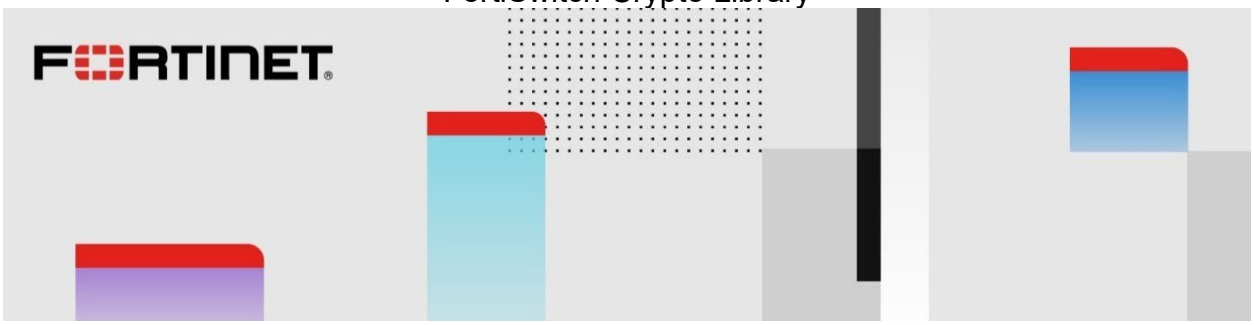
Fortinet Technologies Inc

FortiSwitch Crypto Library



FIPS 140-3 Non-Proprietary Security Policy

Document Version:	0.1
Publication Date:	Wednesday, Mar 18, 2026
Software Version:	FortiSwitch 7.6

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FortiSwitch 7.6 Crypto Library Module FIPS 140-3 Level 1 Software Security Policy

11-760-1094842-20241205

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 7.6 of the FortiSwitch Crypto Library, hereafter referred to as the Module. It contains the security rules under which the Module must operate and describes how this Module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 Module.

The Federal Information Processing Standards Publication 140-3 - Security Requirements for Cryptographic Modules (FIPS 140-3) details the United States Federal Government requirements for cryptographic modules. Detailed information about the FIPS 140-3 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

This policy deals specifically with operation and implementation of the modules in the technical terms of the FIPS 140-3 standard and the associated validation program. Other Fortinet product manuals, guides and technical notes can be found at the Fortinet technical documentation website at https://docs.fortinet.com.

Additional information on the entire Fortinet product line can be obtained from the following sources:

- Find general product information in the product section of the Fortinet corporate website at https://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at https://support.fortinet.com/.
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at https://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at https://wwww.fortiguard.com.

2 Cryptographic Module Specification

This FortiSwitch Crypto Library, hereafter denoted as the Module, is a software cryptographic module that exclusively provides cryptographic services for Fortinet's FortiSwitch family of Ethernet switches.

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated Ethernet Switches. The Module is exclusively used in the FortiSwitch appliances.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 1. The Module is a multi-chip standalone embodiment. The cryptographic boundary includes the following components:

- OpenSSL
- Fortinet proprietary CTR_DRBG
- FortiSwitch CPU Jitter Entropy Library 1.0

Tested Operational Environment's Physical Perimeter (TOEPP):

The physical perimeter of the module is the physical chassis of the FortiSwitch appliance the module is running on.

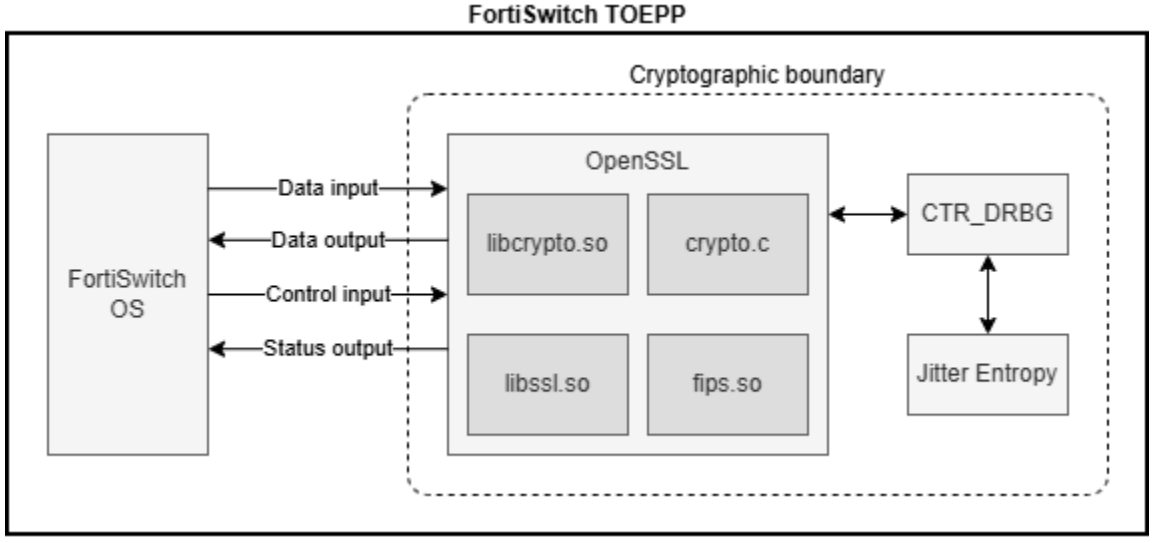


Figure 1: Block Diagram

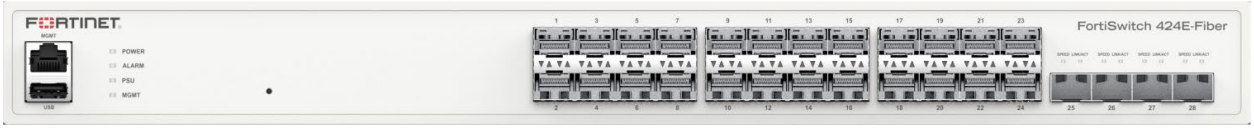


Figure 2: Physical perimeter

2.2 Module Identification

2.2.1 Tested Module Identification

The Module is tested on the following operational environment.

Package or File Name	Software/ Firmware Version	Features	Integrity Test
FSW_424E_FIBER-v7-build8073-FIPS-CC-76-01-FORTINET.out	7.6		RSA

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

The Module is included in the FortiSwitch firmware, which comes as a single binary .out file in a Fortinet proprietary format. This file is protected by an RSA digital signature to ensure its authenticity.

2.2.2 Tested Operational Environments

The Module is tested on the following operational environment

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
FortiSwitchOS 7.6.1	FSW-424E-Fiber	Broadcom BCM 56174	No		7.6

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

2.2.3 Vendor-Affirmed Operational Environments

The Module can also be executed on any of the following FortiSwitch appliances and remain vendor affirmed FIPS 140-3 compliant:

Operating System	Hardware Platform
FortiSwitchOS	FSR_424F_POE
FortiSwitchOS	FSW_1048E
FortiSwitchOS	FSW_108F
FortiSwitchOS	FSW_2048F
FortiSwitchOS	FSW_3032E
FortiSwitchOS	FSW_424E
FortiSwitchOS	FSW_424E_FPOE
FortiSwitchOS	FSW_424E_POE
FortiSwitchOS	FSW_426_FPOE_MG
FortiSwitchOS	FSW_448E
FortiSwitchOS	FSW_448E_FPOE
FortiSwitchOS	FSW_448E_POE
FortiSwitchOS	FSW_624F
FortiSwitchOS	FSW_624F_FPOE
FortiSwitchOS	FSW_648F
FortiSwitchOS	FSW_648F_FPOE
FortiSwitchOS	FSW_1024E
FortiSwitchOS	FSW_T1024E

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

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

2.3 Excluded Components

There are no components within the cryptographic boundary that are excluded from the module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	Approved mode can only be enabled via console access. The approved mode only consists of FIPS 140-3 compliant cryptography.	Approved	FIPS-CC indicator on CLI/GUI i.e Global Indicator. Thus an implicit indication via the successful completion of a service is sufficient FIPS-CC indicator on CLI/GUI.

Table 5: Modes List and Description

Mode Change Instructions and Status:

The Module only has one mode of operation and thus cannot change mode.

2.5 Algorithms

2.5.1 Approved Algorithms

The Module implements the Approved cryptographic algorithms listed the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6436	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6436	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - No	SP 800-38A
AES-GCM	A6436	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 16, 128, 136, 256, 264 AAD Length - AAD Length: 0, 128, 136, 256	SP 800-38D
Counter DRBG	A6436	Prediction Resistance - No Supports Reseed - Yes Mode - AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0-256 Increment 256 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0-256 Increment 256 Returned Bits - 256	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6436	Curve - P-256, P-384, P-521 Secret Generation Mode - extra bits, testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6436	Curve - P-256, P-384, P-521	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigGen (FIPS186-5)	A6436	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6436	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA-1	A6436	MAC - MAC: 32-160 Increment 8 Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6436	MAC - MAC: 32-224 Increment 8 Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6436	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6436	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6436	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6436	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A6436	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SNMP (CVL)	A6436	Password Length - Password Length: 64, 8192 Engine ID - 000002b87766554433221100, 800002B805123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456	SP 800-135 Rev. 1
KDF SSH (CVL)	A6436	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A6436	Key Generation Mode - probable Modulo - 2048, 3072, 4096 p mod 8 - 0 Primality Tests - 2powSecStr q mod 8 - 0 Info Generated By Server - No Private Key Format - standard Public Exponent Mode - random	FIPS 186-5
RSA SigGen (FIPS186-5)	A6436	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5
RSA SigVer (FIPS186-5)	A6436	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Public Exponent Mode - random	FIPS 186-5
Safe Primes Key	A6436	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
Generation			
Safe Primes Key Verification	A6436	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
SHA-1	A6436	Message Length - Message Length: 160, 0-65528 Increment 8	FIPS 180-4
SHA2-224	A6436	Message Length - Message Length: 224, 0-65528 Increment 8	FIPS 180-4
SHA2-256	A6436	Message Length - Message Length: 256, 0-65528 Increment 8	FIPS 180-4
SHA2-384	A6436	Message Length - Message Length: 384, 0-65528 Increment 8	FIPS 180-4
SHA2-512	A6436	Message Length - Message Length: 512, 0-65528 Increment 8	FIPS 180-4
SHA3-256	A6436	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
TLS v1.2 KDF RFC7627 (CVL)	A6436	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 512-1024 Increment 8	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A6436	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE	SP 800-135 Rev. 1

Table 6: Approved Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AuthCipher	BC-Auth	Encryption and decryption using authenticated block cipher modes.		AES-GCM: (A6436)
Cipher	BC-UnAuth	Encryption and decryption using unauthenticated block cipher modes.		AES-CBC: (A6436) AES-CTR: (A6436)
DH KeyGen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation Safe Primes		Safe Primes Key Generation: (A6436)
DH KeyVer	AsymKeyPair-KeyVer	Safe primes key pair verification		Safe Primes Key Verification: (A6436)
ECDSA KeyGen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation		ECDSA KeyGen (FIPS186-5): (A6436)
ECDSA KeyVer	AsymKeyPair-KeyVer	Asymmetric Key-Pair Verification		ECDSA KeyVer (FIPS186-5): (A6436)
ECDSA SigGen	DigSig-SigGen	Digital Signature Generation		ECDSA SigGen (FIPS186-5): (A6436) SHA2-256: (A6436) SHA2-384: (A6436) SHA2-512: (A6436)

Name	Type	Description	Properties	Algorithms
ECDSA SigVer	DigSig-SigVer	Digital Signature Verification		ECDSA SigVer (FIPS186-5): (A6436) SHA2-256: (A6436) SHA2-384: (A6436) SHA2-512: (A6436)
Entropy	ENT-ESV	Entropy generation		SHA3-256: (A6436)
Hash	SHA	Secure Hash Standard		SHA-1: (A6436) SHA2-224: (A6436) SHA2-384: (A6436) SHA2-512: (A6436) SHA2-256: (A6436)
KDF SNMP	KAS-135KDF	Key derivation within SNMP		KDF SNMP: (A6436) SHA-1: (A6436)
KDF SSH	KAS-135KDF	Key derivation within SSH		KDF SSH: (A6436) SHA-1: (A6436) SHA2-256: (A6436)
KDF TLS 1.2	KAS-135KDF	Key Derivation within TLS 1.2		TLS v1.2 KDF RFC7627: (A6436) HMAC-SHA2-256: (A6436) HMAC-SHA2-384: (A6436) HMAC-SHA2-512: (A6436) SHA2-256: (A6436) SHA2-384: (A6436) SHA2-512: (A6436)
KDF TLS 1.3	KAS-135KDF	Key Derivation within TLS 1.3		TLS v1.3 KDF: (A6436) HMAC-SHA2-256: (A6436) HMAC-SHA2-384: (A6436) SHA2-256: (A6436) SHA2-384: (A6436)
MAC	MAC	Message authentication code generation and verification		HMAC-SHA-1: (A6436) HMAC-SHA2-224: (A6436) HMAC-SHA2-256: (A6436) HMAC-SHA2-384: (A6436) HMAC-SHA2-512: (A6436) SHA-1: (A6436) SHA2-224: (A6436) SHA2-256: (A6436) SHA2-384: (A6436) SHA2-512: (A6436)
RBG	DRBG	Random Number Generation		Counter DRBG: (A6436) AES-CTR: (A6436)
RSA KeyGen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation		RSA KeyGen (FIPS186-5): (A6436)
RSA SigGen	DigSig-SigGen	Digital Signature Generation		RSA SigGen (FIPS186-5):

Name	Type	Description	Properties	Algorithms
				(A6436) SHA2-224: (A6436) SHA2-256: (A6436) SHA2-384: (A6436) SHA2-512: (A6436)
RSA SigVer	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-5): (A6436) SHA2-224: (A6436) SHA2-256: (A6436) SHA2-384: (A6436) SHA2-512: (A6436)
SSC-ECC	KAS-SSC	Shared secret computation for ECC schemes		KAS-ECC-SSC Sp800-56Ar3: (A6436)
SSC-FFC	KAS-SSC	Shared secret computation for FFC schemes		KAS-FFC-SSC Sp800-56Ar3: (A6436)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV Uniqueness

The AES GCM implementation generates GCM IVs deterministically as specified in SP800-38D Section 8.2.1 using the following protocols:

SSHv2

This Module is compliant with RFCs 4252, 4253 and the rules for using AES-GCM documented in RFC 5647. The IV is only used in the context of the AES-GCM mode encryptions within the SSHv2 protocol.

No more than 2^{64}–1 AES-GCM encryptions may be performed in the same session and if the invocation counter reaches its maximum value 2^{64}–1, the next AES-GCM encryption is performed with the invocation counter set to either 0 or 1.

When a session is terminated for any reason, a new key and a new initial IV is derived.

In case the Module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is established. This condition is not enforced by the Module but is met implicitly. The Module does not retain any state across reset or power-cycles. Re-connection occurs with a fresh key establishment operation and the associated SSPs

TLS 1.2

The Module is compliant with TLS v1.2 and SP800-52 Rev2, Section 3.3.1. The Module supports TLS 1.2 GCM Cipher Suites for TLS, as described in RFCs 5116, 5246, 5288 and 5289. The module only uses the TLS protocol version 1.2 to be compliant with FIPS140-3 [IG C.H], Option 1.

During operational testing, the Module was tested against an independent version of TLS and found to behave correctly.

The counter portion of the IV is set by the Module within its cryptographic boundary.

The nonce_explicit part of the IV is incremented each time an AES-GCM computation is performed. The Module establishes a new session key when the nonce_explicit part of the IV exhausts the maximum number of possible values (2^{32}-1).

When a session is terminated for any reason, a new key and a new IV are derived.

In case the Module's power is lost and then restored, a new key for use AES-GCM will be established. This condition is not enforced by the Module but is met implicitly. The Module does not retain any state across reset or power-cycles. Re-connection occurs with a fresh key establishment operation and the associated SSPs.

TLS 1.3

The Module supports the TLS 1.3 GCM cipher suites from section 3.3.1.2 of NIST SP 800-52rev2. The AES-GCM IV generation is performed internally, is compliant with the RFC 8446 Section 5.3 and Section 8.1, and is only used for the TLS 1.3 protocol. Thus, the module is compliant with scenario 5 of FIPS 140-3 [IG C.H].

During operational testing, the Module was tested against an independent version of TLS1.3 and found to behave correctly.

2.7.2 KAS-SSC

KAS-SSC [56Ar3] - Per [IG] D.F Scenario 2 path (2), compliant with the derivation of a shared secret Z in one or more of the key agreement schemes in Section 6 of SP 800-56Arev3.

2.7.3 Approved Modulus Sizes for RSA Digital Signature

Following [IG C.F], RSA SigGen (FIPS 186-5) and RSA SigVer (FIPS 186-5) have been CAVP tested with all supported approved RSA modulus lengths (2048, 3072, 4096). This is documented in the Approved Algorithms table. There are no modulus sizes available in approved services which have not been CAVP tested. The minimum number of the Miller-Rabin tests used in primality testing is consistent with Table B.1 in FIPS 186-5.

2.8 RBG and Entropy

Cert Number	Vendor Name
E118	Fortinet Technologies

Table 8: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
FortiSwitch CPU Jitter Entropy Library 1.0	Non-Physical	FortiSwitch OS	Full Entropy	256	SHA3-256

Table 9: Entropy Sources

2.9 Key Generation

Asymmetric keys are generated in conformance to methods described in FIPS 186-5 and 800-56Arev3. The algorithms that implement these methods have been CAVP tested.

The module does not generate symmetric keys.

2.10 Key Establishment

The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS.

2.11 Industry Protocols

The Module conforms to FIPS 140-3 IG D.C References to the Support of Industry Protocols: while it provides SP 800-56A Rev. 3 conformant schemes and API entry points oriented to HTTS/TLS usage. The Module also conforms to FIPS 140-3 IG D.C for SSH and SNMP but does not contain the full implementation of the SSH or SNMP protocols. The following caveat is required:

No parts of the SSH or SNMP protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

2.12 Additional Information

When the module is powered on, it initiates self-tests against the algorithms claimed in section 2.5. Once all the tests are passed, the module continues to function in the approved mode. Please refer to section 11.1 start up procedure for installation process.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	API input parameters for data- plain text and cipher text, digital signatures, SSPs
N/A	Data Output	API output parameters for data- encrypted or decrypted, digital signatures, hashes, SSPs
N/A	Control Input	API input commands from FortiSwitch console, Web GUI
N/A	Status Output	API return values to the FortiSwitch appliance

Table 10: Ports and Interfaces

The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The Module is Level 1 and does not implement any Authentication techniques.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer	None

Table 11: Roles

The Module only supports Cryptographic Officer (CO). The Crypto Officer role has read-write- execute access to all the Module's administrative services. The initial Crypto Officer can create additional operator accounts. These additional accounts are assigned the Crypto Officer role and can be assigned a range of read-write-execute or read only access permissions including the ability to create operator accounts.

The Module does not provide a Maintenance role

The Module does not support concurrent operators.

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

The access types are abbreviated as follows:

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Decrypt	Network packet decryption	Implicit	Ciphertext, key	Plaintext	AuthCipher Cipher	CO - SNMP-LK: W,E - SSH-SEK: W,E - TLS-SEK: W,E
Encrypt	Network packet encryption	Implicit	Plaintext, key	Ciphertext	AuthCipher Cipher	CO - SNMP-LK: E,W - SSH-SEK: W,E - TLS-SEK: W,E
Hash	Hash generation	Implicit	Message	Hash	Hash	CO
Key Generation	Asymmetric key pair generation	Implicit	Command	Key pair	ECDSA KeyGen RSA KeyGen DH KeyGen	CO - DRBG output: E - ECDSA Public Key: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- ECDSA Private Key: G,R - RSA Public Key: G,R - RSA Private Key: G,R - DH Private key: G,R - DH Public key: G,R - EC Private key: G,R - EC Public key: G,R
Key Verification	Key pair verification	Implicit	API Call	Keys Verified	ECDSA KeyVer DH KeyVer	CO - DH Public key: G,W,E - DH Private key: G,W,E - EC Public key: G,W,E - EC Private key: G,W,E
MAC	Network packet authentication	Implicit	Message, key	MAC	MAC	CO - SSH-SAK: W,E - TLS-SAK: W,E
Module Initialization	Initialize and install the Module	Implicit	Power On	None	None	CO
Random Bit Generation	Random bit generation	Implicit	Command, number of bits requested	Random bits	Entropy RBG	CO - DRBG Entropy Input: G,E - DRBG Seed: G,E - DRBG Key: G,E - DRBG V: G,E - DRBG output: G,R
SNMP Key Derivation	SNMP Key Derivation	Implicit	Password, engine ID	Localized key	KDF SNMP	CO - SNMP-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						UK: G,Z - SNMP-LK: G,R
SSH Key Derivation	SSH Key Derivation	Implicit	Shared secret, session hash, session ID	Key	KDF SSH	CO - DH Shared secret: W,E - EC Shared secret: W,E - SSH-SAK: G,R - SSH-SEK: G,R
Self-Test	Perform known answer tests for all the cryptographic algorithms	Implicit	Power On for startup self-tests, CLI/Console command for on-demand self-tests	Pass/Fail status via Console output	None	CO
Shared secret computation	Computation of shared secret	Implicit	Private and peer public key	Shared secret	SSC-ECC SSC-FFC	CO - EC Peer public key: W,E,Z - EC Private key: W,E,Z - EC Shared secret: G,R - DH Peer public key: W,E,Z - DH Private key: W,E,Z - DH Shared secret: G,R
Show Version	Shows module's name and versioning	Implicit	CLI/Console command	Module Base Name + Module Version Number	None	CO
Show status	Shows module's status	Implicit	CLI/Console command	CLI/Console status output	None	CO
Sign	Signature generation	Implicit	Message, key	Signature	ECDSA SigGen RSA SigGen	CO - ECDSA Private Key: W,E - RSA Private Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TLSv1.2 Key Derivation	TLSv1.2 Key Derivation functions	Implicit	Pre-master or master secret, session nonce or hash	Master secret or session keys	KDF TLS 1.2	CO - TLS-PMS: W,E - TLS-MS: G,W,E - TLS-SAK: G,R - TLS-SEK: G,R
TLSv1.3 Key Derivation	TLSv1.3 Key Derivation functions	Implicit	Secret, label	Secret or key	KDF TLS 1.3	CO - TLS-MS: G,R,W,E - TLS-SEK: G,R
Verify	Signature verification	Implicit	Message, key, signature	Ruling	ECDSA SigVer RSA SigVer	CO - ECDSA Public Key: W,E - RSA Public Key: W,E
Zeroization	Zeroises flash memory of host device	Implicit	CLI Command	-	None	CO

Table 12: Approved Services

4.4 Non-Approved Services

The module does not provide any non-approved services.

4.5 External Software/Firmware Loaded

The module does not support software loading.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module is composed of the following single software consisting following separate component(s):

- Component 1: FSW_424E_FIBER-v7-build8073-FIPS-CC-76-01-FORTINET.out

The Module uses RSA digital signature as an approved integrity technique for software integrity.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by using the following Module Self-Test service command:

```
execute system security kat Firmware-integrity on CLI
```

6 Operational Environment

6.1 Operational Environment Type and Requirements

The Operational environment consists of the combination of the FortiSwitchOS operating system, the Broadcom BCM 56174 processor and the FortiSwitch platform. The FortiSwitchOS operating system can only be installed, and run, on a FortiSwitch appliance. The FortiSwitchOS operating system provides a proprietary and modifiable operating system. For specific information regarding the operational environment, please refer to section 2.3. Please refer to section 11.1 for more information on the installation process. The Module's CSPs and key components are entered into or output in plaintext form only within the operational environment.

Type of Operational Environment: Modifiable

7 Physical Security

Not applicable as the Module is validated against FIPS 140-3 level 1.

8 Non-Invasive Security

The Module does not implement any mitigation methods against non-invasive attacks.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Only stored in volatile memory (RAM).	Dynamic

Table 13: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API Input	API Calling Process	RAM	Plaintext	Manual	Electronic	
API Output	RAM	API Calling Process	Plaintext	Manual	Electronic	

Table 14: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Auto	Automatic zeroisation of SSPs that are no longer needed.	Memory is overwritten with 0's	N/A
Reboot	Power-cycle the host device	All RAM is zeroised by a power-cycle.	Unplugging the host device

Table 15: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DH Peer public key	Peer public key for key agreement	2048 to 8192 - 112 to 200	Asymmetric - PSP			SSC-FFC
DH Private key	Private key for key agreement	2048 to 8192 - 112 to 200	Asymmetric - CSP	DH KeyGen		SSC-FFC
DH Public key	Public key for key agreement	2048 to 8192 - 112 to 200	Asymmetric - PSP	DH KeyGen		SSC-FFC
DH Shared secret	Shared secret computation	2048 to 8192 - 112 to 200	Shared secret - CSP		SSC-FFC	SSC-FFC
DRBG Entropy Input	Input string from the entropy pool	384 - 384	Entropy - CSP	Entropy		RBG
DRBG Key	Internal state values for the DRBG	256 - -	DRBG State - CSP	RBG		RBG
DRBG Seed	256-bit seed used by the DRBG	384 - 384	DRBG Seed - CSP	RBG		RBG
DRBG V	Internal state values for the DRBG	128 - -	DRBG State - CSP	RBG		RBG
DRBG output	Output of the DRBG	256 - 256	DRBG - CSP	RBG		ECDSA KeyGen ECDSA SigGen RSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						KeyGen RSA SigGen DH KeyGen
EC Peer public key	Peer public key used for key agreement	P-256, P-384, P-521 - 128, 192, 256	Asymmetric - PSP			SSC-ECC
EC Private key	Private key used for key agreement	P-256, P-384, P-521 - 128, 192, 256	Asymmetric - CSP	ECDSA KeyGen		SSC-ECC
EC Public key	Public key used for key agreement	P-256, P-384, P-521 - 128, 192, 256	Asymmetric - PSP	ECDSA KeyGen		
EC Shared secret	Shared secret	256, 384, 521 - 128, 192, 256	Shared secret - CSP		SSC-ECC	SSC-ECC
ECDSA Private Key	ECDSA Signature generation key	P-256, P-384, P-521 - 128, 192, 256	Asymmetric - CSP	ECDSA KeyGen		ECDSA SigGen
ECDSA Public Key	ECDSA Signature verification key	P-256, P-384, P-521 - 128, 192, 256	Asymmetric - PSP	ECDSA KeyGen		ECDSA SigVer
RSA Private Key	RSA Signature generation key	2048, 3072, 4096 - 112 to 150	Asymmetric - CSP	RSA KeyGen		RSA SigGen
RSA Public Key	RSA Signature verification key	2048, 3072, 4096 - 112 to 150	Asymmetric - PSP	RSA KeyGen		RSA SigVer
SNMP-LK	SNMP localized key	160 - 128	Symmetric - CSP	KDF SNMP		Cipher
SNMP-UK	SNMP User key	160 - 128	Symmetric - CSP	KDF SNMP		KDF SNMP
SSH-SAK	SSH session authentication key, used to verify data authenticity	128, 192, 256 - 112, 128, 192, 256	Symmetric - CSP	KDF SSH		MAC
SSH-SEK	SSH session encryption key, used to encrypt/decrypt data	128, 192, 256 - 112, 128, 192, 256	Symmetric - CSP	KDF SSH		AuthCipher Cipher
TLS-MS	TLS Master secret	384 - 384	Secret - CSP	KDF TLS 1.2 KDF TLS 1.3		KDF TLS 1.2 KDF TLS 1.3
TLS-PMS	TLS 1.2 Pre-Master Secret	256 to 521, 2048 to 8192 - 112 to 256	Shared secret - CSP		SSC-ECC SSC-FFC	KDF TLS 1.2
TLS-SAK	TLS 1.2 Session authentication key, used for authentication of data packets	160 to 384 - 160 to 384	Symmetric - CSP	KDF TLS 1.2		MAC
TLS-SEK	TLS Session encryption key, used to	128, 256 - 128, 256	Symmetric - CSP	KDF TLS 1.2		AuthCipher Cipher

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	encrypt/decrypt data packets			KDF TLS 1.3		

Table 16: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DH Peer public key	API Input	RAM:Plaintext	-	Auto	
DH Private key	API Input API Output	RAM:Plaintext	-	Auto	DH Public key:Paired With
DH Public key	API Output	RAM:Plaintext	-	Auto	DH Private key:Paired With
DH Shared secret	API Output	RAM:Plaintext	-	Auto	DH Private key:Derived From DH Peer public key:Derived From
DRBG Entropy Input		RAM:Plaintext	-	Reboot	
DRBG Key		RAM:Plaintext	-	Reboot	DRBG Seed:Derived From
DRBG Seed		RAM:Plaintext	-	Reboot	DRBG Entropy Input:Derived From
DRBG V		RAM:Plaintext	-	Reboot	DRBG Seed:Derived From
DRBG output	API Output	RAM:Plaintext	-	Reboot	DRBG Key:Derived From DRBG V:Derived From
EC Peer public key	API Input	RAM:Plaintext	-	Auto	
EC Private key	API Input API Output	RAM:Plaintext	-	Auto	EC Public key:Paired With
EC Public key	API Output	RAM:Plaintext	-	Auto	EC Private key:Paired With
EC Shared secret	API Output	RAM:Plaintext	-	Auto	EC Peer public key:Derived From EC Private key:Derived From
ECDSA Private Key	API Input API Output	RAM:Plaintext	-	Reboot	ECDSA Public Key:Paired With
ECDSA Public Key	API Input API Output	RAM:Plaintext	-	Reboot	ECDSA Private Key:Paired With
RSA Private Key	API Input API Output	RAM:Plaintext	-	Reboot	RSA Public Key:Paired With
RSA Public Key	API Input API Output	RAM:Plaintext	-	Reboot	RSA Private Key:Paired With
SNMP-LK	API Output	RAM:Plaintext	-	Reboot	SNMP-UK:Derived From
SNMP-UK		RAM:Plaintext	-	Auto	
SSH-SAK	API Output	RAM:Plaintext	-	Reboot	DH Shared secret:Derived From EC Shared secret:Derived From
SSH-SEK	API Output	RAM:Plaintext	-	Reboot	DH Shared secret:Derived From EC Shared secret:Derived From
TLS-MS	API Input API Output	RAM:Plaintext	-	Reboot	TLS-PMS:Derived From
TLS-PMS	API Input API Output	RAM:Plaintext	-	Reboot	DH Shared secret:Alias of EC Shared secret:Alias of
TLS-SAK	API Input API Output	RAM:Plaintext	-	Reboot	TLS-MS:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS-SEK	API Input API Output	RAM:Plaintext	-	Reboot	TLS-MS:Derived From

Table 17: SSP Table 2

9.5 Transitions

The module implements the following security methods that are forecasted to transition over the lifetime of the validation:

- SHA-1

10 Self-Tests

10.1 Pre-Operational Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Self-tests provide the operator with assurance that faults have not been introduced to the Module that can hinder correct operation as outlined in ISO/IEC 19790:2012 section 7.10.1. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

The Module performs the following pre-operational self-tests in the table below:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Integrity test	2048-bit RSA, SHA2-256	SigVer	SW/FW Integrity	Successful boot	Signature verification

Table 18: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB Encrypt	128-bit key	KAT	CAST	Successful boot	Encrypt	On boot
AES-ECB Decrypt	128-bit key	KAT	CAST	Successful boot	Decrypt	On boot
AES-GCM Encrypt	256-bit key	KAT	CAST	Successful boot	Encrypt	On boot
AES-GCM Decrypt	256-bit key	KAT	CAST	Successful boot	Decrypt	On boot
CTR_DRBG	128-bit key	KAT	CAST	Successful boot	Instantiate, Generate, and Reseed	On boot
DH Key pairs	-	PCT	PCT	No error	Shared secret computation	On Key Generation
EC Key pairs	-	PCT	PCT	No error	Sign then verify	On Key Generation
ECDSA SigGen	P-224	KAT	CAST	Successful boot	Sign	On boot
ECDSA SigVer	P-224	KAT	CAST	Successful boot	Verify	On boot
HMAC	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Successful boot	Generate	On boot
RSA SigGen	2048-bit	KAT	CAST	Successful boot	Sign	On boot
RSA SigVer	2048-bit	KAT	CAST	Successful boot	Verify	On boot
RSA Key pairs	-	PCT	PCT	No error	Encrypt then decrypt	On Key Generation
SHA-1	-	KAT	CAST	Successful boot	Generate	On boot
SHA2-256	SHA2-224, SHA2-256	KAT	CAST	Successful boot	Generate	On boot
SHA2-512	SHA2-384, SHA2-512	KAT	CAST	Successful boot	Generate	On boot
SHA3	-	KAT	CAST	Successful boot	Generate	On boot
SSC-ECC	P-256	KAT	CAST	Successful boot	Shared secret computation	On boot
SSC-FFC	ffdhe2048	KAT	CAST	Successful boot	Shared secret computation	On boot
SSH KDF	SHA2-256	KAT	CAST	Successful boot	Derive	On boot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TLS 1.2KDF	SHA2-256	KAT	CAST	Successful boot	Derive	On boot
TLS 1.3KDF	SHA2-256	KAT	CAST	Successful boot	Extract, expand	On boot
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Successful completion outputs status of 0, otherwise it indicates failure by outputs status of -148	As specified in [90B] RCT startup health tests	At boot up
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Successful completion outputs status of 0, otherwise it indicates failure by outputs status of -148	As specified in [90B] APT startup health tests	At boot up
Entropy 90B Continuous Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	The RDSEED instruction provides error signaling via the CF flag. If CF = 1, the RDSEED return value is valid. If CF = 0, the value is invalid.	As specified in [90B] RCT continuous health tests	Continuous when entropy is requested
Entropy 90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	The RDSEED instruction provides error signaling via the CF flag. If CF = 1, the RDSEED return value is valid. If CF = 0, the value is invalid.	As specified in [90B] APT continuous health tests	Continuous when entropy is requested

Table 19: Conditional Self-Tests

10.3 Periodic Self-Test Information

N/A. The module has been tested to security level 1 and is not subject to periodic self-testing requirements.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error Mode	All data output and cryptographic services are inhibited in the error state.	If any of the self-tests or conditional tests fail, the module enters an error state.	Power Cycling	The module outputs a failing status of the algorithm that failed its' self-test. Example: Running RSA test...failed.

Table 20: Error States

10.5 Operator Initiation of Self-Tests

The approved mode of operation includes a set of startups and conditional self-tests. The tests include algorithm known answer tests (KATs), a software integrity test. Refer to Section 10.1 & 10.2 of FortiSwitch 7.6 Security Policy for a complete list of the self-tests. The administrator can run self-tests manually at any time. To run all the tests, enter the following CLI command:

```
execute fips kat all
```

To run an individual test, enter:

```
execute fips kat <test_name>
```

To see the list of valid test names, enter:

```
execute fips kat ?
```

The administrator can also invoked self–tests by power cycling the host FortiSwitch device.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The following steps must be performed in order to securely install, initialize, and start up Module in the Approved mode of operation:

There are no special startup procedures to set up the FortiSwitch Crypto Library as in comes pre-installed in the operational environment. However, the FortiSwitch hardware is shipped in a non-FIPS 140-3 compliant configuration. The following steps must be performed to put the Module into a FIPS compliant configuration:

1. Download the model specific FIPS validated firmware image from the Fortinet Support site at https://support.fortinet.com/
2. Verify the integrity of the firmware image
3. Install the FIPS validated firmware image
4. Enable the FIPS-CC mode of operation

Note: If you do not follow the above mentioned steps, the module will not be configured to operate in an Approved mode and is not in project scope/ validated configuration.

These steps are described in detail in the Administrator Guidance found on the Fortinet Technical Documentation website. In addition, FIPS 140-3 compliant operation requires both that you use the module in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the FortiSwitch unit. You must ensure that:

- The FortiSwitch unit is configured in the FIPS-CC mode of operation.
- The FortiSwitch unit is installed in a secure physical location.
- Physical access to the FortiSwitch unit is restricted to authorized operators.

To enable the FIPS 140-3 compliant mode of operation, the operator must execute the following command from the Local Console:

```
config system security
set mode fips-cc
end
```

Upon restart, the Module will execute self-tests to ensure the correct initialization of the module's cryptographic functions. After restarting, the Crypto Officer can confirm that the Module is running in FIPS-CC mode by executing the following command from the CLI:

```
get system status
```

If the Module is running in FIPS-CC mode, the system status output will display the line:

```
FIPS-CC mode: enable
```

Once the FIPS validated firmware has been installed and the Module properly configured in the Approved Mode of operation, the Module is running in an Approved compliant configuration within the operational environment. It is the responsibility of the CO to ensure the Module is in the Approved Mode of operation.

11.2 Administrator Guidance

FortiSwitch administrator guidance is publicly available from the Fortinet Technical Documentation site. The key administrator guidance documents are listed below:

- FortiSwitch (Standalone) Administrator Guide

- FortiSwitch CLI Reference
- FortiSwitch Quickstart Guide

11.3 Non-Administrator Guidance

None. Non-Administrator guidance is included in the FortiSwitch Administration Guide.

11.4 Design and Rules

Rules of operation:

- The Module provides single distinct operator role: Cryptographic Officer.
- The Module does not claim role-based/identity-based authentication.
- An operator does not have access to any cryptographic services prior to assuming an authorized role.
- The Module allows the operator to initiate power-up self-tests by power cycling power or invoking the Self-Test of the Module.
- Self-tests do not require any operator action. However, the operator has the ability to manually invoke individual self-tests.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
- There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
- The Module does not support concurrent operators.
- The Module does not support a maintenance interface or role.
- The Module does not support SSP establishment.
- The Module does not have any proprietary external input/output devices used for entry/output of data.
- The Module does not persistently store any plaintext CSPs.
- The Module does not output intermediate key values.
- The Module does not provide bypass services.
- When the Show Module Info service runs the module output this identifier, “FSW_424E_FIBER-v7-build8073-FIPS-CC-76-01”. This identifies the FortiSwitch Crypto Library is running on the device.

11.6 End of Life

At End of Life the CO must issue the `exec factoryreset` command before recycling the chassis.

12 Mitigation of Other Attacks

The Module does not implement any mitigation method against other attacks.

References and Definitions

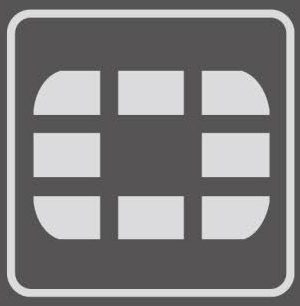
The following standards are referred to in this Security Policy.

Abbreviation	Full Specification Name
[FIPS140-3]	Security Requirements for Cryptographic Modules, March 22, 2019
[ISO19790]	International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017
[ISO24759]	International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015
[IG]	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, 23 October 2024
[131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019
[133r2]	NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020
[135]	National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.
[186]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.
[197]	National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001
[198]	National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008
[180]	National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015
[38A]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001
[38B]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005
[38D]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007
[56Arev3]	NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018
[90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.
[90B]	National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.

Table 21: References

Acronym	Definition
APT	Adaptative Proportion Test
CSP	Critical Security Parameter
KAT	Know Answer Test
PCT	Pair-Wise Consistency Test
PSP	Public Security Parameter
RCT	Repetition Count Test
SSP	Sensitive Security Parameter

Table 22: Acronyms and Definitions



FORTINET®