IBM

IBM DataPower FIPS Provider

FIPS 140-3 Non-Proprietary Security Policy

Prepared by:

atsec information security corporation

4516 Seton Center Parkway, Suite 250

Austin, TX 78759

www.atsec.com

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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....8
2.4 Modes of Operation....8
2.5 Algorithms....9
2.6 Security Function Implementations....25
2.7 Algorithm Specific Information....44
2.8 RBG and Entropy....45
2.9 Key Generation....46
2.10 Key Establishment....47
2.11 Industry Protocols....47
3 Cryptographic Module Interfaces....48
3.1 Ports and Interfaces....48
4 Roles, Services, and Authentication....49
4.1 Authentication Methods....49
4.2 Roles....49
4.3 Approved Services....49
4.4 Non-Approved Services....55
4.5 External Software/Firmware Loaded....55
5 Software/Firmware Security....57
5.1 Integrity Techniques....57
5.2 Initiate on Demand....57
6 Operational Environment....58
6.1 Operational Environment Type and Requirements....58
6.2 Configuration Settings and Restrictions....58
7 Physical Security....59
8 Non-Invasive Security....60
9 Sensitive Security Parameters Management....61
9.1 Storage Areas....61
9.2 SSP Input-Output Methods....61
9.3 SSP Zeroization Methods....61
9.4 SSPs....62

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9.5 Transitions....66
10 Self-Tests....67
10.1 Pre-Operational Self-Tests....67
10.2 Conditional Self-Tests....67
10.3 Periodic Self-Test Information....76
10.4 Error States....81
10.5 Operator Initiation of Self-Tests....82
11 Life-Cycle Assurance....83
11.1 Installation, Initialization, and Startup Procedures....83
11.2 Administrator Guidance....83
11.3 Non-Administrator Guidance....83
11.6 End of Life....83
12 Mitigation of Other Attacks....84
Appendix A. Glossary and abbreviations....85
Appendix B. References....87

© 2024 IBM Corporation/ 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: Modes List and Description....8
Table 5: Approved Algorithms....24
Table 6: Vendor-Affirmed Algorithms....24
Table 7: Non-Approved, Not Allowed Algorithms....25
Table 8: Security Function Implementations....44
Table 9: Entropy Certificates....45
Table 10: Entropy Sources....46
Table 11: Ports and Interfaces....48
Table 12: Roles....49
Table 13: Approved Services....54
Table 14: Non-Approved Services....55
Table 15: Storage Areas....61
Table 16: SSP Input-Output Methods....61
Table 17: SSP Zeroization Methods....61
Table 18: SSP Table 1....64
Table 19: SSP Table 2....66
Table 20: Pre-Operational Self-Tests....67
Table 21: Conditional Self-Tests....76
Table 22: Pre-Operational Periodic Information....76
Table 23: Conditional Periodic Information....81
Table 24: Error States....82

List of Figures

Figure 1: Block Diagram....7

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 3.0.9-B3346E1D91BA83B7BAB52F472F3E6A0D of the IBM DataPower FIPS Provider. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.
This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

1.2 Security Levels

Section	Security Level
1	1
2	1
3	1
4	1
5	1
6	1
7	N/A
8	N/A
9	1
10	1
11	1
12	1

Table 1: Security Levels

© 2024 IBM Corporation/ 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 IBM DataPower FIPS Provider (hereafter referred to as “the module”) is defined as a software module in a multi-chip standalone embodiment. It provides a C language application program interface (API) for use by other applications that require cryptographic functionality. The module consists of one software component, the “FIPS provider”, which implements the FIPS requirements and the cryptographic functionality provided to the operator.

Module Type: Software

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

The cryptographic boundary of the module is defined as the fips.so shared library, which contains the compiled code implementing the FIPS provider.

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 (a general-purpose computer on which the module is installed) is indicated by a purple dashed line. The cryptographic boundary is represented by the component painted in orange, which consists only of the shared library implementing the FIPS provider (fips.so).
Green lines indicate the flow of data between the cryptographic module and its operator application, through the logical interfaces defined in Section 3.
Components in white are only included in the diagram for informational purposes. They are not included in the cryptographic boundary (and therefore not part of the module’s validation). For example, the kernel is responsible for managing system calls issued by the module itself, as well as other applications using the module for cryptographic services.

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

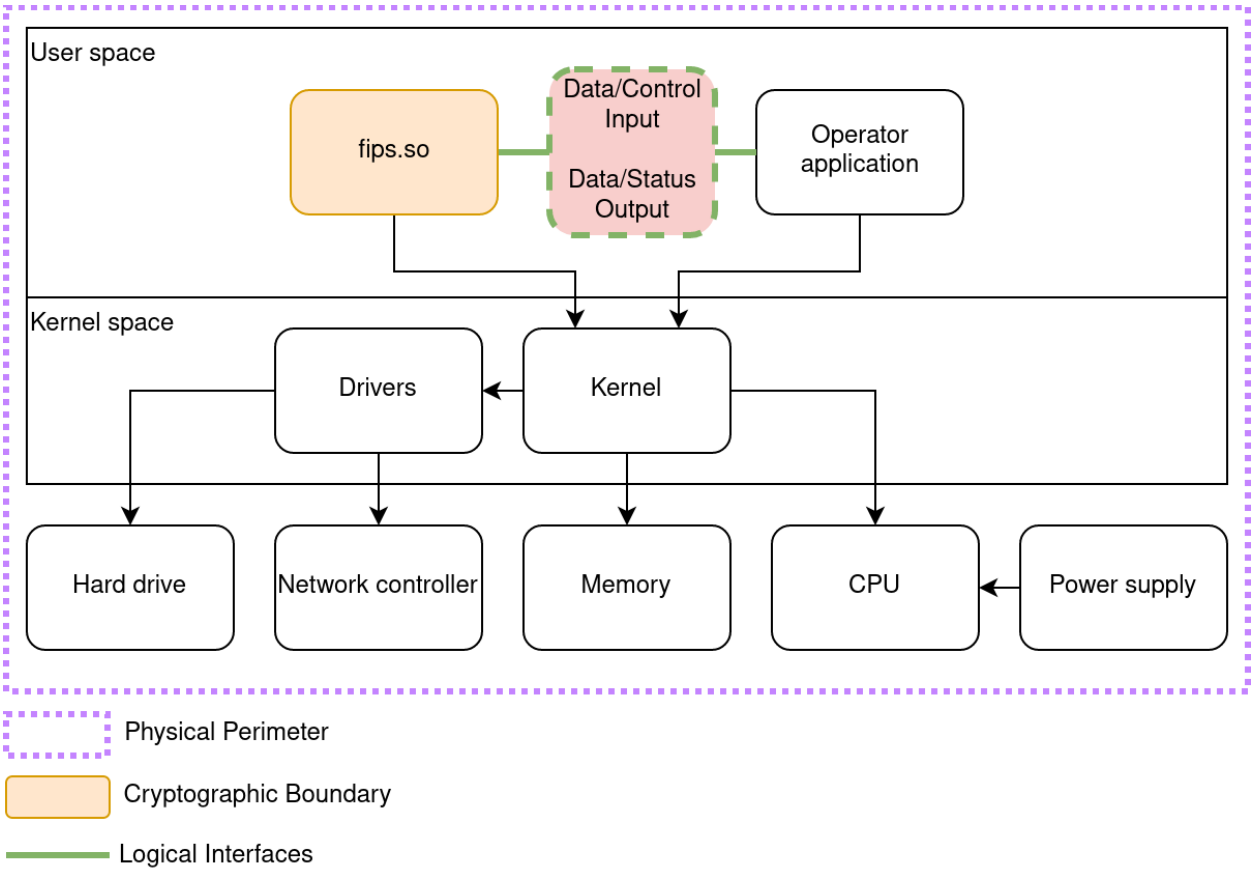

Figure 1: Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP of the module is defined as the general-purpose computer on which the module is installed.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
fips.so	3.0.9-B3346E1D91BA83B7BAB52F472F3E6A0D		HMAC-SHA2-256

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

Tested Module Identification – Hybrid Disjoint Hardware:

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/ PAI	Hypervisor or Host OS	Version(s)
CentOS Stream 8	IBM DataPower Gateway X3	Intel Xeon Gold 6326	Yes		3.0.9-B3346E1D91BA83B7BAB52F472F3E6A0D
CentOS Stream 8	IBM DataPower Gateway X3	Intel Xeon Gold 6326	No		3.0.9-B3346E1D91BA83B7BAB52F472F3E6A0D

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

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

N/A for this module.

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:

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

Table 4: 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.

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, thus causing the module to end its operation.

Mode Change Instructions and Status:

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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
KDA HKDF Sp800-56Cr1	A4355	Derived Key Length: 2048 Shared Secret Length: 224-2048 Increment 8 HMAC Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384	SP 800-56C Rev. 2
TLS v1.3 KDF (CVL)	A4355	HMAC Algorithm: SHA2-256, SHA2-384 KDF Running Modes: DHE, PSK, PSK-DHE	SP 800-135 Rev. 1
Counter DRBG	A4356	Prediction Resistance: Yes, No Supports Reseed Mode: AES-128, AES-192, AES-256 Derivation Function Enabled: Yes, No	SP 800-90A Rev. 1
Hash DRBG	A4356	Prediction Resistance: Yes, No Supports Reseed Mode: SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A4356	Prediction Resistance: Yes, No Supports Reseed Mode: SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
AES-CBC	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CBC-CS1	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CBC-CS2	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CBC-CS3	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CCM	A4357	Key Length: 128, 192, 256 Tag Length: 32, 48, 64, 80, 96, 112, 128 IV Length: 56, 64, 72, 80, 88, 96, 104	SP 800-38C
AES-CFB1	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CFB128	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CFB8	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CMAC	A4357	Direction: Generation, Verification	SP 800-38B

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Key Length: 128, 192, 256 MAC Length: 128	
AES-CTR	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-ECB	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-KW	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38F
AES-KWP	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38F
AES-OFB	A4357	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A4357	Direction: Decrypt, Encrypt Key Length: 128, 256 Tweak Mode: Hex Data Unit Length Matches Payload	SP 800-38E
AES-CBC	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CBC-CS1	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CBC-CS2	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CBC-CS3	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CCM	A4358	Key Length: 128, 192, 256 Tag Length: 32, 48, 64, 80, 96, 112, 128 IV Length: 56, 64, 72, 80, 88, 96, 104	SP 800-38C
AES-CFB1	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CFB128	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CFB8	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CMAC	A4358	Direction: Generation, Verification Key Length: 128, 192, 256 MAC Length: 128	SP 800-38B
AES-CTR	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-ECB	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-KW	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38F
AES-KWP	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38F
AES-OFB	A4358	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A4358	Direction: Decrypt, Encrypt Key Length: 128, 256 Tweak Mode: Hex Data Unit Length Matches Payload	SP 800-38E
AES-CBC	A4359	Direction: Decrypt, Encrypt	SP 800-38A

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Key Length: 128, 192, 256	
AES-CBC-CS1	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CBC-CS2	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CBC-CS3	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CCM	A4359	Key Length: 128, 192, 256 Tag Length: 32, 48, 64, 80, 96, 112, 128 IV Length: 56, 64, 72, 80, 88, 96, 104	SP 800-38C
AES-CFB1	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CFB128	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CFB8	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-CMAC	A4359	Direction: Generation, Verification Key Length: 128, 192, 256 MAC Length: 128	SP 800-38B
AES-CTR	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-ECB	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-KW	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38F
AES-KWP	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38F
AES-OFB	A4359	Direction: Decrypt, Encrypt Key Length: 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A4359	Direction: Decrypt, Encrypt Key Length: 128, 256 Tweak Mode: Hex Data Unit Length Matches Payload	SP 800-38E
AES-GCM	A4360	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96, 128	SP 800-38D
AES-GMAC	A4360	Direction: Decrypt, Encrypt IV Generation: External Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	SP 800-38D
ECDSA KeyGen (FIPS186-5)	A4361	Curve: P-224, P-256, P-384, P-521 Secret Generation Mode: testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A4361	Curve: P-224, P-256, P-384, P-521	FIPS 186-5

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigGen (FIPS186-5)	A4361	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4361	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
HMAC-SHA-1	A4361	MAC: 160 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4361	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4361	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4361	MAC: 384 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4361	MAC: 512 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A4361	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A4361	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4361	P-224, P-256, P-384, P-521 Scheme: ephemeralUnified KAS Role: initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A4361	Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 zz Length: 8-4096 Increment 8 Key Data Length: 8-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A4361	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Shared Info Length: 0-1024 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A4361	Iteration Count: 1000-10000 Increment 1 HMAC Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Password Length: 8-128 Increment 1 Salt Length: 128-4096 Increment 8	SP 800-132

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Key Data Length: 128-4096 Increment 8	
RSA KeyGen (FIPS186-5)	A4361	Key Generation Mode: probableWithProbableAux Modulo: 2048, 3072, 4096 Private Key Format: standard Public Exponent Mode: random	FIPS 186-5
RSA SigGen (FIPS186-5)	A4361	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A4361	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 1024 Signature Type: pkcs1v1.5, pss	FIPS 186-4
RSA SigVer (FIPS186-5)	A4361	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
SHA-1	A4361	-	FIPS 180-4
SHA2-224	A4361	-	FIPS 180-4
SHA2-256	A4361	-	FIPS 180-4
SHA2-384	A4361	-	FIPS 180-4
SHA2-512	A4361	-	FIPS 180-4
SHA2-512/224	A4361	-	FIPS 180-4
SHA2-512/256	A4361	-	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4361	Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 Key Block Length: 1024	SP 800-135 Rev. 1
ECDSA SigGen (FIPS186-5)	A4362	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4362	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
HMAC-SHA3-224	A4362	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A4362	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A4362	MAC: 384 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A4362	MAC: 512 Key Length: 112-524288 Increment 8	FIPS 198-1
KDF ANS 9.42 (CVL)	A4362	Hash Algorithm: SHA3-224, SHA3-256, SHA3-384, SHA3-512 zz Length: 8-4096 Increment 8	SP 800-135 Rev. 1

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Key Data Length: 8-4096 Increment 8	
KDF ANS 9.63 (CVL)	A4362	Hash Algorithm: SHA3-224, SHA3-256, SHA3-384, SHA3-512 Shared Info Length: 0-1024 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A4362	Iteration Count: 1000-10000 Increment 1 HMAC Algorithm: SHA3-224, SHA3-256, SHA3-384, SHA3-512 Password Length: 8-128 Increment 1 Salt Length: 128-4096 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-132
RSA SigGen (FIPS186-5)	A4362	Hash Algorithm: SHA3-224, SHA3-256, SHA3-384, SHA3-512 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A4362	Hash Algorithm: SHA3-224, SHA3-256, SHA3-384, SHA3-512 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
SHA3-224	A4362	-	FIPS 202
SHA3-256	A4362	-	FIPS 202
SHA3-384	A4362	-	FIPS 202
SHA3-512	A4362	-	FIPS 202
SHAKE-128	A4362	-	FIPS 202
SHAKE-256	A4362	-	FIPS 202
AES-GCM	A4363	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96, 128	SP 800-38D
AES-GMAC	A4363	Direction: Decrypt, Encrypt IV Generation: External Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	SP 800-38D
AES-GCM	A4364	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96, 128	SP 800-38D
AES-GMAC	A4364	Direction: Decrypt, Encrypt IV Generation: External	SP 800-38D

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	
ECDSA KeyGen (FIPS186-5)	A4365	Curve: P-224, P-256, P-384, P-521 Secret Generation Mode: testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A4365	Curve: P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A4365	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4365	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
HMAC-SHA-1	A4365	MAC: 160 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4365	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4365	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4365	MAC: 384 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4365	MAC: 512 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A4365	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A4365	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4365	P-224, P-256, P-384, P-521 Scheme: ephemeralUnified KAS Role: initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A4365	Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 zz Length: 8-4096 Increment 8 Key Data Length: 8-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A4365	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Shared Info Length: 0-1024 Increment 8 Key Data Length: 128-4096	SP 800-135 Rev. 1

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Increment 8	
PBKDF	A4365	Iteration Count: 1000-10000 Increment 1 HMAC Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Password Length: 8-128 Increment 1 Salt Length: 128-4096 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-5)	A4365	Key Generation Mode: probableWithProbableAux Modulo: 2048, 3072, 4096 Private Key Format: standard Public Exponent Mode: random	FIPS 186-5
RSA SigGen (FIPS186-5)	A4365	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A4365	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 1024 Signature Type: pkcs1v1.5, pss	FIPS 186-4
RSA SigVer (FIPS186-5)	A4365	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
SHA-1	A4365	-	FIPS 180-4
SHA2-224	A4365	-	FIPS 180-4
SHA2-256	A4365	-	FIPS 180-4
SHA2-384	A4365	-	FIPS 180-4
SHA2-512	A4365	-	FIPS 180-4
SHA2-512/224	A4365	-	FIPS 180-4
SHA2-512/256	A4365	-	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4365	Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 Key Block Length: 1024	SP 800-135 Rev. 1
ECDSA KeyGen (FIPS186-5)	A4366	Curve: P-224, P-256, P-384, P-521 Secret Generation Mode: testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A4366	Curve: P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A4366	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4366	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-	FIPS 186-5

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		512/224, SHA2-512/256	
HMAC-SHA-1	A4366	MAC: 160 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4366	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4366	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4366	MAC: 384 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4366	MAC: 512 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A4366	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A4366	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4366	P-224, P-256, P-384, P-521 Scheme: ephemeralUnified KAS Role: initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A4366	Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 zz Length: 8-4096 Increment 8 Key Data Length: 8-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A4366	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Shared Info Length: 0-1024 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A4366	Iteration Count: 1000-10000 Increment 1 HMAC Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Password Length: 8-128 Increment 1 Salt Length: 128-4096 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-5)	A4366	Key Generation Mode: probableWithProbableAux Modulo: 2048, 3072, 4096 Private Key Format: standard Public Exponent Mode: random	FIPS 186-5

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
RSA SigGen (FIPS186-5)	A4366	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A4366	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 1024 Signature Type: pkcs1v1.5, pss	FIPS 186-4
RSA SigVer (FIPS186-5)	A4366	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
SHA-1	A4366	-	FIPS 180-4
SHA2-224	A4366	-	FIPS 180-4
SHA2-256	A4366	-	FIPS 180-4
SHA2-384	A4366	-	FIPS 180-4
SHA2-512	A4366	-	FIPS 180-4
SHA2-512/224	A4366	-	FIPS 180-4
SHA2-512/256	A4366	-	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4366	Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 Key Block Length: 1024	SP 800-135 Rev. 1
ECDSA KeyGen (FIPS186-5)	A4367	Curve: P-224, P-256, P-384, P-521 Secret Generation Mode: testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A4367	Curve: P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A4367	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4367	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
HMAC-SHA-1	A4367	MAC: 160 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4367	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4367	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4367	MAC: 384 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4367	MAC: 512 Key Length: 112-524288 Increment 8	FIPS 198-1

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512/224	A4367	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A4367	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4367	P-224, P-256, P-384, P-521 Scheme: ephemeralUnified KAS Role: initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A4367	Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 zz Length: 8-4096 Increment 8 Key Data Length: 8-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A4367	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Shared Info Length: 0-1024 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A4367	Iteration Count: 1000-10000 Increment 1 HMAC Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Password Length: 8-128 Increment 1 Salt Length: 128-4096 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-5)	A4367	Key Generation Mode: probableWithProbableAux Modulo: 2048, 3072, 4096 Private Key Format: standard Public Exponent Mode: random	FIPS 186-5
RSA SigGen (FIPS186-5)	A4367	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A4367	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 1024 Signature Type: pkcs1v1.5, pss	FIPS 186-4
RSA SigVer (FIPS186-5)	A4367	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
SHA-1	A4367	-	FIPS 180-4

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
SHA2-224	A4367	-	FIPS 180-4
SHA2-256	A4367	-	FIPS 180-4
SHA2-384	A4367	-	FIPS 180-4
SHA2-512	A4367	-	FIPS 180-4
SHA2-512/224	A4367	-	FIPS 180-4
SHA2-512/256	A4367	-	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4367	Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 Key Block Length: 1024	SP 800-135 Rev. 1
ECDSA KeyGen (FIPS186-5)	A4368	Curve: P-224, P-256, P-384, P-521 Secret Generation Mode: testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A4368	Curve: P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A4368	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4368	Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
HMAC-SHA-1	A4368	MAC: 160 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4368	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4368	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4368	MAC: 384 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4368	MAC: 512 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A4368	MAC: 224 Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A4368	MAC: 256 Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4368	P-224, P-256, P-384, P-521 Scheme: ephemeralUnified KAS Role: initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A4368	Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 zz Length: 8-4096 Increment 8 Key Data Length: 8-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A4368	Hash Algorithm: SHA2-224, SHA2-	SP 800-135 Rev.

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Shared Info Length: 0-1024 Increment 8 Key Data Length: 128-4096 Increment 8	1
PBKDF	A4368	Iteration Count: 1000-10000 Increment 1 HMAC Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Password Length: 8-128 Increment 1 Salt Length: 128-4096 Increment 8 Key Data Length: 128-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-5)	A4368	Key Generation Mode: probableWithProbableAux Modulo: 2048, 3072, 4096 Private Key Format: standard Public Exponent Mode: random	FIPS 186-5
RSA SigGen (FIPS186-5)	A4368	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A4368	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 1024 Signature Type: pkcs1v1.5, pss	FIPS 186-4
RSA SigVer (FIPS186-5)	A4368	Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Modulo: 2048, 3072, 4096 Signature Type: pkcs1v1.5, pss	FIPS 186-5
SHA-1	A4368	-	FIPS 180-4
SHA2-224	A4368	-	FIPS 180-4
SHA2-256	A4368	-	FIPS 180-4
SHA2-384	A4368	-	FIPS 180-4
SHA2-512	A4368	-	FIPS 180-4
SHA2-512/224	A4368	-	FIPS 180-4
SHA2-512/256	A4368	-	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4368	Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 Key Block Length: 1024	SP 800-135 Rev. 1
KDF SSH (CVL)	A4370	Hash Algorithm: SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
AES-GCM	A4371	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112,	SP 800-38D

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		120, 128 IV Length: 96, 128	
AES-GMAC	A4371	Direction: Decrypt, Encrypt IV Generation: External Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	SP 800-38D
AES-GCM	A4372	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96, 128	SP 800-38D
AES-GMAC	A4372	Direction: Decrypt, Encrypt IV Generation: External Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	SP 800-38D
AES-GCM	A4373	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96, 128	SP 800-38D
AES-GMAC	A4373	Direction: Decrypt, Encrypt IV Generation: External Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	SP 800-38D
AES-GCM	A4374	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96, 128	SP 800-38D
AES-GMAC	A4374	Direction: Decrypt, Encrypt IV Generation: External Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	SP 800-38D
AES-GCM	A4375	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128	SP 800-38D

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		IV Length: 96, 128	
AES-GMAC	A4375	Direction: Decrypt, Encrypt IV Generation: External Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	SP 800-38D
AES-GCM	A4376	Direction: Decrypt, Encrypt IV Generation: External, Internal IV Generation Mode: 8.2.2 Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96, 128	SP 800-38D
AES-GMAC	A4376	Direction: Decrypt, Encrypt IV Generation: External Key Length: 128, 192, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96	SP 800-38D
KDF SSH (CVL)	A4377	Hash Algorithm: SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SSH (CVL)	A4378	Hash Algorithm: SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SSH (CVL)	A4379	Hash Algorithm: SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SSH (CVL)	A4380	Hash Algorithm: SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SP800-108	A4381	KDF Mode: Counter, Feedback MAC Mode: HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/224, HMAC-SHA2-512/256, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512, CMAC-AES128, CMAC-AES192, CMAC-AES256 Supported Lengths: 8, 72, 128, 776, 3456, 4096 Fixed Data Order: Before Fixed Data Counter Length: 32	SP 800-108 Rev. 1
KDA OneStep SP800-56Cr2	A4382	Auxiliary Function: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/224, HMAC-SHA2-512/256, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512	SP 800-56C Rev. 2

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Derived Key Length: 2048 Shared Secret Length: 224-2048 Increment 8	
KDA TwoStep SP800-56Cr2	A4382	KDF Mode: feedback MAC Modes: HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/224, HMAC-SHA2-512/256, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384 Derived Key Length: 2048 Shared Secret Length: 224-2048 Increment 8	SP 800-56C Rev. 2
KAS-FFC-SSC Sp800-56Ar3	A4383	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
Safe Primes Key Generation	A4383	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
Safe Primes Key Verification	A4383	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

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

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES GCM (external IV)	Encryption
HMAC (< 112-bit keys)	Message authentication

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Use and Function
KBKDF, KDA OneStep, KDA TwoStep, HKDF, ANS X9.42 KDF, ANS X9.63 KDF (< 112-bit input or output keys)	Key derivation
KDA OneStep, KDA TwoStep (SHAKE128, SHAKE256)	Key derivation
ANS X9.42 KDF (SHAKE128, SHAKE256)	Key derivation
ANS X9.63 KDF (SHA-1, SHAKE128, SHAKE256)	Key derivation
SSH KDF (SHA-512/224, SHA-512/256, SHA-3, SHAKE128, SHAKE256)	Key derivation
TLS 1.2 KDF (SHA-1, SHA-224, SHA-512/224, SHA-512/256, SHA-3)	Key derivation
TLS 1.3 KDF (SHA-1, SHA-224, SHA-512, SHA-512/224, SHA-512/256, SHA-3)	Key derivation
PBKDF2 (short password; short salt; insufficient iterations; < 112-bit output keys)	Password-based key derivation
KAS-IFC-SSC (KAS1 and KAS2 schemes)	Shared secret computation
RSA and ECDSA (pre-hashed message)	Signature generation; Signature verification
RSA-PSS (invalid salt length)	Signature generation; Signature verification
RSA-OAEP	Asymmetric encryption; Asymmetric decryption

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Random number generation	DRBG	Random number generation		Counter DRBG HMAC DRBG Hash DRBG AES-ECB AES-ECB AES-ECB HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/256 HMAC-SHA2-512/256

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-512 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Encryption/ Decryption	BC-UnAuth BC-Auth KTS-Wrap	Encryption/ Decryption		AES-CBC AES-CBC AES-CBC AES-CBC-CS1 AES-CBC-CS1 AES-CBC-CS1 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS3 AES-CBC-CS3 AES-CBC-CS3 AES-CCM AES-CCM AES-CCM AES-CFB1 AES-CFB1 AES-CFB1 AES-CFB128 AES-CFB128 AES-CFB128 AES-CFB8 AES-CFB8 AES-CFB8 AES-CTR AES-CTR AES-CTR AES-ECB

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				AES-ECB AES-ECB AES-KW AES-KW AES-KW AES-KWP AES-KWP AES-KWP AES-OFB AES-OFB AES-OFB AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0 AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM
Message authentication	MAC	Message authentication		AES-CMAC AES-CMAC AES-CMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				SHA-1 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-512/224 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-512 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512/224

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Signature generation	DigSig-SigGen	Signature generation		ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) SHA2-224

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Signature verification	DigSig-SigVer	Signature verification		ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-512 SHA2-512 SHA2-512

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				SHA2-512 SHA2-512 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Shared secret computation	KAS-SSC	Shared secret computation	KAS-ECC-SSC Strength:112-256 bits KAS-ECC-FFC Strength:112-200 bits	KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-FFC-SSC Sp800-56Ar3
Key derivation	KAS-135KDF KAS-56CKDF KBKDF	Key derivation		KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.42 KDF ANS

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				9.42 KDF ANS 9.42 KDF ANS 9.63 KDF ANS 9.63 KDF ANS 9.63 KDF ANS 9.63 KDF ANS 9.63 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 KDF SSH KDF SSH KDF SSH KDF SSH KDF SSH KDF SP800-108 KDA OneStep SP800-56Cr2 KDA TwoStep SP800-56Cr2 KDA HKDF Sp800-56Cr1 TLS v1.3 KDF AES-CMAC AES-CMAC AES-CMAC

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512/224

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-512 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-384 SHA2-384 SHA2-384

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				SHA2-384 SHA2-384 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Password-based key derivation	PBKDF	Password-based key derivation		PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/256 HMAC-

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-512 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				512/224 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Key pair generation	AsymKeyPair-KeyGen AsymKeyPair-SafePri	Key pair generation		ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) Safe Primes Key Generation
Key pair verification	AsymKeyPair-KeyVer AsymKeyPair-SafePri	Key pair verification		ECDSA KeyVer (FIPS186-5) ECDSA KeyVer

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				(FIPS186-5) ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5) Safe Primes Key Verification
Message digest	SHA	Message digest		SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/224 SHA2-512/256 SHA2-512/256 SHA2-

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				512/256 SHA2-512/256 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
XOF	XOF	XOF		SHAKE-128 SHAKE-256

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM:
For TLS 1.2, the module offers the AES-GCM implementation and uses the context of Scenario 1 of FIPS 140-3 IG C.H. OpenSSL 3 is compliant with SP 800-52r2 Section 3.3.1 and the mechanism for IV generation is compliant with RFC 5288 and 8446.
The module does not implement the TLS protocol. The module's implementation of AES GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS protocol implicitly ensures that the counter (the nonce_explicit part of the IV) does not exhaust the maximum number of possible values for a given session key. In the event the module's power is lost and restored, the consuming application must ensure that a new key for use with the AES-GCM key encryption or decryption under this scenario shall be established.
Alternatively, the Crypto Officer can use the module's API to perform AES-GCM encryption using internal IV generation. These IVs are always 96 bits and generated using the approved DRBG internal to the module's boundary, compliant to Scenario 2 of FIPS 140-3 IG C.H.
The module also provides a non-approved AES-GCM encryption service which accepts arbitrary external IVs from the operator. This service can be requested by invoking the EVP_EncryptInit_ex2 API function with a non-NULL iv value. When this is the case, the API will set a non-approved service indicator as described in Section 4.3.
Finally, for TLS 1.3, the AES-GCM implementation uses the context of Scenario 5 of FIPS 140-3 IG C.H. The protocol that provides this compliance is TLS 1.3, defined in RFC8446 of August 2018, using the cipher-suites that explicitly select AES-GCM as the encryption/decryption cipher (Appendix B.4 of RFC8446). The module supports acceptable AES-GCM cipher suites from Section 3.3.1 of SP800-52r2. TLS 1.3 employs separate 64-bit sequence numbers, one for protocol records that are received, and one for protocol records that are sent to a peer. These sequence numbers are set at zero at the beginning of a TLS 1.3 connection and each time when the AES-GCM key is changed. After reading or writing a record, the respective sequence number is incremented by one. The protocol specification determines that the sequence number should not wrap, and if this condition is observed, then the protocol implementation must either trigger a re-key of the session (i.e., a new key for AES-GCM), or terminate the connection.

AES-XTS:
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 per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E.

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

The XTS mode shall only be used for the cryptographic protection of data on storage devices. It shall not be used for other purposes, such as the encryption of data in transit.

PBKDF2:
The module provides password-based key derivation (PBKDF2), compliant with SP 800-132. The module supports option 1a from Section 5.4 of SP 800-132, in which the Master Key (MK) or a segment of it is used directly as the Data Protection Key (DPK). In accordance with SP 800-132 and FIPS 140-3 IG D.N, the following requirements shall be met:

- Derived keys shall only be used in storage applications. The MK shall not be used for other purposes. The length of the MK or DPK shall be 112 bits or more.
- Passwords or passphrases, used as an input for the PBKDF2, shall not be used as cryptographic keys.
- The length of the password or passphrase shall be at least 8 characters, and shall consist of lowercase, uppercase, and numeric characters. The probability of guessing the value is estimated to be at most $1/62^8 = 4 \times 10^{-15}$. Combined with the minimum iteration count as described below, this provides an acceptable trade-off between user experience and security against brute-force attacks.
- A portion of the salt, with a length of at least 128 bits, shall be generated randomly using the SP 800-90Ar1 DRBG provided by the module.
- The iteration count shall be selected as large as possible, as long as the time required to generate the key using the entered password is acceptable for the users. The minimum value is 1000.

If any of these requirements is not met, the requested service is non-approved.

RSA:
For RSA key pair generation, signature generation, and signature verification, the module supports any modulus size between 2048 and 16384 bits. Additionally, the module supports a modulus size of 1024 bits for RSA signature verification. Only modulus sizes 1024, 2048, 3072, and 4096 bits have been CAVP tested. Any other modulus size is untested.

SP 800-56Ar3 assurances:
To comply with the assurances found in Section 5.6.2 of SP 800-56Ar3, the operator must use the module together with an application that implements the TLS protocol. 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 800-56Ar3.

Legacy use:
Digital Signature Verification using RSA with a 1024-bit modulus is allowed for legacy use only.

2.8 RBG and Entropy

Cert Number	Vendor Name
E91	IBM Corporation

Table 9: Entropy Certificates

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Entropy Source for the IBM DataPower FIPS Provider	Non-Physical	IBM DataPower Gateway X3	256 bits	256 bits	SHA3-256 (A4294); AES-256 CTR DRBG (A4294); AES-256 CTR DRBG (A4356)

Table 10: Entropy Sources

The module employs two Deterministic Random Bit Generator (DRBG) implementations based on SP 800-90Ar1. These DRBGs are used internally by the module (e.g. to generate seeds for asymmetric key pairs and random numbers for security functions). They can also be accessed using the specified API functions. The following parameters are used:

1. Private DRBG: AES-256 CTR_DRBG with derivation function. This DRBG is used to generate secret random values (e.g. during asymmetric key pair generation). It can be accessed using the RAND_priv_bytes API function.
2. Public DRBG: AES-256 CTR_DRBG with derivation function. This DRBG is used to generate general purpose random values that do not need to remain secret (e.g. initialization vectors). It can be accessed using the RAND_bytes API function.

The DRBGs are seeded with 384 bits of seed material (corresponding to 384 bits of entropy) obtained from an SP 800-90B compliant entropy source. During reseeding, the DRBGs obtain 256 bits of seed material (corresponding to 256 bits of entropy). These DRBGs will always employ prediction resistance. More information regarding the configuration and design of these DRBGs can be found in the module's manual pages.
The module complies with the Public Use Document for ESV certificate E91 seeding the aforementioned DRBGs using the EVP_RAND_generate function, which corresponds to the GetEntropy() function. The operational environment of the module is identical to the one listed on the ESV certificate. There are no maintenance requirements for the entropy source.

2.9 Key Generation

The module implements Cryptographic Key Generation (CKG, vendor affirmed), compliant with SP 800-133r2. When random values are required, they are obtained from the SP 800-90Ar1 approved DRBG, compliant with Section 4 of SP 800-133r2. The following methods are implemented:

- Safe primes key pair generation: compliant with SP 800-133r2, Section 5.2, which maps to SP 800-56Ar3. The method described in Section 5.6.1.1.4 of SP 800-56Ar3 ("Testing Candidates") is used.
- RSA key pair generation: compliant with SP 800-133r2, Section 5.1, which maps to FIPS 186-5. The method described in Appendix A.1.6 of FIPS 186-5 ("Probable Primes with Conditions Based on Auxiliary Probable Primes") is used.
- ECDSA key pair generation: compliant with SP 800-133r2, Section 5.1, which maps to FIPS 186-5. The method described in Appendix B.2.2 of FIPS 186-5 ("Rejection Sampling") is used. Note that this generation method is also used to generate ECDH key pairs.

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

Additionally, the module implements the following key derivation methods, with a security strength of 112-256 bits:

- KBKDF: compliant with SP 800-108r1. This implementation can be used to derive secret keys from a pre-existing key-derivation-key.

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

- KDA OneStep, KDA TwoStep, HKDF: compliant with SP 800-56Cr2. These implementations shall only be used to derive secret keys in the context of an SP 800-56Ar3 key agreement scheme.
- ANS X9.42 KDF, ANS X9.63 KDF: compliant with SP 800-135r1. These implementations shall only be used to derive secret keys in the context of an ANS X9.42-2001 resp. ANS X9.63- 2001 key agreement scheme.
- SSH KDF, TLS 1.2 KDF, TLS 1.3 KDF: compliant with SP 800-135r1 and RFC 8446. These implementations shall only be used to derive secret keys in the context of the SSH, TLS 1.2, or TLS 1.3 protocols, respectively.
- PBKDF2: compliant with option 1a of SP 800-132. This implementation shall only be used to derive keys for use in storage applications.

2.10 Key Establishment

The module implements SSP agreement and SSP transport methods as listed in the SFI table.

2.11 Industry Protocols

The module implements the SSH key derivation function for use in the SSH protocol (RFC 4253 and RFC 6668).
GCM with internal IV generation in the approved mode is compliant with versions 1.2 and 1.3 of the TLS protocol (RFC 5288 and 8446) and shall only be used in conjunction with the TLS protocol. Additionally, the module implements the TLS 1.2 and TLS 1.3 key derivation functions for use in the TLS protocol.
For Diffie-Hellman, the module supports the use of the following safe primes:

- IKE (RFC 3526): MODP-2048 (ID = 14), MODP-3072 (ID = 15), MODP-4096 (ID = 16), MODP-6144 (ID = 17), MODP-8192 (ID = 18)
- TLS (RFC 7919): ffdhe2048 (ID = 256), ffdhe3072 (ID = 257), ffdhe4096 (ID = 258), ffdhe6144 (ID = 259), ffdhe8192 (ID = 260)

No parts of the SSH, TLS, or IKE protocols, other than those mentioned above, have been tested by the CAVP or CMVP.

© 2024 IBM Corporation/ 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

Physical Port	Logical Interface(s)	Data That Passes
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Data Input	API input parameters
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Data Output	API output parameters
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Control Input	API function calls
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Status Output	API return codes, error queue

Table 11: Ports and Interfaces

The logical interfaces are the APIs through which the applications request services. These logical interfaces are logically separated from each other by the API design.

© 2024 IBM Corporation/ 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

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 12: Roles

No support is provided for multiple concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message digest	Compute a message digest	EVP_DigestFinal_ex returns 1	Message	Digest value	Message digest	Crypto Officer
XOF	Compute the output of an XOF	EVP_DigestFinalXOF returns 1	Message, output length	Digest value	XOF	Crypto Officer
Encryption	Encrypt a plaintext	EVP_EncryptFinal_ex returns 1	Plaintext, IV, AES key	Ciphertext	Encryption/ Decryption	Crypto Officer - AES key: W,E
Decryption	Decrypt a cipher text	EVP_DecryptFinal_ex returns 1	Ciphertext, IV, AES key	Plaintext	Encryption/ Decryption	Crypto Officer - AES key: W,E
Authenticated encryption	Encrypt a plaintext	AES GCM: EVP_CIPHER_DATAPOWER_FIPS_INDICATOR_APPROVED; Others: EVP_EncryptFinal_ex returns 1	Plaintext, IV, AES key	Ciphertext, MAC tag	Encryption/ Decryption	Crypto Officer - AES key: W,E
Authenticated decryption	Decrypt a cipher text	AES GCM: EVP_CIPHER_DATAPOWER_FIPS_INDICATOR_APPROVED; Others: EVP_DecryptFinal_ex returns 1	Ciphertext, IV, AES key,	Plaintext or fail	Encryption/ Decryption	Crypto Officer - AES key: W,E

© 2024 IBM Corporation/ 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
			MAC tag			
Message authentication	Compute a MAC tag	HMAC: EVP_MAC_DATAPOWER_FIPS_INDICATOR_APPROVED; Others: EVP_MAC_final returns 1	Message, key	MAC tag	Message authentication	Crypto Officer - AES key: W,E - HMAC key: W,E
Key derivation	Derive a key from a key-derivation key or a shared secret	EVP_KDF_DATAPOWER_FIPS_INDICATOR_APPROVED	Key-derivation key or shared secret, output length	Derived key	Key derivation	Crypto Officer - Key-derivation key: W,E - Shared secret: W,E - Derived key: G,R
Password-based key derivation	Derive a key from a password	EVP_KDF_DATAPOWER_FIPS_INDICATOR_APPROVED	Password, salt, iteration count, output length	Derived key	Password-based key derivation	Crypto Officer - Password: W,E - Derived key: G,R
Random number generation	Generate random bytes	RAND_bytes, RAND_priv_bytes, RAND_bytes_ex, RAND_priv_bytes_ex returns 1	Output length	Random bytes	Random number generation	Crypto Officer - Entropy input: W,E,Z - DRBG seed: G,E,Z - DRBG intern

© 2024 IBM Corporation/ 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
						al state (V, Key): G,E - DRBG internal state (V, C): G,E
Shared secret computation	Compute a shared secret	EVP_PKEY_derive returns 1	Owner private key, peer public key		Shared secret computation	Crypto Officer - DH public key: W,E - DH private key: W,E - EC public key: W,E - EC private key: W,E - Shared secret: G,R
Signature generation	Generate a signature	RSA: OSSL_DP_FIPSINDICATOR_APPROVED and EVP_SIGNATURE_DATAPOWER_FIPS_INDICATOR_APPROVED; ECDSA: OSSL_DP_FIPSINDICATOR_APPROVED	Message, private key	Signature	Signature generation	Crypto Officer - EC private key: W,E - RSA private key: W,E
Signature verification	Verify a signature	RSA: OSSL_DP_FIPSINDICATOR_APPROVED and EVP_SIGNATURE_DATAPOWER_FIPS_INDICATOR_APPROVED; ECDSA: OSSL_DP_FIPSINDICATOR_APPR	Message, public key, signature	Pass/ fail	Signature verification	Crypto Officer - EC public key: W,E - RSA

© 2024 IBM Corporation/ 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
		OVED				public key: W,E
Key pair generation	Generate a key pair	EVP_PKEY_generate returns 1	Group, curve, or modulus size	Key pair	Key pair generation	Crypto Officer - DH public key: G,R - DH private key: G,R - EC public key: G,R - EC private key: G,R - RSA public key: G,R - RSA private key: G,R - Intermediate key generation value: G,E,Z
Key pair verification	Verify a key pair	Successful execution and non-approved indicator is not present	Key pair	Pass/ fail	Key pair verification	Crypto Officer - DH public key: W,E - DH private key: W,E - EC public key: W,E - EC

© 2024 IBM Corporation/ 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
						private key: W,E
Show version	Return the name and version information	None	None	Module name and version	None	Crypto Officer
Show status	Return the module status	None	None	Module status	None	Crypto Officer
Self-test	Perform the CASTs and integrity test	None	None	Pass/fail	None	Crypto Officer
Zeroization	Zeroize any SSP	None	Any SSP	None	None	Crypto Officer - AES key: Z - HMAC key: Z - Key-derivation key: Z - Shared secret: Z - Password: Z - Derived key: Z - DRBG internal state (V, Key):

© 2024 IBM Corporation/ 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
						Z - DRBG internal state (V, C): Z - DH public key: Z - DH private key: Z - EC public key: Z - EC private key: Z - RSA public key: Z - RSA private key: Z

Table 13: Approved Services

The following convention is used to specify access rights to SSPs:

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

To interact with the module, a calling application must use the EVP API layer provided by OpenSSL. This layer will delegate the request to the FIPS provider, which will in turn perform the requested service. Additionally, this EVP API layer can be used to retrieve the approved service indicator for the module. The datapower_ossl_query_fipsindicator API function indicates whether an EVP API function is approved. After a cryptographic service was performed by the module, the API context associated with this request can contain a parameter which represents the approved service indicator. The contexts and parameters are listed in the table below.

Context	Service Indicator
EVP_CIPHER_CTX	OSSL_CIPHER_PARAM_DATAPOWER_FIPS_INDICATOR
EVP_MAC_CTX	OSSL_MAC_PARAM_DATAPOWER_FIPS_INDICATOR
EVP_KDF_CTX	OSSL_KDF_PARAM_DATAPOWER_FIPS_INDICATOR

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

EVP_PKEY_CTX	OSSL_SIGNATURE_PARAM_DATAPOWER_FIPS_INDICATOR
EVP_PKEY_CTX	OSSL_ASYM_CIPHER_PARAM_DATAPOWER_FIPS_INDICATOR
EVP_PKEY_CTX	OSSL_KEM_PARAM_DATAPOWER_FIPS_INDICATOR

The details to use these functions and parameters are described in the module's manual pages.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Encryption	Encrypt a plaintext	AES GCM (external IV)	Crypto Officer
Message authentication	Compute a MAC tag	HMAC (< 112-bit keys)	Crypto Officer
Key derivation	Derive a key from a key-derivation key or a shared secret	KBKDF, KDA OneStep, KDA TwoStep, HKDF, ANS X9.42 KDF, ANS X9.63 KDF (< 112-bit input or output keys) KDA OneStep, KDA TwoStep (SHAKE128, SHAKE256) ANS X9.42 KDF (SHAKE128, SHAKE256) ANS X9.63 KDF (SHA-1, SHAKE128, SHAKE256) SSH KDF (SHA-512/224, SHA-512/256, SHA-3, SHAKE128, SHAKE256) TLS 1.2 KDF (SHA-1, SHA-224, SHA-512/224, SHA-512/256, SHA-3) TLS 1.3 KDF (SHA-1, SHA-224, SHA-512, SHA-512/224, SHA-512/256, SHA-3)	Crypto Officer
Password-based key derivation	Derive a key from a password	PBKDF2 (short password; short salt; insufficient iterations; < 112-bit output keys)	Crypto Officer
Shared secret computation	Compute a shared secret	KAS-IFC-SSC (KAS1 and KAS2 schemes)	Crypto Officer
Signature generation	Generate a signature	RSA and ECDSA (pre-hashed message) RSA-PSS (invalid salt length)	Crypto Officer
Signature verification	Verify a signature	RSA and ECDSA (pre-hashed message) RSA-PSS (invalid salt length)	Crypto Officer
Asymmetric encryption	Encrypt a plaintext	RSA-OAEP	Crypto Officer
Asymmetric decryption	Decrypt a ciphertext	RSA-OAEP	Crypto Officer

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

The module does not load external software or firmware.

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified by comparing a HMAC-SHA2-256 value calculated at run time with the HMAC-SHA2-256 value embedded in the fips.so file that was computed at build time.

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 resetting the module, or by calling the OSSL_PROVIDER_self_test API function. This will perform (among others) the software integrity test.

© 2024 IBM Corporation/ 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

How Requirements are Satisfied:

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

6.2 Configuration Settings and Restrictions

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

© 2024 IBM Corporation/ 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.

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

8 Non-Invasive Security

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

© 2024 IBM Corporation/ 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

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

Table 15: Storage Areas

SSPs are provided to the module by the calling process and are destroyed when released by the appropriate zeroization function calls.

9.2 SSP Input-Output Methods

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

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Free cipher handle	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 appropriate zeroization API functions
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 the module is unloaded	By unloading the module

Table 17: SSP Zeroization Methods

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	AES key used for encryption, decryption, and computing MAC tags	XTS: 256, 512 bits; Other modes: 128, 192, 256 bits - XTS: 128, 256 bits; Other modes: 128, 192, 256 bits	Symmetric key - CSP			Encryption/ Decryption Message authentication
HMAC key	HMAC key used computing MAC tags	112-524288 bits - 112-256 bits	Symmetric key - CSP			Message authentication
Key-derivation key	Key-derivation key used for: Key derivation	112-4096 bits - 112-256 bits	Symmetric key - CSP			Key derivation
Shared secret	Shared secret generated by (EC) Diffie-Hellman	224-8192 bits - 112-256 bits	Shared secret - CSP		Shared secret computation	Key derivation
Password	Password used to derive symmetric keys	8-128 characters - N/A	Password - CSP			Password-based key derivation
Derived key	Symmetric key derived from a key-derivation key, shared secret, or password	8-4096 bits - 112-256 bits	Symmetric key - CSP	Key derivation Password-based key derivation		
Entropy input	Entropy input used to seed the	128-384 bits - 128-384 bits	Entropy input - CSP	Random number generation		

© 2024 IBM Corporation/ 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
	DRBG					
DRBG seed	DRBG seed derived from entropy input	CTR_DRBG: 256, 320, 348 bits; Hash_DRBG: 440, 888 bits; HMAC_DRBG: 160, 256, 512 bits - CTR_DRBG: 128, 192, 256 bits; Hash_DRBG: 128, 256 bits; HMAC_DRBG: 128, 256 bits	Seed - CSP	Random number generation		Random number generation
DRBG internal state (V, Key)	Internal state of CTR_DRBG and HMAC_DRBG instances	CTR_DRBG: 256, 320, 348 bits HMAC_DRBG: 320, 512, 1024 bits - CTR_DRBG: 128, 192, 256 bits; HMAC_DRBG: 128, 256 bits	Internal state - CSP	Random number generation		Random number generation
DRBG internal state (V, C)	Internal state of Hash_DRBG instances	Hash_DRBG: 880, 1776 bits - Hash_DRBG: 128, 256 bits	Internal state - CSP	Random number generation		Random number generation
DH public key	Public key used for Diffie-Hellman	2048-8192 bits - 112-200 bits	Public key - PSP	Key pair generation		Shared secret computation Key pair verification
DH private key	Private key used for Diffie-	2048-8192 bits - 112-200	Private key - CSP	Key pair generation		Shared secret computation Key pair

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Hellman	bits				verification
EC public key	Public key used for ECDH and ECDSA	P-224, P-256, P-384, P-521 - 112-256 bits	Public key - PSP	Key pair generation		Signature verification Shared secret computation Key pair verification
EC private key	Private key used for ECDH and ECDSA	P-224, P-256, P-384, P-521 - 112-256 bits	Private key - CSP	Key pair generation		Signature generation Shared secret computation Key pair verification
RSA public key	Public key used for: Signature verification, Key pair generation; Related keys: RSA private key	Signature verification: 1024 and 2048-16384 bits; Key pair generation: 2048-16384 bits - Signature verification: 80 and 112-256 bits; Key pair generation: 112-256 bits	Public key - PSP	Key pair generation		Signature verification
RSA private key	Private key used RSA signature verification	2048-16384 bits - 112-256 bits	Private key - CSP	Key pair generation		Signature generation
Intermediate key generation value	Temporary value generated during key pair generation services	2048-16384 bits - 112-256 bits	Intermediate value - CSP	Key pair generation		Key pair generation

Table 18: SSP Table 1

© 2024 IBM Corporation/ 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
AES key	API input parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	
HMAC key	API input parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	
Key-derivation key	API input parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	
Shared secret	API input parameters API output parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	
Password	API input parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	
Derived key	API output parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	Key-derivation key:Derived From Shared secret:Derived From Password:Derived From
Entropy input		RAM:Plaintext	From generation until DRBG seed is created	Automatic Module reset	
DRBG seed		RAM:Plaintext	While the DRBG is being instantiated	Automatic Module reset	Entropy input:Derived From
DRBG internal state (V, Key)		RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	DRBG seed:Derived From
DRBG internal state (V, C)		RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	DRBG seed:Derived From
DH public key	API input parameters	RAM:Plaintext	Until the cipher handle is	Free cipher handle Module	DH private key:Paired With

© 2024 IBM Corporation/ 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
	API output parameters		freed	reset	
DH private key	API input parameters API output parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	DH public key:Paired With
EC public key	API input parameters API output parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	EC private key:Paired With
EC private key	API input parameters API output parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	EC public key:Paired With
RSA public key	API input parameters API output parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	RSA private key:Paired With
RSA private key	API input parameters API output parameters	RAM:Plaintext	Until the cipher handle is freed	Free cipher handle Module reset	RSA public key:Paired With
Intermediate key generation value		RAM:Plaintext	From service invocation to service completion	Automatic	

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, 2030.

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests

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 does not return control to the calling application until the tests are completed.

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A4365)	256-bit key	Message authentication	SW/FW Integrity	OSSL_PROV_PARAM_STATUS is set to 1	Used for fips.so

Table 20: 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. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A4361)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4365)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4366)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4367)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4368)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4361)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4365)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the

© 2024 IBM Corporation/ 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
						integrity test
SHA2-512 (A4366)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4367)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4368)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A4362)	32-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A4362)	32-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
AES-GCM (A4360)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4363)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4364)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4371)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4372)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4373)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4374)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4375)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the

© 2024 IBM Corporation/ 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
						integrity test
AES-GCM (A4376)	Encryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4360)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4363)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4364)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4371)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4372)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4373)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4374)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4375)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4376)	Decryption with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4357)	Decryption with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4358)	Decryption with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4359)	Decryption with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the

© 2024 IBM Corporation/ 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
						integrity test
KDF SP800-108 (A4381)	Counter mode, HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDA OneStep SP800-56Cr2 (A4382)	SHA2-224	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDA HKDF Sp800-56Cr1 (A4355)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4361)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4362)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4365)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4366)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4367)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4368)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4361)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4362)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4365)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63	SHA2-256	KAT	CAST	Module becomes	Key derivation	Test runs at power-on

© 2024 IBM Corporation/ 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
(A4366)				operational		before the integrity test
KDF ANS 9.63 (A4367)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4368)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF SSH (A4370)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF SSH (A4377)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF SSH (A4378)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF SSH (A4379)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
KDF SSH (A4380)	SHA-1	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4361)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4365)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4366)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4367)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4368)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Test runs at power-on before the integrity test
TLS v1.3 KDF	SHA2-256, extract and	KAT	CAST	Module becomes	Key derivation	Test runs at power-on

© 2024 IBM Corporation/ 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
(A4355)	expand			operational		before the integrity test
PBKDF (A4361)	SHA2-256, 24-character password, 288-bit salt, iteration count: 4096	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4362)	SHA2-256, 24-character password, 288-bit salt, iteration count: 4096	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4365)	SHA2-256, 24-character password, 288-bit salt, iteration count: 4096	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4366)	SHA2-256, 24-character password, 288-bit salt, iteration count: 4096	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4367)	SHA2-256, 24-character password, 288-bit salt, iteration count: 4096	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4368)	SHA2-256, 24-character password, 288-bit salt, iteration count: 4096	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
Counter DRBG (A4356)	AES-128	KAT	CAST	Module becomes operational	Instantiate, generate, reseed, generate (compliant with SP 800-90Ar1)	Test runs at power-on before the integrity test
Hash DRBG (A4356)	SHA2-256	KAT	CAST	Module becomes operational	Instantiate, generate, reseed, generate (compliant with SP 800-90Ar1)	Test runs at power-on before the integrity test

© 2024 IBM Corporation/ 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 (A4356)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Instantiate, generate, reseed, generate (compliant with SP 800-90Ar1)	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A4383)	ffdhe2048	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4361)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4365)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4366)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4367)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4368)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A4361)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A4362)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A4365)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A4366)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A4367)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen	PKCS#1 v1.5	KAT	CAST	Module	Digital	Test runs at

© 2024 IBM Corporation/ 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
(FIPS186-5) (A4368)	with 2048 bit key and SHA2-256			becomes operational	signature generation	power-on before the integrity test
RSA SigVer (FIPS186-5) (A4361)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A4362)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A4365)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A4366)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A4367)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A4368)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A4361)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A4362)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A4365)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A4366)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A4367)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen (FIPS186-5) (A4368)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A4361)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A4362)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A4365)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A4366)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A4367)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A4368)	P-224, P-256, P-384, and P-521 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
Safe Primes Key Generation (A4383)	N/A	PCT	PCT	Successful key pair generation	SP 800-56Ar3 Section 5.6.2.1.4	Key pair generation
ECDSA KeyGen (FIPS186-5) (A4361)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A4365)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A4366)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA	SHA2-256	PCT	PCT	Successful	Signature	Key pair

© 2024 IBM Corporation/ 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
KeyGen (FIPS186-5) (A4367)				key pair generation	generation & verification	generation
ECDSA KeyGen (FIPS186-5) (A4368)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A4361)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A4365)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A4366)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A4367)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A4368)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

Table 21: Conditional Self-Tests

Upon generation of a DH, RSA or EC key pair, the module will perform a pair-wise consistency test (PCT) as shown in the table above, which provides some assurance that the generated key pair is well formed. For DH key pairs, this tests consists of the PCT described in Section 5.6.2.1.4 of SP 800-56Ar3. For RSA and EC key pairs, this test consists of a signature generation and a signature verification operation.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A4365)	Message authentication	SW/FW Integrity	On demand	Manually

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A4361)	KAT	CAST	On demand	Manually
SHA-1 (A4365)	KAT	CAST	On demand	Manually
SHA-1 (A4366)	KAT	CAST	On demand	Manually
SHA-1 (A4367)	KAT	CAST	On demand	Manually
SHA-1 (A4368)	KAT	CAST	On demand	Manually

© 2024 IBM Corporation/ 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
SHA2-512 (A4361)	KAT	CAST	On demand	Manually
SHA2-512 (A4365)	KAT	CAST	On demand	Manually
SHA2-512 (A4366)	KAT	CAST	On demand	Manually
SHA2-512 (A4367)	KAT	CAST	On demand	Manually
SHA2-512 (A4368)	KAT	CAST	On demand	Manually
SHA3-256 (A4362)	KAT	CAST	On demand	Manually
SHA3-256 (A4362)	KAT	CAST	On demand	Manually
AES-GCM (A4360)	KAT	CAST	On demand	Manually
AES-GCM (A4363)	KAT	CAST	On demand	Manually
AES-GCM (A4364)	KAT	CAST	On demand	Manually
AES-GCM (A4371)	KAT	CAST	On demand	Manually
AES-GCM (A4372)	KAT	CAST	On demand	Manually
AES-GCM (A4373)	KAT	CAST	On demand	Manually
AES-GCM (A4374)	KAT	CAST	On demand	Manually
AES-GCM (A4375)	KAT	CAST	On demand	Manually
AES-GCM (A4376)	KAT	CAST	On demand	Manually
AES-GCM (A4360)	KAT	CAST	On demand	Manually
AES-GCM (A4363)	KAT	CAST	On demand	Manually
AES-GCM (A4364)	KAT	CAST	On demand	Manually
AES-GCM (A4371)	KAT	CAST	On demand	Manually
AES-GCM (A4372)	KAT	CAST	On demand	Manually
AES-GCM (A4373)	KAT	CAST	On demand	Manually
AES-GCM (A4374)	KAT	CAST	On demand	Manually
AES-GCM (A4375)	KAT	CAST	On demand	Manually
AES-GCM (A4376)	KAT	CAST	On demand	Manually
AES-ECB (A4357)	KAT	CAST	On demand	Manually

© 2024 IBM Corporation/ 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 (A4358)	KAT	CAST	On demand	Manually
AES-ECB (A4359)	KAT	CAST	On demand	Manually
KDF SP800-108 (A4381)	KAT	CAST	On demand	Manually
KDA OneStep SP800-56Cr2 (A4382)	KAT	CAST	On demand	Manually
KDA HKDF Sp800-56Cr1 (A4355)	KAT	CAST	On demand	Manually
KDF ANS 9.42 (A4361)	KAT	CAST	On demand	Manually
KDF ANS 9.42 (A4362)	KAT	CAST	On demand	Manually
KDF ANS 9.42 (A4365)	KAT	CAST	On demand	Manually
KDF ANS 9.42 (A4366)	KAT	CAST	On demand	Manually
KDF ANS 9.42 (A4367)	KAT	CAST	On demand	Manually
KDF ANS 9.42 (A4368)	KAT	CAST	On demand	Manually
KDF ANS 9.63 (A4361)	KAT	CAST	On demand	Manually
KDF ANS 9.63 (A4362)	KAT	CAST	On demand	Manually
KDF ANS 9.63 (A4365)	KAT	CAST	On demand	Manually
KDF ANS 9.63 (A4366)	KAT	CAST	On demand	Manually
KDF ANS 9.63 (A4367)	KAT	CAST	On demand	Manually
KDF ANS 9.63 (A4368)	KAT	CAST	On demand	Manually
KDF SSH (A4370)	KAT	CAST	On demand	Manually
KDF SSH (A4377)	KAT	CAST	On demand	Manually
KDF SSH (A4378)	KAT	CAST	On demand	Manually
KDF SSH (A4379)	KAT	CAST	On demand	Manually
KDF SSH (A4380)	KAT	CAST	On demand	Manually
TLS v1.2 KDF RFC7627 (A4361)	KAT	CAST	On demand	Manually
TLS v1.2 KDF RFC7627 (A4365)	KAT	CAST	On demand	Manually

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
TLS v1.2 KDF RFC7627 (A4366)	KAT	CAST	On demand	Manually
TLS v1.2 KDF RFC7627 (A4367)	KAT	CAST	On demand	Manually
TLS v1.2 KDF RFC7627 (A4368)	KAT	CAST	On demand	Manually
TLS v1.3 KDF (A4355)	KAT	CAST	On demand	Manually
PBKDF (A4361)	KAT	CAST	On demand	Manually
PBKDF (A4362)	KAT	CAST	On demand	Manually
PBKDF (A4365)	KAT	CAST	On demand	Manually
PBKDF (A4366)	KAT	CAST	On demand	Manually
PBKDF (A4367)	KAT	CAST	On demand	Manually
PBKDF (A4368)	KAT	CAST	On demand	Manually
Counter DRBG (A4356)	KAT	CAST	On demand	Manually
Hash DRBG (A4356)	KAT	CAST	On demand	Manually
HMAC DRBG (A4356)	KAT	CAST	On demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A4383)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4361)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4365)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4366)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4367)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4368)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A4361)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A4362)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A4365)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5)	KAT	CAST	On demand	Manually

© 2024 IBM Corporation/ 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
(A4366)				
RSA SigGen (FIPS186-5) (A4367)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A4368)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A4361)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A4362)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A4365)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A4366)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A4367)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A4368)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A4361)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A4362)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A4365)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A4366)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A4367)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A4368)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A4361)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A4362)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A4365)	KAT	CAST	On demand	Manually

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) (A4366)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A4367)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A4368)	KAT	CAST	On demand	Manually
Safe Primes Key Generation (A4383)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A4361)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A4365)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A4366)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A4367)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A4368)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A4361)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A4365)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A4366)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A4367)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A4368)	PCT	PCT	On demand	Manually

Table 23: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The module immediately stops functioning	Software integrity test failure	Module reset	OSSL_PROV_PARAM_STATUS is set to 0 or Module is aborted

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Conditions	Recovery Method	Indicator
		CAST failure PCT failure		

Table 24: Error States

In the error state, the module immediately stops functioning and ends the application process. Consequently, the data output interface is inhibited, and the module accepts no more inputs or requests (as the module is no longer running).

10.5 Operator Initiation of Self-Tests

The software integrity tests and cryptographic algorithm self-tests can be invoked on demand by resetting the module. The pair-wise consistency tests can be invoked on demand by requesting the key pair generation service.

© 2024 IBM Corporation/ 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

The IBM DataPower security appliance ships with signed firmware which contains the module embedded in it. No additional steps are required to install or initialize the module.

11.2 Administrator Guidance

After delivery of the DataPower security appliance, the module name and version can be verified by executing the “openssl list -providers” command. The FIPS provider will be listed in the output as follows:

```
  fips
    name: IBM DataPower FIPS Provider
    version: 3.0.9-B3346E1D91BA83B7BAB52F472F3E6A0D
    status: active
```

The cryptographic boundary consists only of the FIPS provider as listed. If any other OpenSSL or third-party provider is invoked, the user is not interacting with the module specified in this Security Policy.

11.3 Non-Administrator Guidance

There is no non-administrator guidance.

11.6 End of Life

As the module does not persistently store SSPs, secure sanitization of the module consists of unloading the module. This will zeroize all SSPs in volatile memory.

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

Certain cryptographic subroutines and algorithms are vulnerable to timing analysis. The module mitigates this vulnerability by using constant-time implementations. This includes, but is not limited to:

- Big number operations: computing GCDs, modular inversion, multiplication, division, and modular exponentiation (using Montgomery multiplication)
- Elliptic curve point arithmetic: addition and multiplication (using the Montgomery ladder)
- Vector-based AES implementations

In addition, RSA, ECDSA, ECDH, and DH employ blinding techniques to further impede timing and power analysis. No configuration is needed to enable the aforementioned countermeasures.

© 2024 IBM Corporation/ 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
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CPACF	CP Assist for Cryptographic Functions
CSP	Critical Security Parameter
CTR	Counter
CTS	Ciphertext Stealing
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EVP	Envelope
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GMAC	Galois Counter Mode Message Authentication Code
HKDF	HMAC-based Key Derivation Function
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange
KAS	Key Agreement Scheme
KAT	Known Answer Test
KBKDF	Key-based Key Derivation Function
KW	Key Wrap
KWP	Key Wrap with Padding
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OAEP	Optimal Asymmetric Encryption Padding
OFB	Output Feedback
PAA	Processor Algorithm Acceleration
PCT	Pair-wise Consistency Test
PBKDF2	Password-based Key Derivation Function v2
PKCS	Public-Key Cryptography Standards
PSP	Public Security Parameter
PSS	Probabilistic Signature Scheme
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSH	Secure Shell
SSP	Sensitive Security Parameter
TLS	Transport Layer Security
XOF	Extendable Output Function

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Glossary and abbreviations

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix B. References

ANS X9.42-2001	**Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography** 2001 https://webstore.ansi.org/standards/ascx9/ansix9422001
ANS X9.63-2001	**Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography** 2001 https://webstore.ansi.org/standards/ascx9/ansix9632001
FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
FIPS 140-3 IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 180-4	**Secure Hash Standard (SHS)** March 2012 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS 186-4	**Digital Signature Standard (DSS)** July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS 186-5	**Digital Signature Standard (DSS)** February 2023 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS 197	**Advanced Encryption Standard** November 2001 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf
FIPS 198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** February 2003 https://www.ietf.org/rfc/rfc3447.txt
RFC 3526	**More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)** May 2003 https://www.ietf.org/rfc/rfc3526.txt

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

RFC 5288 **AES Galois Counter Mode (GCM) Cipher Suites for TLS**
August 2008
https://www.ietf.org/rfc/rfc5288.txt

RFC 7919 **Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)**
August 2016
https://www.ietf.org/rfc/rfc7919.txt

RFC 8446 **The Transport Layer Security (TLS) Protocol Version 1.3**
August 2018
https://www.ietf.org/rfc/rfc8446.txt

SP 800-38A **Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP 800-38A Addendum **Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode**
October 2010
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a-add.pdf

SP 800-38B **Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication**
May 2005
https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

SP 800-38C **Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality**
May 2004
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

SP 800-38D **Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**
November 2007
https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

SP 800-38E **Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices**
January 2010
https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

SP 800-38F **Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping**
December 2012
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

SP 800-52r2 **Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations**
August 2019
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

SP 800-56Ar3 **Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography**
April 2018
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

SP 800-56Cr2	**Recommendation for Key-Derivation Methods in Key-Establishment Schemes** August 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf
SP 800-90Ar1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP 800-90B	**Recommendation for the Entropy Sources Used for Random Bit Generation** January 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
SP 800-108r1	**NIST Special Publication 800-108 - Recommendation for Key Derivation Using Pseudorandom Functions** August 2022 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-108r1.pdf
SP 800-131Ar2	**Transitioning the Use of Cryptographic Algorithms and Key Lengths** March 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
SP 800-132	**Recommendation for Password-Based Key Derivation - Part 1: Storage Applications** December 2010 https://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
SP 800-133r2	**Recommendation for Cryptographic Key Generation** June 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf
SP 800-135r1	**Recommendation for Existing Application-Specific Key Derivation Functions** December 2011 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
SP 800-140Br1	**CMVP Security Policy Requirements** November 2023 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf

© 2024 IBM Corporation/ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.