SonicWALL SMA Series v12.4
SMA 8200v

FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.10
Date: January 26, 2023

Contents

Tables

Figures

1 Introduction

This document defines the Security Policy for the SonicWall SMA Series v12.4 SMA 8200v running OS SMA1000 12.4, hereafter denoted as "the module". The module is software-hybrid due to reliance on CPU-implemented AES-NI (PAA). The primary purpose of the module is to provide secure remote access to internal resources via the Internet Protocol (IP). The module provides network interfaces for data input and output. The appliance encryption technology uses FIPS approved algorithms. FIPS approved algorithms are approved by the U.S. government for protecting Unclassified data.

The Module is designated as a modifiable operational environment under the FIPS 140-2 definitions. The Module includes a software load service to support necessary updates.
New software versions within the scope of this validation must be validated to FIPS 140-2 through the CMVP. Any other software loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

The module runs on many different UCS Servers with various hypervisors. For the purpose of this validation, the module was tested on the following operational environment:

	Module	OS	Tested Platforms	Hypervisor	Processor
1	SMA 8200v	SMA1000 12.4	Dell PowerEdge R640	VMWare ESXi 6.7	Intel Xeon Silver 4208

Table 1 – Cryptographic Module List

As per FIPS 140-2 Implementation Guidance G.5, compliance is maintained for other versions of the respective operational environments where the module binary is unchanged and the Intel AES-NI (PAA) exists within the operational environment's CPU.

The following Hypervisors/Cloud are vendor affirmed on the additional platforms listed above: ESXi 6.5, ESXi 7.0, HyperV 2019, KVM, AWS and Azure.

The above vendor affirmed modules and platforms were not tested for this FIPS 140-2 validation. As per FIPS 140-2 Implementation Guidance G.5, compliance is maintained for other versions of the respective operational environments where the module binary is unchanged.

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.

The module software version for all tested models is SMA 8200v v12.4.1-02451

The FIPS 140-2 security levels for the module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2 – Security Level of Security Requirements

1.1 Module Description and Cryptographic Boundary

The cryptographic module is defined as a multi-chip standalone software-hybrid module. As such, the module has no physical characteristics; however, the physical boundary of the cryptographic module is defined by the hard enclosure around the tested host platform on which it runs. The module's physical cryptographic boundary is illustrated by the green dashed line in Figure 1.

The module makes use of the physical interfaces of the tested platform hosting the virtual environment upon which the module is installed. The hypervisor controls and directs all interactions between the module and the operator and is responsible for mapping the module's virtual interfaces to the tested platform's physical interfaces.

The module is software-hybrid because it relies on CPU-implemented AES-NI (PAA)

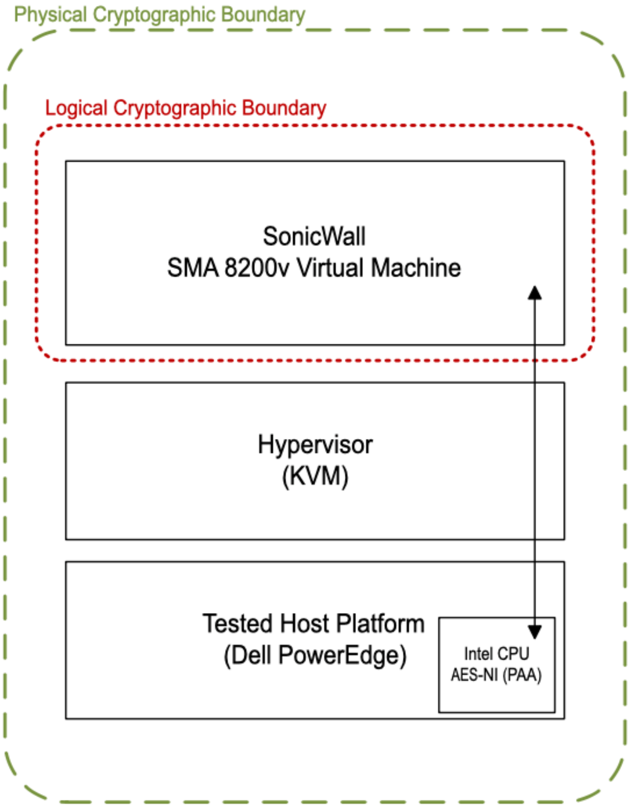

Physical Cryptographic Boundary
Logical Cryptographic Boundary
SonicWall
SMA 8200v Virtual Machine
Hypervisor
(KVM)
Tested Host Platform
(Dell PowerEdge)
Intel CPU
AES-NI (PAA)

Figure 1 – Block Diagram

Figure 1 also shows the logical cryptographic boundary of the module executing in memory and its interactions with the hypervisor. The logical cryptographic boundary of the module (shown by the red dashed line in Figure 1) is the SMA 8200v Guest OS which interacts directly with the hypervisor that runs directly on the tested host platform.

Figure 2 – CPU, Intel Xeon Silver 4208

1.2 Ports and Interfaces

The module's ports and associated FIPS 140-2 defined logical interface categories are listed in the following table:

Physical Port/Interface	8200v Virtual Ports	FIPS 140-2 Interface
Host Platform Ethernet (10/100/1000) ports	Virtual Ethernet Ports	Data Input Interface
Host Platform Ethernet (10/100/1000) ports	Virtual Ethernet Ports	Data Output Interface
Host Platform Ethernet (10/100/1000) ports; Host Platform Serial Port	Virtual Ethernet Ports, Virtual Serial Port	Control Input Interface
Host Platform Ethernet (10/100/1000) ports; Host Platform Serial Port	Virtual Ethernet Ports, Virtual Serial Port	Status Output Interface

Table 3 – Ports and Interfaces

1.3 Modes of Operation

The module's Management Console provides the mechanism to configure the module for the Approved mode of operation, found in *General Settings* > *Configure FIPS Security*. Attempts to check the *Enable FIPS mode* checkbox execute a FIPS Approved mode compliance checking tool, which provides clearly visible warnings if any of the following configuration conditions are not met:

- The following authentication servers may be used, if connected using only FIPS approved ciphers:
    - LDAP
    - Active Directory single domain
    - RSA Authentication Manager
- Use of RADIUS authentication servers is not permitted in the Approved mode.
- Clustering (High Availability) is not supported in FIPS mode.
- Configured connections with SonicWALL GMS or Viewpoint servers are not permitted in the Approved mode.
- Ciphers not specified in Table 4 are not permitted in the Approved mode.

Unchecking the *Enable FIPS* mode checkbox will revert the module configuration back to non-Approved mode, removing all configured CSPs. Approved mode may then be configured once again via the process noted above. In the non-Approved mode, the features cited in the bullets above are available for use. See Section 8, *Security Rules and Guidance* for additional Approved mode operation guidance.

2 Cryptographic Functionality

The cryptographic protocols and primitves implemented and used by the modules are listed in this section. Table 4 and Table 5 list the TLS ciphersuites available in the Approved and non-Approved modes, respectively. Table 6 lists the SSH security methods; unlike TLS ciphersuites, SSH methods are independently selectable and may be used in any combination.

Cipher Suite String (IETF enumeration)	TLS	Key Exchange	Cipher	Auth
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256[1]	1.2	ECDH_P256	AES-128	GCM
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	1.2	ECDH_P384	AES-256	GCM
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	1.2	ECDH_P256	AES-128	GCM
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	1.2	ECDH_P384	AES-256	GCM
TLS_AES_256_GCM_SHA384	1.3	ECDH_P384	AES-256	GCM
TLS_AES_128_GCM_SHA256	1.3	ECDH_P256	AES-128	GCM

Table 4 – Management Console and VPN session TLS Ciphersuites used in the Approved mode

[1] These GCM ciphersuites are from SP 800-52 Rev 1, Section 3.3.1. The module's nonce_explicit management logic shuts down the TLS connection if it detects that the nonce_explicit part of the IV has exhausted its counter.

Cipher Suite String (IETF enumeration)	TLS	Key Exchange	Cipher	Auth
TLS_RSA_WITH_AES_128_CBC_SHA	1.2, 1.1, 1.0	RSA	AES-128	SHA-1
TLS_RSA_WITH_AES_128_CBC_SHA256	1.2	RSA	AES-128	SHA-256
TLS_RSA_WITH_AES_256_CBC_SHA	1.2, 1.1, 1.0	RSA	AES-256	SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA256	1.2	RSA	AES-256	SHA-256

Table 5 – TLS Ciphersuites used in the non-Approved mode

Key Exchange	Mode
ecdh-sha2-nistp256	Approved and Non-Approved
ecdh-sha2-nistp384	Approved and Non-Approved
Server Host Key (Authentication)	
ecdsa-sha2-nistp384	Approved and Non-Approved
ssh-rsa	Approved and Non-Approved
Digest	
hmac-sha2-256	Approved and Non-Approved
hmac-sha1	Approved and Non-Approved
Encryption	
aes256-cbc	Approved and Non-Approved
aes128-cbc	Approved and Non-Approved
aes256-gcm[2]	Approved and Non-Approved

Table 6 – SSH Security Methods Available (Approved and non-Approved modes)

The module uses IPsec ESP mode only over UDP for data transport, using AES-128 and AES-256 in CBC mode. IKE is not used[3]; rather, the keys and IVs are generated by the module and provided to the peer over an out-of-band TLS tunnel[4].

Cipher Suite String (IETF enumeration)	Cipher	Auth	Mode
AES128-GCM-SHA256[5]	AES-128	GCM	Approved and Non-Approved
AES256-GCM-SHA384[5]	AES-256	GCM	Approved and Non-Approved
AES128-CBC-SHA	AES-128	SHA-1	Non-Approved
AES128-CBC-SHA256	AES-128	SHA256	Non-Approved
AES256-CBC-SHA	AES-256	SHA-1	Non-Approved
AES256-CBC-SHA256	AES-256	SHA256	Non-Approved

Table 7 – IPsec ESP Cipher and Digest Methods Available

[2] This GCM security method is used in compliance with RFCs 4252, 4253, and 5647, deriving the AES GCM Key and IV using the SP 800-135r1 compliant SSH KDF; these are only used within SSHv2. The module's nonce management logic shuts down the SSH connection if it detects that the nonce part of the IV has exhausted its counter.

[3] Since IKE is not used the IKE/IPSec KDF is not used

[4] The ESP protocol has not been reviewed or tested by the CAVP and CMVP

[5] These GCM ciphersuites are used in compliance with RFC 4106. The module generates the AES GCM keys and IVs internally from the module's Approved DRBG. The module's nonce management logic shuts down the IPsec connection if it detects that the nonce part of the IV has exhausted its counter.

CAVP	Algorithm	Mode/Method	Strength[6]	Usage
A1338	AES [197],[38A], [38D]	CBC, ECB, GCM	128, 256	Data Encryption/ Decryption [A].
A1358	AES [197],[38A], [38D]	CBC, ECB, GCM	128, 256	Data Encryption/ Decryption [O].
A1352	AES [197],[38A], [38D]	CBC, ECB, GCM	128, 256	Data Encryption/ Decryption [L].
Vendor Affirm	CKG [133][7]			Cryptographic Key Generation [A].
Vendor Affirm	CKG [133][8]			Cryptographic Key Generation [O].
Vendor Affirm	CKG [133][9]			Cryptographic Key Generation [L].
A1353	CVL-SNMP[10] KDF [135]	SHA-1		SNMP AES key KDF.
A1352	CVL-TLS KDF [135]	TLS 1.2 (SHA-256)		TLS session keys KDF [L]
A1352	CVL-TLS KDF [8446]	TLS 1.3 (SHA-256, SHA-384)		TLS session keys KDF [L]
A1354	CVL-SSH KDF [135]	SHA-256		SSH v2 session key KDF
A1358	CVL-TLS KDF [135]	TLS 1.2 (SHA-256)		TLS session keys KDF. [O]
A1358	CVL-TLS KDF [8446]	TLS 1.3 (SHA-256, SHA-384)		TLS session keys KDF [O]
A1338	DRBG[11] [90A]	CTR_DRBG	AES-256	Random Bit Generation [A].
A1358	ECDSA [186]	P-256 (SHA-256) P-384 (SHA-384)		ECC Key Generation; Digital Signature Generation, Verification [O].
A1352	ECDSA [186]	P-256 (SHA-256) P-384 (SHA-384)		ECC Key Generation; Digital Signature Generation, Verification [L].
A1358	KAS-SSC [56A]	ECDHE Key Agreement	P-256 P-384	For use with TLS/SSH KDFs [O].
A1352	KAS-SSC [56A]	ECDHE Key Agreement	P-256 P-384	For use with TLS/SSH KDFs [L].
A1338	HMAC [198]	HMAC-SHA-1 HMAC-SHA-256	128 256	Message Authentication [A].
A1358	HMAC [198]	HMAC-SHA-1 HMAC-SHA-256	128 256	Message Authentication. [O]
A1352	HMAC [198]	HMAC-SHA-1[12] HMAC-SHA-1-96[12] HMAC-SHA-256	128 128 256	Message Authentication. [L]

A1358	RSA [186]	n=2048 (SHA-256, SHA-384)
		n=3072 (SHA-256, SHA-384)
				RSA Key generation; Digital Signature Generation and Verification [O].

A1352	RSA [186]	n=2048 (SHA-256, SHA-384)
		n=3072 (SHA-256, SHA-384)
				RSA Key generation; Digital Signature Generation and Verification. [L]

A1338	SHS [180]	SHA-1, SHA-256, SHA-384, SHA-3-256		Message Digest generation. [A]
A1358	SHS [180]	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest generation. [O]
A1352	SHS [180]	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest generation. [L]
A1358	KTS [38F]	CBC, GCM, HMAC-SHA-1, HMAC-SHA-256	128, 256	Key Transport via TLS [O] Provides 128 or 256 bits of encryption strength.
A1338	KTS [38F]	CBC, GCM, HMAC-SHA-1, HMAC-SHA-256	128, 256	Key Transport via TLS [A] Provides 128 or 256 bits of encryption strength.
	ENT (NP) [90B]			Entropy Generation for DRBG (re)seeding [A] Seeded with at least 256 bits of entropy.
A1358	KAS [56A]	KAS-SSC + TLS 1.2/1.3 KDF	P-256, P-384	TLS
A1352, A1353, A1354	KAS [56A]	KAS-SSC + TLS 1.2/1.3 KDF, SSH KDF, SNMP KDF	P-256, P-384	TLS, SSH, or SNMP

Table 8 – Approved algorithms (Implementations: [A]=avcrypto; [L]=libcrypto; [O]=ojdk)

[6] Strength indicates DRBG Strength, Key Lengths, Curves or Moduli

[7] The symmetric key or a generated seed is an unmodified output from a DRBG

[8] The symmetric key or a generated seed is an unmodified output from a DRBG

References to standards are given in square bracket [ ]; see the References table.
The module uses only the RSA functions shown above in the Approved mode under FIPS 186-4.

Algorithm	Use
Triple-DES (No Security Claimed)	Used for PBE within PKCS12 files

Table 9 - Non-Approved Algorithms

[9] The symmetric key or a generated seed is an unmodified output from a DRBG

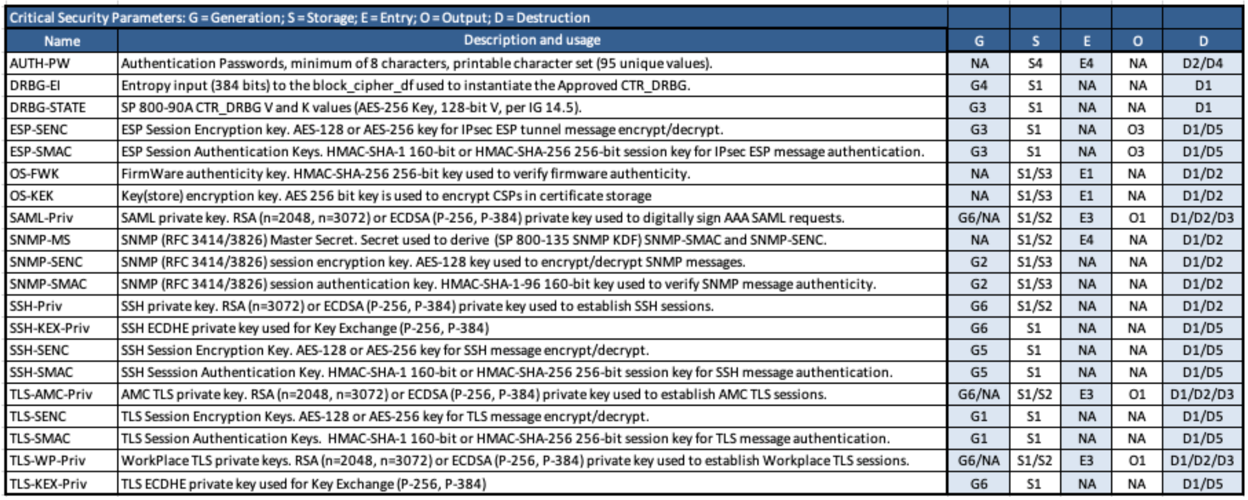
[10] No parts of the TLS, SSH, and SNMP protocols, other than the KDF, have been tested by the CAVP. No parts of those protocols have been reviewed or tested by the CMVP.

[11] No prediction resistance; block_cipher_df derivation function used for instantiation.

[12] HMAC-SHA-96 is also supported, by truncating existing HMAC-SHA-1 output to 96 bits

2.1 Critical Security Parameters

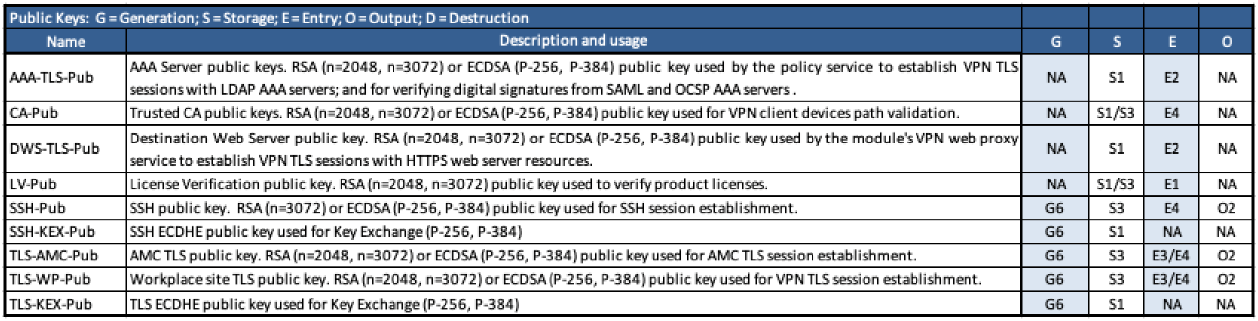
All CSPs used by the module are described in this section.



Critical Security Parameters: G = Generation; S = Storage; E = Entry; O = Output; D = Destruction						
Name	Description and usage	G	S	E	O	D
AUTH-PW	Authentication Passwords, minimum of 8 characters, printable character set (95 unique values).	NA	S4	E4	NA	D2/D4
DRBG-EI	Entropy input (384 bits) to the block_cipher_df used to instantiate the Approved CTR_DRBG.	G4	S1	NA	NA	D1
DRBG-STATE	SP 800-90A CTR_DRBG V and K values (AES-256 Key, 128-bit V, per IG 14.5).	G3	S1	NA	NA	D1
ESP-SENC	ESP Session Encryption key. AES-128 or AES-256 key for IPsec ESP tunnel message encrypt/decrypt.	G3	S1	NA	O3	D1/D5
ESP-SMAC	ESP Session Authentication Keys. HMAC-SHA-1 160-bit or HMAC-SHA-256 256-bit session key for IPsec ESP message authentication.	G3	S1	NA	O3	D1/D5
OS-FWK	FirmWare authenticity key. HMAC-SHA-256 256-bit key used to verify firmware authenticity.	NA	S1/S3	E1	NA	D1/D2
OS-KEK	Key(store) encryption key. AES 256 bit key is used to encrypt CSPs in certificate storage	NA	S1/S3	E1	NA	D1/D2
SAML-Priv	SAML private key. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) private key used to digitally sign AAA SAML requests.	G6/NA	S1/S2	E3	O1	D1/D2/D3
SNMP-MS	SNMP (RFC 3414/3826) Master Secret. Secret used to derive (SP 800-135 SNMP KDF) SNMP-SMAC and SNMP-SENC.	NA	S1/S2	E4	NA	D1/D2
SNMP-SENC	SNMP (RFC 3414/3826) session encryption key. AES-128 key used to encrypt/decrypt SNMP messages.	G2	S1/S3	NA	NA	D1/D2
SNMP-SMAC	SNMP (RFC 3414/3826) session authentication key. HMAC-SHA-1-96 160-bit key used to verify SNMP message authenticity.	G2	S1/S3	NA	NA	D1/D2
SSH-Priv	SSH private key. RSA (n=3072) or ECDSA (P-256, P-384) private key used to establish SSH sessions.	G6	S1/S2	NA	NA	D1/D2
SSH-KEX-Priv	SSH ECDHE private key used for Key Exchange (P-256, P-384)	G6	S1	NA	NA	D1/D5
SSH-SENC	SSH Session Encryption Key. AES-128 or AES-256 key for SSH message encrypt/decrypt.	G5	S1	NA	NA	D1/D5
SSH-SMAC	SSH Sesssion Authentication Key. HMAC-SHA-1 160-bit or HMAC-SHA-256 256-bit session key for SSH message authentication.	G5	S1	NA	NA	D1/D5
TLS-AMC-Priv	AMC TLS private key. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) private key used to establish AMC TLS sessions.	G6/NA	S1/S2	E3	O1	D1/D2/D3
TLS-SENC	TLS Session Encryption Keys. AES-128 or AES-256 key for TLS message encrypt/decrypt.	G1	S1	NA	NA	D1/D5
TLS-SMAC	TLS Session Authentication Keys. HMAC-SHA-1 160-bit or HMAC-SHA-256 256-bit session key for TLS message authentication.	G1	S1	NA	NA	D1/D5
TLS-WP-Priv	WorkPlace TLS private keys. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) private key used to establish Workplace TLS sessions.	G6/NA	S1/S2	E3	O1	D1/D2/D3
TLS-KEX-Priv	TLS ECDHE private key used for Key Exchange (P-256, P-384)	G6	S1	NA	NA	D1/D5

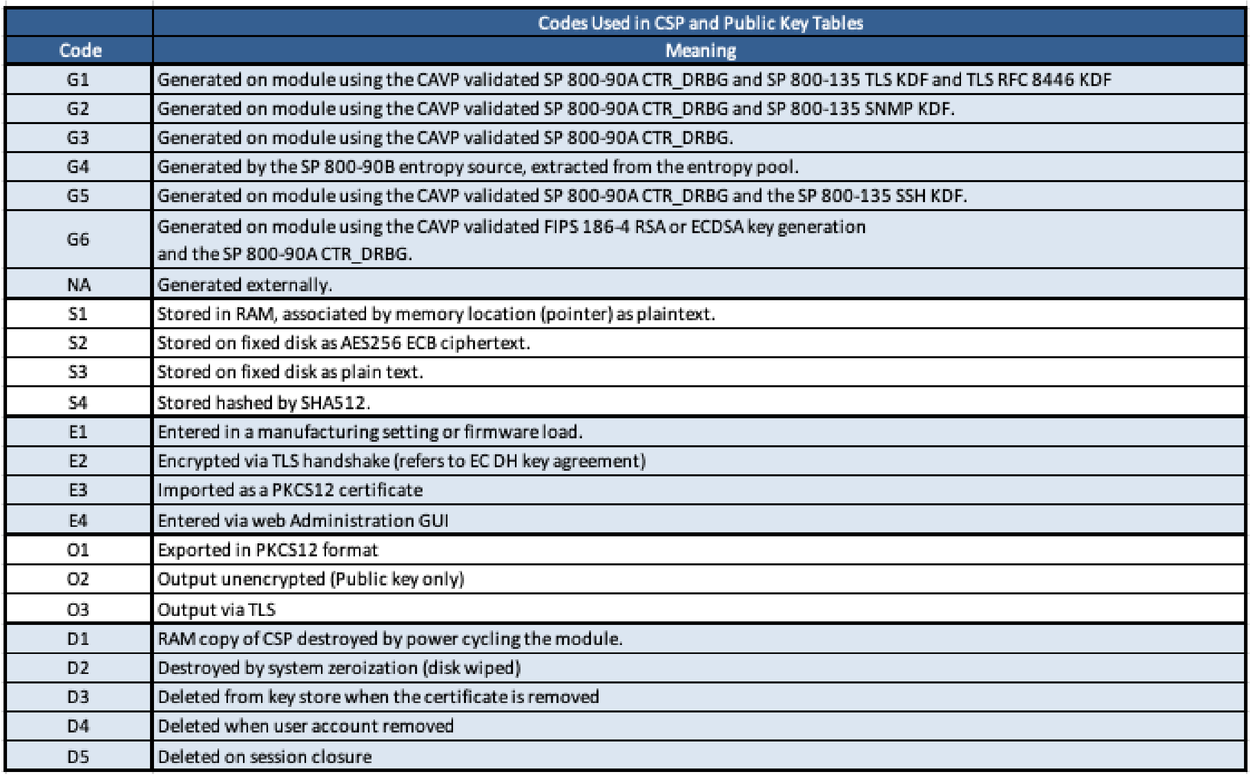
Table 10 – Critical Security Parameters (CSPs)

2.2 Public Keys



Public Keys: G = Generation; S = Storage; E = Entry; O = Output; D = Destruction					
Name	Description and usage	G	S	E	O
AAA-TLS-Pub	AAA Server public keys. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) public key used by the policy service to establish VPN TLS sessions with LDAP AAA servers; and for verifying digital signatures from SAML and OCSP AAA servers .	NA	S1	E2	NA
CA-Pub	Trusted CA public keys. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) public key used for VPN client devices path validation.	NA	S1/S3	E4	NA
DWS-TLS-Pub	Destination Web Server public key. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) public key used by the module's VPN web proxy service to establish VPN TLS sessions with HTTPS web server resources.	NA	S1	E2	NA
LV-Pub	License Verification public key. RSA (n=2048, n=3072) public key used to verify product licenses.	NA	S1/S3	E1	NA
SSH-Pub	SSH public key. RSA (n=3072) or ECDSA (P-256, P-384) public key used for SSH session establishment.	G6	S3	E4	O2
SSH-KEX-Pub	SSH ECDHE public key used for Key Exchange (P-256, P-384)	G6	S1	NA	NA
TLS-AMC-Pub	AMC TLS public key. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) public key used for AMC TLS session establishment.	G6	S3	E3/E4	O2
TLS-WP-Pub	Workplace site TLS public key. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) public key used for VPN TLS session establishment.	G6	S3	E3/E4	O2
TLS-KEX-Pub	TLS ECDHE public key used for Key Exchange (P-256, P-384)	G6	S1	NA	NA

Table 11 – Public Keys



	Codes Used in CSP and Public Key Tables
Code	Meaning
G1	Generated on module using the CAVP validated SP 800-90A CTR_DRBG and SP 800-135 TLS KDF and TLS RFC 8446 KDF
G2	Generated on module using the CAVP validated SP 800-90A CTR_DRBG and SP 800-135 SNMP KDF.
G3	Generated on module using the CAVP validated SP 800-90A CTR_DRBG.
G4	Generated by the SP 800-90B entropy source, extracted from the entropy pool.
G5	Generated on module using the CAVP validated SP 800-90A CTR_DRBG and the SP 800-135 SSH KDF.
G6	Generated on module using the CAVP validated FIPS 186-4 RSA or ECDSA key generation and the SP 800-90A CTR_DRBG.
NA	Generated externally.
S1	Stored in RAM, associated by memory location (pointer) as plaintext.
S2	Stored on fixed disk as AES256 ECB ciphertext.
S3	Stored on fixed disk as plain text.
S4	Stored hashed by SHA512.
E1	Entered in a manufacturing setting or firmware load.
E2	Encrypted via TLS handshake (refers to EC DH key agreement)
E3	Imported as a PKCS12 certificate
E4	Entered via web Administration GUI
O1	Exported in PKCS12 format
O2	Output unencrypted (Public key only)
O3	Output via TLS
D1	RAM copy of CSP destroyed by power cycling the module.
D2	Destroyed by system zeroization (disk wiped)
D3	Deleted from key store when the certificate is removed
D4	Deleted when user account removed
D5	Deleted on session closure

Table 12 - Codes for CSP and Public Key Tables

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports the operator roles and associated authentication methods listed in Table 13.
The Module does not support a maintenance role or bypass capability. The Module supports concurrent users, enforcing separation of roles by the partitioning of major subsystems (such as VPN traffic vs. shell or AMC administrative functions), and by partitioning of the administrative interfaces (e.g.,. by organization of the AMC web GUI pages). Authentication status does not persist across module power cycles. Table 13 lists the available roles.

Role		Authentication	
ID	**Description**	**Type**	**Data**
CO	Cryptographic Officer – Has full access to administer and configure the module as well as delegate admin access control rights to Admin users.	Identity-based (using *Local password verification*) or role-based (using *Transitive trust with authentication*) dependent on configured policy.	Username and PIN or X.509 certificate
User	Admin User – Configure and administer the module per the delegated access rights assigned by the CO.		
VPN	Typical end user accessing the virtual private network resources via an encrypted connection.		
SNMP	SNMP agent and trap – provides module status via SNMP messages	Identity-based (using *SNMP authentication*)	SNMP-SMAC

Table 13 – Roles Description

3.2 Authentication Methods

The *Local password verification* method requires an 8 character minimum password using characters in the printable character set. The maximum rate for local password authentication is conservatively estimated to be approximately one (1) attempt per microsecond.

Hence the probability of false authentication is less than the required 1/1,000,000: 1/(95^8) = **1.5E-16**

And the probability of false authentication in a one minute period is less than the required 1/100,000: (60*10^6)/(95^8) = **9.0E-9**

The *Transitive trust with authentication* method first establishes a secure connection to an external authentication server, which authenticates to the module using X.509 certificates. Subsequent interaction with the authentication server determines the applicable access rights; as such, this method is a role-based authentication method. The maximum rate for local password authentication is conservatively estimated to be approximately one (1) attempt per microsecond.

Based on the minimum strength SAML key (RSA 2048) security strength of 112 bits, the probability of false authentication is less than the required 1/1,000,000: 1/(2^112) = **1.9E-34**

And the probability of false authentication in a one minute period is less than the required 1/100,000: (60*10^6)/(2^112) = **1.2E-26**

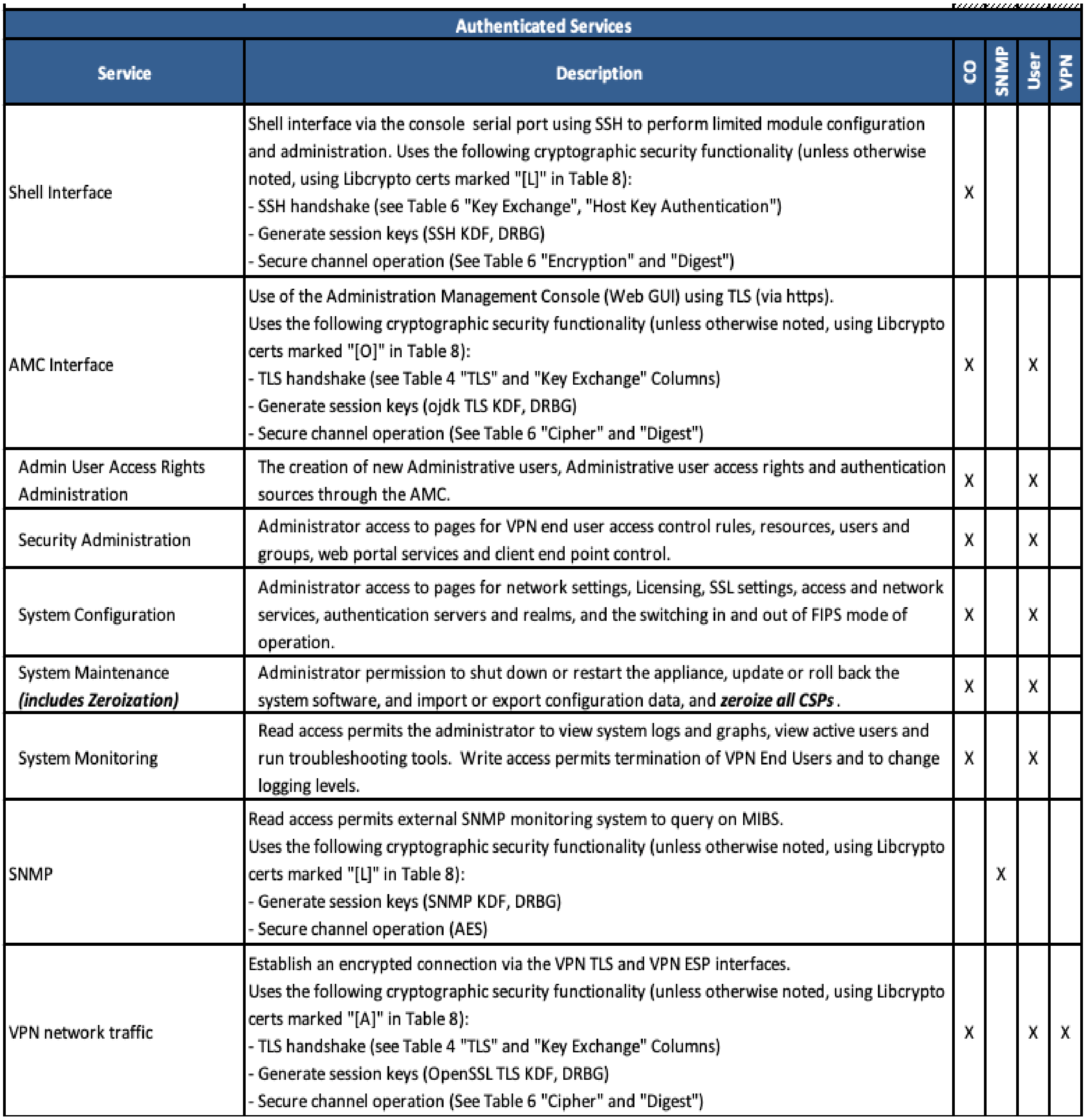
SNMP authentication method: communications established with an SNMP client include verification of a initial message, confirming a 96-bit truncated HMAC-SHA-1 value calculated using the SNMP-SMAC key and a designated message , with maximum processing rate measured on the fastest configuration as requiring at minimum one microsecond:

Hence the probability of false authentication is less than the required 1/1,000,000: 1/(2^96) = **1.3E-29**

And the probability of false authentication in a one minute period is less than the required 1/100,000: (60*10^6)/(2^96) = **7.6E-22**

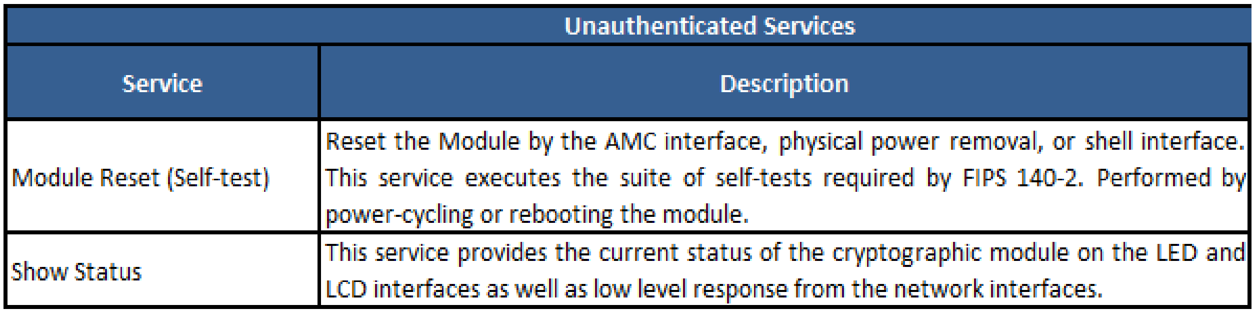
3.3 Services

All services implemented by the module are listed in the tables below.



Authenticated Services					
Service	**Description**	**CO**	**SNMP**	**User**	**VPN**
Shell Interface	Shell interface via the console serial port using SSH to perform limited module configuration and administration. Uses the following cryptographic security functionality (unless otherwise noted, using Libcrypto certs marked "[L]" in Table 8): - SSH handshake (see Table 6 "Key Exchange", "Host Key Authentication") - Generate session keys (SSH KDF, DRBG) - Secure channel operation (See Table 6 "Encryption" and "Digest")	X			
AMC Interface	Use of the Administration Management Console (Web GUI) using TLS (via https). Uses the following cryptographic security functionality (unless otherwise noted, using Libcrypto certs marked "[O]" in Table 8): - TLS handshake (see Table 4 "TLS" and "Key Exchange" Columns) - Generate session keys (ojdk TLS KDF, DRBG) - Secure channel operation (See Table 6 "Cipher" and "Digest")	X		X	
Admin User Access Rights Administration	The creation of new Administrative users, Administrative user access rights and authentication sources through the AMC.	X		X	
Security Administration	Administrator access to pages for VPN end user access control rules, resources, users and groups, web portal services and client end point control.	X		X	
System Configuration	Administrator access to pages for network settings, Licensing, SSL settings, access and network services, authentication servers and realms, and the switching in and out of FIPS mode of operation.	X		X	
System Maintenance ***(includes Zeroization)***	Administrator permission to shut down or restart the appliance, update or roll back the system software, and import or export configuration data, and ***zeroize all CSPs*** .	X		X	
System Monitoring	Read access permits the administrator to view system logs and graphs, view active users and run troubleshooting tools. Write access permits termination of VPN End Users and to change logging levels.	X		X	
SNMP	Read access permits external SNMP monitoring system to query on MIBS. Uses the following cryptographic security functionality (unless otherwise noted, using Libcrypto certs marked "[L]" in Table 8): - Generate session keys (SNMP KDF, DRBG) - Secure channel operation (AES)		X		
VPN network traffic	Establish an encrypted connection via the VPN TLS and VPN ESP interfaces. Uses the following cryptographic security functionality (unless otherwise noted, using Libcrypto certs marked "[A]" in Table 8): - TLS handshake (see Table 4 "TLS" and "Key Exchange" Columns) - Generate session keys (OpenSSL TLS KDF, DRBG) - Secure channel operation (See Table 6 "Cipher" and "Digest")	X		X	X

Table 14 – Authenticated Services

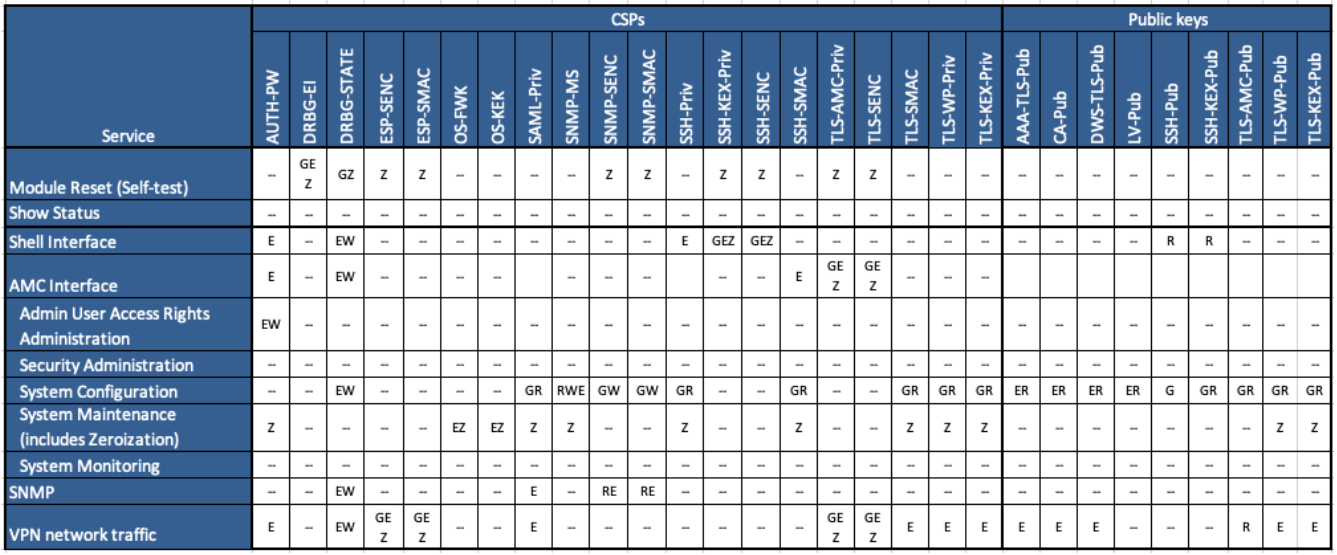


Unauthenticated Services	
Service	**Description**
Module Reset (Self-test)	Reset the Module by the AMC interface, physical power removal, or shell interface. This service executes the suite of self-tests required by FIPS 140-2. Performed by power-cycling or rebooting the module.
Show Status	This service provides the current status of the cryptographic module on the LED and LCD interfaces as well as low level response from the network interfaces.

Table 15 – Unauthenticated Services

Table 16 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.



Service	CSPs																				Public keys								
	AUTH-PW	DRBG-EI	DRBG-STATE	ESP-SENC	ESP-SMAC	OS-FWK	OS-KEK	SAML-Priv	SNMP-MS	SNMP-SENC	SNMP-SMAC	SSH-Priv	SSH-KEX-Priv	SSH-SENC	SSH-SMAC	TLS-AMC-Priv	TLS-SENC	TLS-SMAC	TLS-WP-Priv	TLS-KEX-Priv	AAA-TLS-Pub	CA-Pub	DWS-TLS-Pub	LV-Pub	SSH-Pub	SSH-KEX-Pub	TLS-AMC-Pub	TLS-WP-Pub	TLS-KEX-Pub
Module Reset (Self-test)	--	GE Z	GZ	Z	Z	--	--	--	--	Z	Z	--	Z	Z	--	Z	Z	--	--	--	--	--	--	--	--	--	--	--	--
Show Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Shell Interface	E	--	EW	--	--	--	--	--	--	--	--	E	GEZ	GEZ	--	--	--	--	--	--	--	--	--	--	R	R	--	--	--
AMC Interface	E	--	EW	--	--	--	--		--	--	--		--	--	E	GE Z	GE Z	--	--	--									
Admin User Access Rights Administration	EW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Security Administration	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
System Configuration	--	--	EW	--	--	--	--	GR	RWE	GW	GW	GR	--	--	GR	--	--	GR	GR	GR	ER	ER	ER	ER	G	GR	GR	GR	GR
System Maintenance (includes Zeroization)	Z	--	--	--	--	EZ	EZ	Z	Z	--	--	Z	--	--	Z	--	--	Z	Z	Z	--	--	--	--	--	--	--	Z	Z
System Monitoring	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SNMP	--	--	EW	--	--	--	--	E	--	RE	RE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
VPN network traffic	E	--	EW	GE Z	GE Z	--	--	E	--	--	--	--	--	--	--	GE Z	GE Z	E	E	E	E	E	E	--	--	--	R	E	E

Table 16 – CSP Access Rights within Services

4 Self-tests

Each time the module is powered up virtually within the hypervisor it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by virtual power cycling the module within the hypervisor.

On power up or reset, the module performs the self -tests described in below. All KATs must be completed successfully prior to any other use of cryptography by the module. If any power-up self-test fails, the module remains in the *FIPS Error* state until it is reset. Self-test status is shown on the console and captured into system logs.

Test Target	Description
Software Integrity	HMAC-SHA-256 performed over all code in EEPROM.
AES [A]	Separate KATs for each permutation of: encrypt, decrypt functions; 128, 256 bit keys; CBC, ECB, and GCM modes.
AES [L]	Separate KATs for each permutation of: encrypt, decrypt functions; 128, 256 bit keys; CBC, ECB and GCM modes.
AES [O]	Separate KATs for each permutation of: encrypt, decrypt functions; 128, 256 bit keys; CBC, ECB and GCM modes.
DRBG [A]	AES-256 CTR DRBG test. Performed conditionally (where initial use at power-up is the condition) per SP 800-90 Section 11.3.
ECDSA [L]	Separate signature generation and signature verification KAT's as well as a PCT are performed using a P-256 key.
ECDSA [O]	Separate signature generation and signature verification KAT's as well as a PCT are performed using a P-256 key.
HMAC [A]	Separate HMAC generation and HMAC verification KATs, using SHA-1 and SHA-256[13]
HMAC [L]	Separate HMAC generation and HMAC verification KATs, using SHA-1 and SHA-256[13]
HMAC [O]	Separate HMAC generation and HMAC verification KATs, using SHA-1 and SHA-256[13]
RSA [L]	Separate KATs of n=2048 bit signature generation and signature verification.
RSA [O]	Separate KATs of n=2048 bit signature generation and signature verification.
SHS [A]	Separate KATs of SHA-1, SHA-256, SHA-384[13], SHA-3-256
SHS [L]	Separate KATs of SHA-1, SHA-256, SHA-384[13], SHA-512
SHS [O]	Separate KATs of SHA-1, SHA-256, SHA-384[13], SHA-512
ECDH [L]	Separate KATs of P-256, P-384
ECDH [O]	Separate KATs of P-256, P-384
TLSKDF [O] [SSL]	TLSv1.2 SHA-256, TLSv1.2 SHA-384, TLSv1.3 SHA-256, TLSv1.3 SHA-384
TLSKDF [L] [SSL]	TLSv1.2 SHA-256, TLSv1.2 SHA-384, TLSv1.3 SHA-256, TLSv1.3 SHA-384
SSHKDF [SSH]	SHA-1, SHA-256
SNMPKDF [SNMP]	SHA1
CSP Integrity	(Critical function) A CSP integrity test is performed at power-on and at each system configuration invocation and configuration update.
ENT (NP)	Stuck, APT and RCT tests, run over 1024 samples, are performed at power-on.

Table 17 – Power Up Self-tests

[13] IG 9.4 requires separate self-tests of each of the SHA-1, SHA-256 and SHA-384 methods. IG 9.4 requires an HMAC KAT for at least one of the implemented underlying SHS methods.

Test Target	Description
CSP Integrity	(Critical function) A CSP integrity test is performed at power-on and at each system configuration invocation and configuration update.
DRBG	AS09.42 Continuous RNG Test performed when a random value is requested from the DRBG.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation.
Software Load	HMAC-SHA-256 verification performed when software is loaded. HMAC-SHA-1 is possible to use only for fallback scenarios.
NDRNG	AS09.42 Continuous RNG Test, SP 800-90B Adaptive Proportion Test and Repetition Count Test performed when a random value is requested from the ENT (NP).
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation.

Table 18 – Conditional Self-tests

5 Physical Security Policy

Physical security requirements for this module apply only to the Intel CPU provided in the host platform, which meets the requirement of being a production-grade component that includes standard passivation techniques.

6 Operational Environment

The Module is designated as a modifiable operational environment under the FIPS 140-2 definitions; see the statement in §1 *Introduction* ¶2.

7 Mitigation of Other Attacks Policy

The modules have not been designed to mitigate attacks outside the scope of FIPS 140-2.

8 Security Rules and Guidance

The Module design corresponds to the module security rules. The module implements and enforces the following security rules:

1. An unauthenticated operator does not have access to any CSPs or cryptographic services.
2. The module inhibits data output during power up self-tests and error states.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
4. Certificates are entered and output from the module in PKCS #12 format which stores but does not protect them. All import and export of key values shall be performed over VPN tunnels.
5. Zeroization overwrites all CSPs. Performance of the zeroization process will prevent the module from successfully booting, effectively disabling the module. The operator is required to be physically present while the module completes this process. The process may take up to one (1) hour to complete.
6. The module does not share CSPs between the Approved mode of operation and the non-Approved mode of operation.

The following security rules must be adhered to for operation in the FIPS 140-2 Approved mode:

1. Before enabling the FIPS Approved mode, a strong password, secure connection to the authentication server, and valid license are required.
2. The module must be configured for FIPS Security as detailed in §1.3, with no warnings present.
3. Passwords must be at least 8 characters; Good practice is to use 14 characters or more with a mix of numbers, letters and symbols.
4. Do not use RSA Authentication Manager servers without strong passwords as shared secrets.
5. Do not load or unload any kernel modules via the shell command line.
6. Do not install third party software via the shell command line.
7. Do not attempt Software upgrades via the shell command line.
8. Do not use Debug 1, Debug 2, Debug 3 or plaintext logs. Plaintext logs do not contain CSPs, but may contain information sensitive to users.
9. Do not use certificates with private/public key-pairs generated by non-FIPS validated systems.
10. Do not use 4096-bit RSA keys.
11. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is established.
12. Do not take or restore snapshots of the module when in a running state.

References and Definitions

Ref	Full Specification Name
[133]	SP 800-133 Revision 2, NIST, Recommendation for Cryptographic Key Generation, June 2020
[135]	SP 800-135, NIST, Recommendation for Existing Application-Specific Key Derivation Functions, December 2011.
[180]	FIPS 180-4, NIST, Secure Hash Standard (SHS), August 2015.
[186]	FIPS 186-4, NIST, Digital Signature Standard (DSS), July 2013.
[197]	FIPS 197, NIST, Advanced Encryption Standard (AES), November 26, 2001.
[198]	FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008.
[2865]	Rigney, C., Rubens, A., Simpson, W. and S. Willens, “Remote Authentication Dial In User Service RFC 2865, (RADIUS), RFC 2865, Internet Engineering Task Force, June 2000.
[38A]	SP 800-38A, NIST, Recommendation for Block Cipher Modes of Operation - Methods and Techniques, December 2001.
[38D]	SP 800-38D, NIST, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.
[38F]	SP 800-38F, NIST, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012
[4254]	RFC 4254, Ylonen, T. and C. Lonvick, “The Secure Shell (SSH) Connection Protocol”, Internet Engineering Task Force, January 2006.
[4303]	RFC 4303, Kent, S., “IP Encapsulating Security Payload (ESP)”, RFC 4303, Internet Engineering Task Force, December 2005.
[4511]	RFC 4511, Semersheim, J., Ed., “Lightweight Directory Access Protocol (LDAP): The Protocol”, RFC 4511, Internet Engineering Task Force, June 2006.
[5246]	RFC 5246, Dierks, T., and E. Rescoria, “The Transport Layer Security (TLS) Protocol Version 1.2”,. RFC 5246, Internet Engineering Task Force, August 2008.
[6239]	RFCTBD, K. Igoe, “Suite B Cryptography in Suites for Secure Shell (SSH)”, Internet Engineering Task Force, May 2011.
[6379]	RFC 6379, Law, L. and J. Solinas, “Suite B Cryptography Suites for IPsec”, RFC 6379, Internet Engineering Task Force, October 2011.
[6460]	RFCTBD, Salter, M and R. Housely, “Suite B Profile for Transport Layer Security (TLS)”, Internet Engineering Task Force, January 2012.
[67]	SP 800-67, NIST, Recommendation for the Triple Data Encryption Algorithm (Triple-DES) Block Cipher, January 2012.
[90A]	SP 800-90A, NIST, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015.
[90B]	SP 800-90B, NIST, Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018
[56A]	SP 800-56A Revision 3, NIST, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, April 2018
[8446]	RFC 8446, E. Lescorla, “The Transport Layer Security (TLS) Protocol Version 1.3”, Section 7.1, RFC 8446, August 2018

Table 19 – References

Term	Definition
AAA	Authentication, Authorization and Accounting - access control, policy enforcement and auditing framework for computing systems, e.g. LDAP
AMC	Administration Management Console
ESP	Encapsulated Security Payload (a subset of IPsec, Internet Protocol Security)
IKE	Internet Key Agreement, a key agreement scheme associated with IPsec (but not used by the module)
GMS	Global Management System
GUI	Graphical User Interface
LDAP	Lightweight Directory Access Protocol
PKCS #12	Public-Key Cryptography Standards #12, regarding certificate formats.
RADIUS	Remote Authentication Dial-In Service
SAML	Security Assertion Markup Language
SNMP	Simple Network Management Protocol
SSH	Secure Shell
VPN	Virtual Private Network
TLS	Transport Layer Security

Table 20 – Acronyms and Definitions (for terms not defined in FIPS 140-2 and associated documents)