c , crct10dif	The indicator can be verified through the contents of the /proc/sys/crypto/fips_enabled file which must contain the numeric value of "1".	None	Code	None	Crypto Officer
Data compression	Compress data with deflate, lz4, lz4hc, lzo, zlib, 842	Implicit (always approved)	Data to compress	Compressed data	None	Crypto Officer
Memory copy operation	Copy memory	Implicit (always approved)	Source, destination, offset, amount	Return codes and/or log messages	None	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
Show status	Show module status	Implicit (always approved)	None	Return codes and/or log messages	None	Crypto Officer
On-Demand Self-tests	Perform self-tests on demand	Implicit (always approved)	None	Success or Failure	Symmetric encryption Symmetric decryption Authenticated symmetric encryption Authenticated symmetric decryption Message authentication code (MAC) Key wrapping Key unwrapping Deterministic random bit generation EC Diffie-Hellman key generation Safe Primes key generation EC Diffie-Hellman shared secret computation Diffie-Hellman shared secret	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
					computation Digital signature verification Digital signature verification (Legacy Use) Message digest	
Module installation and configuration	Install and configure module	Implicit (always approved)	Configuration parameters	Return codes and/or log	None	Crypto Officer
Module initialization	Initialize module	Implicit (always approved)	None	None	None	Crypto Officer
Zeroization	Zeroize SSPs	Implicit (always approved)	Context containing SSPs	Return codes and/or log	None	Crypto Officer - AES key: Z - HMAC key: Z - Entropy input: Z - DRBG seed: Z - DRBG internal state (V, C or key): Z - Module-generated EC Diffie-Hellman public key: Z - 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 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

© 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
						secret: Z - Intermediate key generation value: Z
Show module name and version	Show module name and version	Implicit (always approved)	None	Name and version information	None	Crypto Officer

Table 13: 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	Symmetric encryption	AES-GCM with external IV	CO
AES-GMAC	Message authentication code (MAC)	AES-GMAC	CO
RSA	RSA encryption primitive; RSA decryption primitive; RSA signature generation primitive; RSA signature verification primitive	RSA	CO
ECDSA	ECDSA signature verification primitive	ECDSA	CO

Table 14: 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 module uses the HMAC-SHA2-256 algorithm for the integrity test of the static kernel binary and the fipscheck application. The HMAC calculation is performed by the fipscheck application itself. The key used is hardcoded in the fipscheck application.
Additionally, the module uses RSA signature verification with a SHA2-256 message digest and a 2048-bit key for the integrity test of each of the kernel object files loaded during boot-up time. The key used for these integrity tests is hardcoded in the static kernel binary.
If any integrity value does not match the expected value, the test fails, and the module enters the error state.

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. The module does not perform persistent storage of SSPs	Dynamic

Table 15: 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 16: 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 zeroization routine indicates that the zeroization procedure succeeded.	By calling the cipher related zeroization API
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 17: SSP Zeroization Methods

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

The application is responsible for calling the appropriate destruction functions from the Kernel Crypto API. When a calling application calls the appropriate API function, that function overwrites the memory with zeros and deallocates the memory when the cipher handler is freed. The completion of a zeroization and freeing the cipher handler routines 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 Authenticated symmetric decryption Key wrapping Key unwrapping
HMAC key	HMAC key	112-256 bits - 112-256 bits	Symmetric key - CSP			Message authentication code (MAC)
Entropy input	Entropy input	192-384 bits - 192 to 384 bits	Entropy Input - CSP			Deterministic random bit generation
DRBG seed	DRBG seed	440, 888 bits (Hash_DRBG); 256, 320, 384 bits (CTR_DRBG); 192-2^36 bits (HMAC_DRBG) - 128, 192, 256 bits	Seed - CSP	Deterministic random bit generation		Deterministic random bit generation
DRBG internal state (V, C or key)	DRBG internal state (V, C or key)	880, 1776 bits (Hash_DRBG); 256, 320, 384 bits (CTR_DRBG); 320, 448, 512, 768, 1024 bits (HMAC_DRBG	Internal state - CSP	Deterministic random bit generation		Deterministic random bit 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
		) - 128, 192, 256 bits				
Module-generated EC Diffie-Hellman public key	Module-generated EC Diffie-Hellman public key	P-256, P-384 - 128, 192	Public key - PSP	EC Diffie-Hellman key generation		
Module-generated EC Diffie-Hellman private key	Module-generated EC Diffie-Hellman private key	P-256, P-384 - 128, 192	Private key - CSP	EC Diffie-Hellman key generation		
EC Diffie-Hellman public key	EC Diffie-Hellman public key	P-256, P-384 - 128, 192	Public key - PSP			EC Diffie-Hellman shared secret computation
EC Diffie-Hellman private key	EC Diffie-Hellman private key	P-256, P-384 - 128, 192	Private key - CSP			EC Diffie-Hellman shared secret computation
Module-generated Diffie-Hellman public key	Module-generated Diffie-Hellman public key	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112, 128, 149, 172, 200 bits	Public key - PSP	Safe Primes key generation		
Module-generated Diffie-Hellman private key	Module-generated Diffie-Hellman private key	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112, 128, 149, 172, 200 bits	Private key - CSP	Safe Primes key 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
Diffie-Hellman public key	Diffie-Hellman public key	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112, 128, 149, 172, 200 bits	Public key - PSP			Diffie-Hellman shared secret computation
Diffie-Hellman private key	Diffie-Hellman private key	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112, 128, 149, 172, 200 bits	Private key - CSP			Diffie-Hellman shared secret computation
EC Diffie-Hellman shared secret	EC Diffie-Hellman shared secret	P-256, P-384 - 128, 192	Shared Secret - CSP		EC Diffie-Hellman shared secret computation	
Diffie-Hellman shared secret	Diffie-Hellman shared secret	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112, 128, 149, 172, 200	Shared Secret - CSP		Diffie-Hellman shared secret computation	
Intermediate key generation value	Intermediate key pair generation value	112-384 bits - 112-200 bits	Intermediate value - CSP	EC Diffie-Hellman key generation Safe Primes		EC Diffie-Hellman key generation Safe Primes

© 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
	generated during key generation and key derivation services (SP 800-133 Rev. 2 Section 4, 5.1, and 5.2)			key generation		key generation

Table 18: 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	Wipe and Free memory block allocated Module Reset	
HMAC key	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	
Entropy input	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Automatic Module Reset	DRBG seed:Derives
DRBG seed		RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Automatic Module Reset	Entropy input:Derived From DRBG internal state (V, C or key):Derives
DRBG internal state (V, C or key)		RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Automatic Module Reset	DRBG seed:Derived From
Module-generated EC Diffie-Hellman public key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block	Module-generated EC Diffie-Hellman private 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
				allocated Module Reset	Intermediate key generation value:Derived From
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 Intermediate key generation value:Derived From
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
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 Intermediate key generation value:Derived From
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 Intermediate key generation value:Derived From
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

© 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 shared secret	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	EC Diffie-Hellman public key:Established from EC Diffie-Hellman private key:Established from
Diffie-Hellman shared secret	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Diffie-Hellman public key:Established from Diffie-Hellman private key:Established from
Intermediate key generation value			From service invocation to service completion	Wipe and Free memory block allocated Automatic Module Reset	Module-generated EC Diffie-Hellman public key:Derives Module-generated EC Diffie-Hellman private key:Derives Module-generated Diffie-Hellman public key:Derives Module-generated Diffie-Hellman private key:Derives

Table 19: 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 (A3043)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3044)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3045)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3071)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3072)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3073)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3074)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3078)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3087)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3088)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3089)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3090)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3116)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3117)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3118)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3119)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3125)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A
HMAC-SHA2-256 (A3131)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A

© 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
HMAC-SHA2-256 (A3132)	SHA2-256	MAC tag verification	SW/FW Integrity	Module become operational	N/A

Table 20: Pre-Operational Self-Tests

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 (A3128) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3053) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3080) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3051) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3078) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3062) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3096) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3052) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3064) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	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-ECB (A3063) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3100) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3079) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3066) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3089) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3065) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3061) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3076) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3043) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3097) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3075) - Encryption	128/192/256-bit keys, 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 (A3088) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3044) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3129) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3131) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3125) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3111) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3110) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3107) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3077) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3108) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3098) - Encryption	128/192/256-bit keys, 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 (A3090) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3055) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3130) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3101) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3106) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3056) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3109) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3045) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3128) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3053) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3080) - Decryption	128/192/256-bit keys, 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 (A3051) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3078) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3062) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3096) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3052) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3064) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3063) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3100) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3079) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3066) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3089) - Decryption	128/192/256-bit keys, 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 (A3065) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3061) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3076) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3043) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3097) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3075) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3088) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3044) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3129) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3131) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3125) - Decryption	128/192/256-bit keys, 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 (A3111) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3110) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3107) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3077) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3108) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3098) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3090) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3055) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3130) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3101) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3106) - Decryption	128/192/256-bit keys, 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 (A3056) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3109) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3045) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3128) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3053) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3078) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3064) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3061) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3075) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3131) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3125) - Encryption	128/192/256-bit keys, 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-CBC (A3098) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3090) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3106) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3109) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3045) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3128) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3053) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3078) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3064) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3061) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3075) - Decryption	128/192/256-bit keys, 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-CBC (A3131) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3125) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3098) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3090) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3106) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3109) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3045) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3128) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3053) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3078) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3064) - Encryption	128/192/256-bit keys, 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-CTR (A3061) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3075) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3131) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3125) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3098) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3090) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3106) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3109) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3045) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3128) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3053) - Decryption	128/192/256-bit keys, 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-CTR (A3078) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3064) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3061) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3075) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3131) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3125) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3098) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3090) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3106) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3109) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3045) - Decryption	128/192/256-bit keys, 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 (A3128) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3053) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3080) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3051) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3078) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3062) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3096) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3052) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3064) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3063) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3100) - Encryption	128/192/256-bit keys, 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 (A3079) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3066) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3065) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3061) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3076) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3097) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3075) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3129) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3111) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3110) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3107) - Encryption	128/192/256-bit keys, 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 (A3077) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3108) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3098) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3090) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3055) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3130) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3101) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3106) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3056) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3109) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3045) - Encryption	128/192/256-bit keys, 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 (A3128) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3053) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3080) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3051) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3078) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3062) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3096) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3052) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3064) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3063) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3100) - Decryption	128/192/256-bit keys, 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 (A3079) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3066) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3065) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3061) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3076) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3097) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3075) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3129) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3111) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3110) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3107) - Decryption	128/192/256-bit keys, 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 (A3077) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3108) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3098) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3090) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3055) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3130) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3101) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3106) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3056) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3109) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3045) - Decryption	128/192/256-bit keys, 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 (A3128) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3053) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3078) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3064) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3075) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3125) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3098) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3090) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3109) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3045) - Encryption	128/192/256-bit keys, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3128) - Decryption	128/192/256-bit keys, 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 (A3053) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3078) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3064) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3075) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3125) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3098) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3090) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3109) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3045) - Decryption	128/192/256-bit keys, decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CMAC (A3128)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3053)	128/192/256-bit keys, MAC generation	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 (A3078)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3064)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3075)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3125)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3098)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3090)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3109)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3045)	128/192/256-bit keys, MAC generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
SHA-1 (A3078)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3119)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3086)		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 (A3117)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3087)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3118)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3089)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3071)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3043)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3116)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3088)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3044)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3125)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3073)		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 (A3090)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3072)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3074)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3045)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3132)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3078)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3119)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3117)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3087)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3118)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3089)		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 (A3071)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3043)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3116)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3088)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3044)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3131)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3125)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3073)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3090)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3072)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3074)		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 (A3045)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3132)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3078)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3119)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3117)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3087)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3118)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3089)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3071)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3043)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3116)		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 (A3088)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3044)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3131)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3125)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3073)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3090)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3072)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3074)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3045)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3132)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3078)		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 (A3127)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3117)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3118)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3089)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3071)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3043)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3116)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3088)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3044)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3073)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3090)		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 (A3072)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3045)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3132)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3078)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3127)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3117)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3118)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3089)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3071)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3043)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3116)		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 (A3088)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3044)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3073)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3090)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3072)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3045)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A3085)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A3092)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A3126)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A3047)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3085)		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 (A3092)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3126)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3047)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A3085)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A3092)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A3126)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A3047)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3085)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3092)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3126)		KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3047)		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
HMAC-SHA-1 (A3078)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3119)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3086)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3117)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3087)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3118)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3089)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3071)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3043)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3116)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3088)	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 (A3044)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3125)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3073)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3090)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3072)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3074)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3045)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3132)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3078)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3119)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3117)	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 (A3087)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3118)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3089)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3071)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3043)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3116)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3088)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3044)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3131)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3125)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3073)	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 (A3090)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3072)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3074)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3045)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3132)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3078)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3119)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3117)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3087)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3118)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3089)	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 (A3071)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3043)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3116)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3088)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3044)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3131)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3125)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3073)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3090)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3072)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3074)	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 (A3045)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3132)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3078)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3127)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3117)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3118)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3089)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3071)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3043)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3116)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3088)	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 (A3044)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3073)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3090)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3072)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3045)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3132)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3078)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3127)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3117)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3118)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3089)	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 (A3071)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3043)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3116)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3088)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3044)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3073)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3090)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3072)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3045)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3085)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3092)	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 (A3126)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3047)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3085)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3092)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3126)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3047)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3085)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3092)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3126)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3047)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3085)	SHA3-512	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-SHA3-512 (A3092)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3126)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3047)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
Counter DRBG (3128) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3053) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3080) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3051) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3078) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3062) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3096) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3052) - with prediction resistance	128-bit key, with df, with pr	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
Counter DRBG (3064) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3063) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3100) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3079) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3066) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3089) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3065) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3061) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3076) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3043) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3097) - with prediction resistance	128-bit key, with df, with pr	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
Counter DRBG (3075) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3088) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3044) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3129) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3111) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3110) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3107) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3077) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3108) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3098) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3090) - with prediction resistance	128-bit key, with df, with pr	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
Counter DRBG (3055) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3130) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3101) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3106) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3056) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3109) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3045) - with prediction resistance	128-bit key, with df, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3128) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3053) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3080) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3051) - without	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	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
prediction resistance						before the integrity test
Counter DRBG (3078) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3062) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3096) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3052) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3064) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3063) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3100) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3079) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3066) - without	128/192/256-bit key, with df, without pr	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 (3089) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3065) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3061) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3076) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3043) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3097) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3075) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3088) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3044) - without	128/192/256-bit key, with df, without pr	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 (3129) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3111) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3110) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3107) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3077) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3108) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3098) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3090) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3055) - without	128/192/256-bit key, with df, without pr	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 (3130) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3101) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3106) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3056) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3109) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (3045) - without prediction resistance	128/192/256-bit key, with df, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3053)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3080)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3051)	SHA2-256, with/without pr	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
Hash DRBG (A3078)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3062)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3096)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3052)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3117)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3064)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3063)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3100)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3079)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3066)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3118)	SHA2-256, with/without pr	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
Hash DRBG (A3089)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3065)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3061)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3071)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3076)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3043)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3097)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3116)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3088)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3044)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3129)	SHA2-256, with/without pr	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
Hash DRBG (A3111)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3110)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3107)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3073)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3077)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3108)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3098)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3090)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3055)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3130)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3101)	SHA2-256, with/without pr	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
Hash DRBG (A3106)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3072)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3056)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3109)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Hash DRBG (A3045)	SHA2-256, with/without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3053) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3080) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3051) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3078) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3062) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3096) - with prediction resistance	HMAC-SHA2-256, with pr	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
HMAC DRBG (A3052) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3117) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3064) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3063) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3100) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3079) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3066) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3118) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3089) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3065) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3061) - with prediction resistance	HMAC-SHA2-256, with pr	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
HMAC DRBG (A3071) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3076) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3043) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3097) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3116) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3088) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3044) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3129) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3111) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3110) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3107) - with prediction resistance	HMAC-SHA2-256, with pr	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
HMAC DRBG (A3073) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3077) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3108) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3098) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3090) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3055) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3130) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3101) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3106) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3072) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3056) - with prediction resistance	HMAC-SHA2-256, with pr	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
HMAC DRBG (A3109) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3045) - with prediction resistance	HMAC-SHA2-256, with pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3053) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3080) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3051) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3078) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3062) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3096) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3052) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3117) - without	HMAC-SHA2-256/HMAC-	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	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
prediction resistance	SHA2-512, without pr					before the integrity test
HMAC DRBG (A3064) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3063) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3100) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3079) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3066) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3118) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3089) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3065) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3061) - without	HMAC-SHA2-256/HMAC-SHA2-512, without pr	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						
HMAC DRBG (A3071) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3076) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3043) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3097) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3116) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3088) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3044) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3129) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3111) - without	HMAC-SHA2-256/HMAC-SHA2-512, without pr	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						
HMAC DRBG (A3110) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3107) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3073) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3077) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3108) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3098) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3090) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3055) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3130) - without	HMAC-SHA2-256/HMAC-SHA2-512, without pr	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						
HMAC DRBG (A3101) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3106) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3072) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3056) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3109) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC DRBG (A3045) - without prediction resistance	HMAC-SHA2-256/HMAC-SHA2-512, without pr	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3089)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3044)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A3043)	MODP-2048, ffdhe3072	PCT	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 (A3088)	MODP-2048, ffdhe3072	PCT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test

Table 21: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3043)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3044)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3045)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3071)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3072)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3073)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3074)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3078)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3087)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3088)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3089)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3090)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3116)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3117)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3118)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3119)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3125)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3131)	MAC tag verification	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3132)	MAC tag verification	SW/FW Integrity	On Demand	Manually

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3128) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3053) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3080) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3051) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3078) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3062) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3096) - 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 (A3052) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3064) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3063) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3100) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3079) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3066) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3089) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3065) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3061) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3076) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3043) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3097) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3075) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3088) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3044) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3129) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3131) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3125) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3111) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3110) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3107) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3077) - 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 (A3108) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3098) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3090) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3055) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3130) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3101) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3106) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3056) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3109) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3045) - Encryption	KAT	CAST	On Demand	Manually
AES-ECB (A3128) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3053) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3080) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3051) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3078) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3062) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3096) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3052) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3064) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3063) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3100) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3079) - 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 (A3066) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3089) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3065) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3061) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3076) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3043) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3097) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3075) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3088) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3044) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3129) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3131) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3125) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3111) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3110) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3107) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3077) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3108) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3098) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3090) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3055) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3130) - 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 (A3101) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3106) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3056) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3109) - Decryption	KAT	CAST	On Demand	Manually
AES-ECB (A3045) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3128) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3053) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3078) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3064) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3061) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3075) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3131) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3125) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3098) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3090) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3106) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3109) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3045) - Encryption	KAT	CAST	On Demand	Manually
AES-CBC (A3128) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3053) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3078) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3064) - 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-CBC (A3061) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3075) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3131) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3125) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3098) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3090) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3106) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3109) - Decryption	KAT	CAST	On Demand	Manually
AES-CBC (A3045) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3128) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3053) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3078) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3064) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3061) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3075) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3131) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3125) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3098) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3090) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3106) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3109) - Encryption	KAT	CAST	On Demand	Manually
AES-CTR (A3045) - 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-CTR (A3128) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3053) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3078) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3064) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3061) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3075) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3131) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3125) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3098) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3090) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3106) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3109) - Decryption	KAT	CAST	On Demand	Manually
AES-CTR (A3045) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3128) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3053) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3080) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3051) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3078) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3062) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3096) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3052) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3064) - 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 (A3063) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3100) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3079) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3066) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3065) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3061) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3076) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3097) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3075) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3129) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3111) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3110) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3107) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3077) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3108) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3098) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3090) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3055) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3130) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3101) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3106) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3056) - 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 (A3109) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3045) - Encryption	KAT	CAST	On Demand	Manually
AES-GCM (A3128) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3053) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3080) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3051) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3078) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3062) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3096) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3052) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3064) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3063) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3100) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3079) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3066) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3065) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3061) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3076) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3097) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3075) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3129) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3111) - 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 (A3110) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3107) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3077) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3108) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3098) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3090) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3055) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3130) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3101) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3106) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3056) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3109) - Decryption	KAT	CAST	On Demand	Manually
AES-GCM (A3045) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3128) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3053) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3078) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3064) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3075) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3125) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3098) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3090) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3109) - 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 (A3045) - Encryption	KAT	CAST	On Demand	Manually
AES-CCM (A3128) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3053) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3078) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3064) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3075) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3125) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3098) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3090) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3109) - Decryption	KAT	CAST	On Demand	Manually
AES-CCM (A3045) - Decryption	KAT	CAST	On Demand	Manually
AES-CMAC (A3128)	KAT	CAST	On Demand	Manually
AES-CMAC (A3053)	KAT	CAST	On Demand	Manually
AES-CMAC (A3078)	KAT	CAST	On Demand	Manually
AES-CMAC (A3064)	KAT	CAST	On Demand	Manually
AES-CMAC (A3075)	KAT	CAST	On Demand	Manually
AES-CMAC (A3125)	KAT	CAST	On Demand	Manually
AES-CMAC (A3098)	KAT	CAST	On Demand	Manually
AES-CMAC (A3090)	KAT	CAST	On Demand	Manually
AES-CMAC (A3109)	KAT	CAST	On Demand	Manually
AES-CMAC (A3045)	KAT	CAST	On Demand	Manually
SHA-1 (A3078)	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
SHA-1 (A3119)	KAT	CAST	On Demand	Manually
SHA-1 (A3086)	KAT	CAST	On Demand	Manually
SHA-1 (A3117)	KAT	CAST	On Demand	Manually
SHA-1 (A3087)	KAT	CAST	On Demand	Manually
SHA-1 (A3118)	KAT	CAST	On Demand	Manually
SHA-1 (A3089)	KAT	CAST	On Demand	Manually
SHA-1 (A3071)	KAT	CAST	On Demand	Manually
SHA-1 (A3043)	KAT	CAST	On Demand	Manually
SHA-1 (A3116)	KAT	CAST	On Demand	Manually
SHA-1 (A3088)	KAT	CAST	On Demand	Manually
SHA-1 (A3044)	KAT	CAST	On Demand	Manually
SHA-1 (A3125)	KAT	CAST	On Demand	Manually
SHA-1 (A3073)	KAT	CAST	On Demand	Manually
SHA-1 (A3090)	KAT	CAST	On Demand	Manually
SHA-1 (A3072)	KAT	CAST	On Demand	Manually
SHA-1 (A3074)	KAT	CAST	On Demand	Manually
SHA-1 (A3045)	KAT	CAST	On Demand	Manually
SHA2-224 (A3132)	KAT	CAST	On Demand	Manually
SHA2-224 (A3078)	KAT	CAST	On Demand	Manually
SHA2-224 (A3119)	KAT	CAST	On Demand	Manually
SHA2-224 (A3117)	KAT	CAST	On Demand	Manually
SHA2-224 (A3087)	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 (A3118)	KAT	CAST	On Demand	Manually
SHA2-224 (A3089)	KAT	CAST	On Demand	Manually
SHA2-224 (A3071)	KAT	CAST	On Demand	Manually
SHA2-224 (A3043)	KAT	CAST	On Demand	Manually
SHA2-224 (A3116)	KAT	CAST	On Demand	Manually
SHA2-224 (A3088)	KAT	CAST	On Demand	Manually
SHA2-224 (A3044)	KAT	CAST	On Demand	Manually
SHA2-224 (A3131)	KAT	CAST	On Demand	Manually
SHA2-224 (A3125)	KAT	CAST	On Demand	Manually
SHA2-224 (A3073)	KAT	CAST	On Demand	Manually
SHA2-224 (A3090)	KAT	CAST	On Demand	Manually
SHA2-224 (A3072)	KAT	CAST	On Demand	Manually
SHA2-224 (A3074)	KAT	CAST	On Demand	Manually
SHA2-224 (A3045)	KAT	CAST	On Demand	Manually
SHA2-256 (A3132)	KAT	CAST	On Demand	Manually
SHA2-256 (A3078)	KAT	CAST	On Demand	Manually
SHA2-256 (A3119)	KAT	CAST	On Demand	Manually
SHA2-256 (A3117)	KAT	CAST	On Demand	Manually
SHA2-256 (A3087)	KAT	CAST	On Demand	Manually
SHA2-256 (A3118)	KAT	CAST	On Demand	Manually
SHA2-256 (A3089)	KAT	CAST	On Demand	Manually
SHA2-256 (A3071)	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
SHA2-256 (A3043)	KAT	CAST	On Demand	Manually
SHA2-256 (A3116)	KAT	CAST	On Demand	Manually
SHA2-256 (A3088)	KAT	CAST	On Demand	Manually
SHA2-256 (A3044)	KAT	CAST	On Demand	Manually
SHA2-256 (A3131)	KAT	CAST	On Demand	Manually
SHA2-256 (A3125)	KAT	CAST	On Demand	Manually
SHA2-256 (A3073)	KAT	CAST	On Demand	Manually
SHA2-256 (A3090)	KAT	CAST	On Demand	Manually
SHA2-256 (A3072)	KAT	CAST	On Demand	Manually
SHA2-256 (A3074)	KAT	CAST	On Demand	Manually
SHA2-256 (A3045)	KAT	CAST	On Demand	Manually
SHA2-384 (A3132)	KAT	CAST	On Demand	Manually
SHA2-384 (A3078)	KAT	CAST	On Demand	Manually
SHA2-384 (A3127)	KAT	CAST	On Demand	Manually
SHA2-384 (A3117)	KAT	CAST	On Demand	Manually
SHA2-384 (A3118)	KAT	CAST	On Demand	Manually
SHA2-384 (A3089)	KAT	CAST	On Demand	Manually
SHA2-384 (A3071)	KAT	CAST	On Demand	Manually
SHA2-384 (A3043)	KAT	CAST	On Demand	Manually
SHA2-384 (A3116)	KAT	CAST	On Demand	Manually
SHA2-384 (A3088)	KAT	CAST	On Demand	Manually
SHA2-384 (A3044)	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 (A3073)	KAT	CAST	On Demand	Manually
SHA2-384 (A3090)	KAT	CAST	On Demand	Manually
SHA2-384 (A3072)	KAT	CAST	On Demand	Manually
SHA2-384 (A3045)	KAT	CAST	On Demand	Manually
SHA2-512 (A3132)	KAT	CAST	On Demand	Manually
SHA2-512 (A3078)	KAT	CAST	On Demand	Manually
SHA2-512 (A3127)	KAT	CAST	On Demand	Manually
SHA2-512 (A3117)	KAT	CAST	On Demand	Manually
SHA2-512 (A3118)	KAT	CAST	On Demand	Manually
SHA2-512 (A3089)	KAT	CAST	On Demand	Manually
SHA2-512 (A3071)	KAT	CAST	On Demand	Manually
SHA2-512 (A3043)	KAT	CAST	On Demand	Manually
SHA2-512 (A3116)	KAT	CAST	On Demand	Manually
SHA2-512 (A3088)	KAT	CAST	On Demand	Manually
SHA2-512 (A3044)	KAT	CAST	On Demand	Manually
SHA2-512 (A3073)	KAT	CAST	On Demand	Manually
SHA2-512 (A3090)	KAT	CAST	On Demand	Manually
SHA2-512 (A3072)	KAT	CAST	On Demand	Manually
SHA2-512 (A3045)	KAT	CAST	On Demand	Manually
SHA3-224 (A3085)	KAT	CAST	On Demand	Manually
SHA3-224 (A3092)	KAT	CAST	On Demand	Manually
SHA3-224 (A3126)	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
SHA3-224 (A3047)	KAT	CAST	On Demand	Manually
SHA3-256 (A3085)	KAT	CAST	On Demand	Manually
SHA3-256 (A3092)	KAT	CAST	On Demand	Manually
SHA3-256 (A3126)	KAT	CAST	On Demand	Manually
SHA3-256 (A3047)	KAT	CAST	On Demand	Manually
SHA3-384 (A3085)	KAT	CAST	On Demand	Manually
SHA3-384 (A3092)	KAT	CAST	On Demand	Manually
SHA3-384 (A3126)	KAT	CAST	On Demand	Manually
SHA3-384 (A3047)	KAT	CAST	On Demand	Manually
SHA3-512 (A3085)	KAT	CAST	On Demand	Manually
SHA3-512 (A3092)	KAT	CAST	On Demand	Manually
SHA3-512 (A3126)	KAT	CAST	On Demand	Manually
SHA3-512 (A3047)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3078)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3119)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3086)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3117)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3087)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3118)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3089)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3071)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3043)	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 (A3116)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3088)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3044)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3125)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3073)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3090)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3072)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3074)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3045)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3132)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3078)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3119)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3117)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3087)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3118)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3089)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3071)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3043)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3116)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3088)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3044)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3131)	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-SHA2-224 (A3125)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3073)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3090)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3072)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3074)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3045)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3132)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3078)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3119)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3117)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3087)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3118)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3089)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3071)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3043)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3116)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3088)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3044)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3131)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3125)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3073)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3090)	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 (A3072)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3074)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3045)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3132)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3078)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3127)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3117)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3118)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3089)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3071)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3043)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3116)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3088)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3044)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3073)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3090)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3072)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3045)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3132)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3078)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3127)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3117)	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-SHA2-512 (A3118)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3089)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3071)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3043)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3116)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3088)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3044)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3073)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3090)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3072)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3045)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3085)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3092)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3126)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3047)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3085)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3092)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3126)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3047)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3085)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3092)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3126)	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 (A3047)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3085)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3092)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3126)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3047)	KAT	CAST	On Demand	Manually
Counter DRBG (3128) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3053) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3080) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3051) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3078) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3062) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3096) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3052) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3064) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3063) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3100) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3079) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3066) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3089) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3065) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3061) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3076) - with prediction resistance	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 (3043) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3097) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3075) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3088) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3044) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3129) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3111) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3110) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3107) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3077) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3108) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3098) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3090) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3055) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3130) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3101) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3106) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3056) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3109) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3045) - with prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3128) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3053) - without prediction resistance	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 (3080) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3051) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3078) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3062) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3096) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3052) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3064) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3063) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3100) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3079) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3066) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3089) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3065) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3061) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3076) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3043) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3097) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3075) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3088) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3044) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3129) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3111) - without prediction resistance	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 (3110) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3107) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3077) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3108) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3098) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3090) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3055) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3130) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3101) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3106) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3056) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3109) - without prediction resistance	KAT	CAST	On Demand	Manually
Counter DRBG (3045) - without prediction resistance	KAT	CAST	On Demand	Manually
Hash DRBG (A3053)	KAT	CAST	On Demand	Manually
Hash DRBG (A3080)	KAT	CAST	On Demand	Manually
Hash DRBG (A3051)	KAT	CAST	On Demand	Manually
Hash DRBG (A3078)	KAT	CAST	On Demand	Manually
Hash DRBG (A3062)	KAT	CAST	On Demand	Manually
Hash DRBG (A3096)	KAT	CAST	On Demand	Manually
Hash DRBG (A3052)	KAT	CAST	On Demand	Manually
Hash DRBG (A3117)	KAT	CAST	On Demand	Manually
Hash DRBG (A3064)	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
Hash DRBG (A3063)	KAT	CAST	On Demand	Manually
Hash DRBG (A3100)	KAT	CAST	On Demand	Manually
Hash DRBG (A3079)	KAT	CAST	On Demand	Manually
Hash DRBG (A3066)	KAT	CAST	On Demand	Manually
Hash DRBG (A3118)	KAT	CAST	On Demand	Manually
Hash DRBG (A3089)	KAT	CAST	On Demand	Manually
Hash DRBG (A3065)	KAT	CAST	On Demand	Manually
Hash DRBG (A3061)	KAT	CAST	On Demand	Manually
Hash DRBG (A3071)	KAT	CAST	On Demand	Manually
Hash DRBG (A3076)	KAT	CAST	On Demand	Manually
Hash DRBG (A3043)	KAT	CAST	On Demand	Manually
Hash DRBG (A3097)	KAT	CAST	On Demand	Manually
Hash DRBG (A3116)	KAT	CAST	On Demand	Manually
Hash DRBG (A3088)	KAT	CAST	On Demand	Manually
Hash DRBG (A3044)	KAT	CAST	On Demand	Manually
Hash DRBG (A3129)	KAT	CAST	On Demand	Manually
Hash DRBG (A3111)	KAT	CAST	On Demand	Manually
Hash DRBG (A3110)	KAT	CAST	On Demand	Manually
Hash DRBG (A3107)	KAT	CAST	On Demand	Manually
Hash DRBG (A3073)	KAT	CAST	On Demand	Manually
Hash DRBG (A3077)	KAT	CAST	On Demand	Manually
Hash DRBG (A3108)	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
Hash DRBG (A3098)	KAT	CAST	On Demand	Manually
Hash DRBG (A3090)	KAT	CAST	On Demand	Manually
Hash DRBG (A3055)	KAT	CAST	On Demand	Manually
Hash DRBG (A3130)	KAT	CAST	On Demand	Manually
Hash DRBG (A3101)	KAT	CAST	On Demand	Manually
Hash DRBG (A3106)	KAT	CAST	On Demand	Manually
Hash DRBG (A3072)	KAT	CAST	On Demand	Manually
Hash DRBG (A3056)	KAT	CAST	On Demand	Manually
Hash DRBG (A3109)	KAT	CAST	On Demand	Manually
Hash DRBG (A3045)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3053) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3080) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3051) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3078) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3062) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3096) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3052) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3117) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3064) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3063) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3100) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3079) - with prediction resistance	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 DRBG (A3066) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3118) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3089) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3065) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3061) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3071) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3076) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3043) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3097) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3116) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3088) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3044) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3129) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3111) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3110) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3107) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3073) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3077) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3108) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3098) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3090) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3055) - with prediction resistance	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 DRBG (A3130) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3101) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3106) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3072) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3056) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3109) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3045) - with prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3053) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3080) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3051) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3078) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3062) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3096) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3052) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3117) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3064) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3063) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3100) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3079) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3066) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3118) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3089) - without prediction resistance	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 DRBG (A3065) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3061) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3071) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3076) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3043) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3097) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3116) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3088) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3044) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3129) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3111) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3110) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3107) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3073) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3077) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3108) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3098) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3090) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3055) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3130) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3101) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3106) - without prediction resistance	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 DRBG (A3072) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3056) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3109) - without prediction resistance	KAT	CAST	On Demand	Manually
HMAC DRBG (A3045) - without prediction resistance	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3089)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3044)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3043)	PCT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3088)	PCT	CAST	On Demand	Manually

Table 23: Conditional Periodic Information

10.4 Error States

When the module fails any pre-operational self-test or conditional test, the module will indicate an error has occurred and will enter the Error state. Any further cryptographic operation is inhibited. In the Error state, all data output is inhibited, and no cryptographic operations are allowed. The error can be recovered by a restart (i.e., powering off and powering on) of the module.
The following table shows the error codes and the corresponding condition:

Name	Description	Conditions	Recovery Method	Indicator
Error	General error state	Failure of pre-operational or conditional self-tests Failure of entropy source health tests Failure of PCT	Restart module	Kernel panic

Table 24: Error States

10.5 Operator Initiation of Self-Tests

On-demand self-tests can be invoked by powering-off and reloading the module which cause the module to run the pre-operational and conditional cryptographic algorithms self-tests. On-demand self-tests can also be invoked by calling kernel_restart() function which effectively powers off the module and then reloads the module.

© 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. 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:

```
"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.

In addition, the Crypto Officer should check the module version via the “uname -r” command. This will return “5.14.21-150400.24.46-default” for version 3.3 of the module, and “5.14.21-150400.15.11-rt” for version 3.4.

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

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.

Operating System	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 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 25 - 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.
The following RPM packages contain the FIPS validated module:

Processor Architecture	RPM Packages
x86_64	dracut-fips-055+suse.252.g4988b0bf-150400.1.8.rpm kernel-default-5.14.21-150400.24.46.1.rpm kernel-rt-5.14.21-150400.15.11.1.rpm (for x86_64 processors architecture) libkcapi-tools-0.13.0-1.114.rpm
aarch64	
z15	
Power10	

Table 26 – RPM packages

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. 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 B. 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 2022 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** April 2024 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
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

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

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
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	**The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)** June 2005 https://www.ietf.org/rfc/rfc4106.txt

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