AudioCodes Ltd.

Mediant Virtual Edition SBC and Cloud Edition SBC

Software Version: 7.6

FIPS 140-3 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.8

Prepared for:

AudioCodes Ltd.
1 Hayarden Street
Airport City, Lod 70151
Israel

Phone: +972 3 976 4000
www.audiocodes.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Abstract

This is a non-proprietary Cryptographic Module Security Policy for the Mediant Virtual Edition SBC and Cloud Edition SBC (version: 7.6) from AudioCodes Ltd. (AudioCodes). This Security Policy describes how the Mediant Virtual Edition SBC and Cloud Edition SBC meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS).

This document also describes how to run the module in an Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-3 validation of the module.

The Mediant Virtual Edition SBC and Cloud Edition SBC represent two deployments of the same software image that differ only in the product labeling, which is defined by an initialization file parameter that is set by the vendor. Collectively, these deployments are referred to in this document as “Mediant VE and CE SBCs”, “SBCs” or “the module”.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-3 cryptographic module security policy. More information is available on the module from the following sources:

- The AudioCodes website (www.audiocodes.com) contains information on the full line of products from AudioCodes.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

Document Organization

ISO/IEC 19790 Annex B uses the same section naming convention as *ISO/IEC 19790* section 7 - Security requirements. For example, Annex B section B.2.1 is named “General” and B.2.2 is named “Cryptographic module specification,” which is the same as *ISO/IEC 19790* section 7.1 and section 7.2, respectively. Therefore, the format of this Security Policy is presented in the same order as indicated in Annex B, starting with “General” and ending with “Mitigation of other attacks.” If sections are not applicable, they have been marked as such in this document.

Table of Contents

List of Tables

List of Figures

1. General

AudioCodes Ltd. (hereafter referred to as AudioCodes) is a leading vendor of advanced networking and media processing solutions for the for the digital workplace. The AudioCodes Mediant family of Session Border Controllers (SBCs) offers a line of versatile IP[1] communications platforms that connect VoIP[2] and TDM[3] networks, built on years of carrier-grade VoIP deployments and expertise. AudioCode's SBCs provide the interoperability, security, and quality assurance that service providers need to connect their enterprise and residential customers reliably and securely to SIP[4] trunk and hosted telephony services.

The Mediant Virtual Edition SBC and Cloud Edition SBC each forms an effective demarcation point between a business's VoIP network and the service provider's SIP trunk, performing SIP protocol mediation and media handling (interoperability), and securing the enterprise VoIP network. It can function as a peering SBC, access SBC, or enterprise SBC.

The AudioCodes Mediant Virtual Edition SBC and Cloud Edition SBC are software-based SBCs that may be installed in a virtual environment or hosted in a cloud computing environment.

The SBCs provide proven performance, resiliency, and security featuring real-time encryption (VoIP signaling and media traffic), DSP[5]-based media transcoding, a flexible and intuitive SIP routing engine, and an integrated WebRTC gateway. Some of the network and security features provided by the SBCs include:

- SIP B2BUA[6]
- SIP Interworking
- Extensive PBX[7] interoperability
- Transport Mediation between SIP over UDP[8]/TCP[9]/TLS[10]/WebSocket, IPv4/IPv6, RTP[11]/SRTP[12] SDES[13]/DTLS[14]
- Header Manipulation
- Local and far-end NAT[15] traversal
- Integrated WebRTC gateway with support for WebSocket, Opus, VP8[16] video coder, lite ICE[17], DTLS, RTP multiplexing, and secure RTCP[18] with feedback

[1] IP – Internet Protocol
[2] VoIP – Voice Over Internet Protocol
[3] TDM – Time-Division Multiplexing
[4] SIP – Session Initiation Protocol
[5] DSP – Digital Signal Processing
[6] B2BUA – Back-to-Back User Agent
[7] PBX – Private Branch Exchange
[8] UDP – User Datagram Protocol
[9] TCP – Transport Control Protocol
[10] TLS – Transport Layer Security
[11] RTP – Real-time Transport Protocol
[12] SRTP – Secure Real-time Transport Protocol
[13] SDES – Session Description Protocol Security Descriptions
[14] DTLS – Datagram Transport Layer Security
[15] NAT – Network Address Translation
[16] VP8 – Video coding format developed by Google
[17] ICE – Interactive Connectivity Establishment
[18] RTCP – Real-Time Transport Control Protocol

- Denial of service protection with DoS[19]/DDoS[20] line rate protection,
- VOIP firewall and deep packet inspections with rogue RTP detection and prevention
- Encryption and authentication with support for TLS, DTLS, SRTP, HTTPS[21], SSH[22], SFTP[23], and SNMP[24]
- Topology hiding and user privacy
- Traffic separation with VLAN[25]/physical interface separation for multiple media, control and OAMP[26] interfaces
- Call Admission Control
- Full Quality of Experience (QoE) monitoring: Jitter, Packet Loss, Delay and MOS[27]

Management of the SBC is accomplished via the following methods:

- Command Line Interface (CLI), which is accessible using the following means:
  - remotely via Ethernet management ports over SSH
  - locally via direct attachment to the RS-232 serial port using a VT100 terminal or a general-purpose computer with a terminal emulation program
  - locally via direct attachment using a VGA monitor and USB-enabled keyboard

- Web-based Graphical User Interface (GUI) called the Web Interface, which is accessible remotely via HTTPS over Ethernet management ports.

- SNMPv3 operations, which are used for remote configuration and obtaining information about the module's state and statistics.

- INI Configuration file, which is a text-based file with .ini file extension containing configuration settings. This file may be loaded to the SBC using SNMPv3 or by using the CLI (over SSH) or Web Interface for automatic configuration/commissioning.

These management interfaces provide authorized operators access to the module for configuration and management of all facets of the module's operation, including system configuration, troubleshooting, security, and service provisioning. Using any of the management interfaces, an operator is able to monitor, configure, control, receive report events, and retrieve logs from the SBC.

To support TLS and SSH, the following types of RSA certificates may be imported to the module using the module's Web Interface (over TLS) or CLI (over SSH):

- X.509 certificate file – plaintext base64 encoded PEM[28] format. These files contain public keys only, while the matching private key is contained in the associated RSA private key file.

[19] DoS – Denial of Service
[20] DoS/DDoS – Denial-of-Service/Distributed Denial-of-Service
[21] HTTPS – Hypertext Transfer Protocol Secure
[22] SSH – Secure Shell
[23] SFTP – SSH (or Secure) File Transfer Protocol
[24] SNMP – Simple Network Management Protocol
[25] VLAN – Virtual Local Area Network
[26] OAMP – Operations, Administration, Maintenance, and Provisioning
[27] MOS – Mean Opinion Score
[28] PEM – Privacy Enhanced Mail

- RSA private key file – plaintext base64 encoded PEM format. These files contain the private key associated with the RSA public key in the X.509 certificate file.

- Root certificate file (CA Public keys) – chains of X.509 certificates in plaintext base64 encoded PEM format. These are used to validate peer certificates and serve as a possible chain used for self-signed certificates to be sent to the peer. The Root certificate file contains public keys only; they do not contain the associated private keys.

The module generates RSA keypairs and Certificate Signing Requests (CSRs). The CSR is signed with the module's private key and then sent to a CA. The CA then signs the certificate and sends it back, where it is then installed for use. The module also generates self-signed certificates corresponding to the internally generated RSA keypairs.

The module provides the option to import certain CSPs by loading a text-based file with a *.ini file extension (INI file) in encrypted form using the module's Web Interface (over TLS) or CLI (over SSH). The module also supports an Automated Update mechanism whereby an INI file is downloaded from a server over HTTPS. The CSPs that may be imported through an INI file are indicated as such in Table 10 below.

The Mediant Virtual Edition SBC and Cloud Edition SBC is validated at the FIPS 140-3 section levels shown in Table 1.

Table 1 – Security Levels

ISO/IEC 24579 Section 6. [Number Below]	FIPS 140-3 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

The module has an overall security level of 1.

2. Cryptographic Module Specification

The Mediant VE and CE SBCs version 7.6 is a software cryptographic module with a multiple-chip standalone embodiment that meets overall Level 1 FIPS 140-3 requirements. The module is designed to operate within a modifiable operational environment and executes as a virtual appliance.

The sections below describe the operational environments, algorithm implementations, module boundary, and modes of operation.

2.1 Operational Environments

The module was tested and found to be compliant with FIPS 140-3 requirements on the environments listed in Table 2.

Table 2 – Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	VMware ESXi 7.0 w/custom Linux based on CentOS Stream 8	HPE ProLiant DL360 Gen10	Intel Xeon Gold 6226R	Without

The cryptographic module maintains validation compliance when operating in a virtual machine (VM) with AudioCodes' custom OS as the guest OS on any compatible GPC using one of the following hypervisors to provide the virtualization layer:

Table 3 – Vendor Affirmed Operational Environments

#	Operating System	Hardware Platform
1	Linux KVM	Any Compatible GPC
2	Microsoft Hyper-V	Any Compatible GPC

Note that the host GPC may be deployed on-prem or in one of the following supported cloud computing environments:

- OpenStack
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

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

2.2 Algorithm Implementations

The module employs the cryptographic algorithm implementations from the sources listed in Table 4 below.

Table 4 – Cryptographic Algorithm Sources

Certificate Number	Implementation Name	Version	Use
A2389	AudioCodes Mediant Session Border Controller KDF Library	7.6	Provides implementations for TLS, SNMP, SRTP, and SSH[29] key derivation functions
A2390	AudioCodes Mediant Session Border Controller Entropy Library	7.6	Provides SHA3 for entropy generation
A2544	AudioCodes Mediant Session Border Controller Cryptographic Library	7.6	Provides implementations for general-purpose cryptographic primitives

Validation certificates for each Approved security function are listed in Table 5. The module also includes implementations that are used solely to support self-tests; only the implementations in the table below are used by the module during operation.

Table 5 – Approved Algorithms

CAVP Cert[30]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
AudioCodes Mediant Session Border Controller KDF Library				
A2389	**KDF SNMP** **CVL**[31] *SP 800-135rev1*	KDF (SNMP)	Password Length: 64-800 Increment 8	Key Derivation *No part of the SNMP protocol, other than the KDFs, have been tested by the CAVP and CMVP.*
A2389	**KDF SRTP** **CVL** *SP 800-135rev1*	KDF (SRTP)	128, 256	Key Derivation *No part of the SRTP protocol, other than the KDFs, have been tested by the CAVP and CMVP.*
A2389	**KDF SSH** **CVL** *SP 800-135rev1*	KDF (SSH)	AES-128 (SHA-1, SHA2-256)	Key Derivation *No part of the SSH protocol, other than the KDFs, have been tested by the CAVP and CMVP.*
A2389	**TLS v1.2 KDF RFC**[32] **7627** **CVL** *SP 800-135rev1* *RFC 7627*	KDF (TLS[33] v1.2)	SHA2-256, SHA2-384, SHA2-512	Key Derivation *No part of the TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.*

[29] SSH – Secure Shell
[30] This table includes vendor-affirmed algorithms that are approved but CAVP testing is not yet available.
[31] CVL – Component Validation List
[32] RFC – Request for Comments
[33] TLS – Transport Layer Security

CAVP Cert[30]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2389	**TLS v1.3 KDF** **CVL** *SP 800-135rev1* *RFC 8446*	KDF (TLS v1.3)	SHA2-256, SHA2-384	Key Derivation *No part of the TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.*
AudioCodes Mediant Session Border Controller Entropy Library				
A2390	**SHA3-256** *FIPS PUB 202*	SHA3-256	-	Conditioning function for entropy
AudioCodes Mediant Session Border Controller Cryptographic Library				
A2544	**AES-CBC** *FIPS PUB 197* *NIST SP 800-38A*	CBC	128, 256	Encryption/Decryption
A2544	**AES-CCM**[34] *NIST SP 800-38C*	CCM	128, 256	Encryption/Decryption
A2544	**AES-CFB128** *FIPS PUB 197* *NIST SP 800-38A*	CFB128	128, 192, 256	Encryption/Decryption
A2544	**AES-CTR** *FIPS PUB 197* *NIST SP 800-38A*	CTR	128, 256	Encryption/Decryption
A2544	**AES-GCM**[35] *NIST SP 800- 38D*	GCM	128, 256	Encryption/Decryption
A2544	**Counter DRBG**[36] *NIST SP 800-90Arev1*	Counter-based	256-bit AES-CTR	Deterministic random bit generation
A2544	**DSA**[37] **KeyGen (FIPS186-4)** *FIPS PUB 186-4*	DSA KeyGen	2048/256	Key Pair Generation
A2544	**ECDSA**[38] **KeyGen (FIPS186-4)** *FIPS PUB 186-4*	ECDSA KeyGen Secrets generation mode: Testing candidates	P-224, P-256, P-384, P-521	Key Pair Generation
A2544	**ECDSA KeyVer (FIPS186-4)** *FIPS PUB 186-4*	ECDSA KeyVer	P-224, P-256, P-384, P-521	Public Key Verification
A2544	**ECDSA SigVer (FIPS186-4)** *FIPS PUB 186-4*	ECDSA SigVer	P-256 (SHA2-256)	Digital Signature Verification
A2544	**HMAC-SHA-1** *FIPS PUB 198-1*	SHA-1	MAC: 32, 80, 160 Key Length: 160	Message Authentication *The module also supports HMAC SHA-1-32 and HMAC SHA-1-80.*

[34] CCM – Counter with Cipher Block Chaining - Message Authentication Code
[35] GCM – Galois Counter Mode
[36] DRBG – Deterministic Random Bit Generator
[37] DSA – Digital Signature Algorithm
[38] ECDSA – Elliptic Curve Digital Signature Algorithm

CAVP Cert[30]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2544	**HMAC-SHA2-256** *FIPS PUB 198-1*	SHA2-256	MAC: 256 Key Length: 256	Message Authentication
A2544	**HMAC-SHA2-384** *FIPS PUB 198-1*	SHA2-384	MAC: 384 Key Length: 384	Message Authentication
A2544	**KAS-ECC-SSC[39] SP800-56Arev3** *NIST SP 800-56Arev3*	ephemeralUnified	P-224, P-256, P-384, P-521	Shared Secret Computation
A2544	**KAS-FFC-SSC[40] SP800-56Arev3** *NIST SP 800-56Arev3*	dhEphem	FC (2048/256), ffdhe2048, ffdhe3072, MODP-2048	Shared Secret Computation
A2544	**RSA[41] KeyGen (FIPS186-4)** *FIPS PUB 186-4*	Key generation mode: B.3.3	2048, 3072, 4096	Key Pair Generation
A2544	**RSA SigGen (FIPS186-4)** *FIPS PUB 186-4*	PKCS#1 v1.5	2048, 3072, 4096 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Generation
A2544	**RSA SigVer (FIPS186-4)** *FIPS PUB 186-4*	PKCS#1 v1.5	1024, 2048, 3072, 4096 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Verification
A2544	**SHA-1** *FIPS PUB 180-4*	SHA-1	Message Length: 0-65528 Increment 8	Message Digest
A2544	**SHA2-224** *FIPS PUB 180-4*	SHA2-224	Message Length: 0-65528 Increment 8	Message Digest
A2544	**SHA2-256** *FIPS PUB 180-4*	SHA2-256	Message Length: 0-65528 Increment 8	Message Digest
A2544	**SHA2-384** *FIPS PUB 180-4*	SHA2-384	Message Length: 0-65528 Increment 8	Message Digest
A2544	**SHA2-512** *FIPS PUB 180-4*	SHA2-512	Message Length: 0-65528 Increment 8	Message digest
A2544	**Safe Primes Key Generation** *NIST SP 800-56Arev3, Appendix D*	-	ffdhe2048, fdhe3072, MODP-2048	Key Generation
A2544	**Safe Primes Key Verification** *NIST SP 800-56Arev3, Appendix D*	-	ffdhe2048, fdhe3072, MODP-2048	Key Verification
Security Function Implementations (SFIs)				
AES-CBC A2544 HMAC A2544	**KTS** *NIST SP 800-38F*	SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys providing between 128 and 256 bits of encryption strength	Key Wrap/Unwrap (Encryption with message authentication) AES-CBC with HMAC (SHA-1, SHA2-256, SHA2-384)

[39] KAS-ECC-SSC – Key Agreement Scheme - Elliptic Curve Cryptography - Shared Secret Computation
[40] KAS-FFC-SSC – Key Agreement Scheme - Finite Field Cryptography - Shared Secret Computation
[41] RSA – Rivest Shamir Adleman

CAVP Cert[30]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
AES-CCM A2544	**KTS** *NIST SP 800-38F*	SP 800-38C and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128 and 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrap/Unwrap (Authenticated Encryption)
AES-CFB128 A2544 HMAC A2544	**KTS** *NIST SP 800-38F*	SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys providing between 128 and 256 bits of encryption strength	Key Wrap/Unwrap (Encryption with message authentication) AES-CFB128 with HMAC (SHA-1, SHA2-256, SHA2-384)
AES-GCM A2544	**KTS** *NIST SP 800-38F*	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128 and 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrap/Unwrap (Authenticated Encryption)
KAS-ECC-SSC A2544 KDF SSH A2389	**KAS**[42] *NIST SP 800-56Arev3* *NIST SP 800-135rev1*	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-224, P-256, P-384, and P-521 curves providing between 112 and 256 bits of encryption strength.	Key Agreement
KAS-ECC-SSC A2544 TLS v1.2 KDF RFC 7627 A2389	**KAS** *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *RFC 7627*	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-224, P-256, P-384, and P-521 curves providing between 112 and 256 bits of encryption strength.	Key Agreement
KAS-ECC-SSC A2544 TLS v1.3 KDF A2389	**KAS** *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *RFC 8446*	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-224, P-256, P-384, and P-521 curves providing between 112 and 256 bits of encryption strength.	Key Agreement
KAS-FFC-SSC A2544 KDF SSH A2389	**KAS** *NIST SP 800-56Arev3* *NIST SP 800-135rev1*	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength.	Key agreement
KAS- FFC -SSC A2544 TLS v1.2 KDF RFC 7627 A2389	**KAS** *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *RFC 7627*	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength.	Key Agreement
KAS- FFC -SSC A2544 TLS v1.3 KDF A2389	**KAS** *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *RFC 8446*	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength.	Key Agreement
Entropy Source				

[42] KAS – Key Agreement Scheme

CAVP Cert[30]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
N/A	**ENT (NP)** *NIST SP 800-90B*	-	-	Entropy input for DRBG
Vendor Affirmed				
Vendor Affirmed	**CKG**[43] *NIST SP 800-133rev2*	-	-	Cryptographic Key Generation

The vendor affirms the following cryptographic security methods:

- Cryptographic key generation – As per sections 4 and 5.1 of *NIST SP 800-133rev2*, the module uses its Approved DRBG to generate seeds for generation of asymmetric keys. The resulting generated seed is an unmodified output from the DRBG. The module's DRBG is seeded via entropy generated from a CPU jitter-based entropy source internal to the module (the module requests a minimum number of 256 bits of entropy per call).

Table 6 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use / Function
RSA SigVer (FIPS 186-4)	Only allowed for non-security relevant use of unclaimed authentication mechanism with SSH and SFTP per IG 2.4.A, Scenario 2	Non-legacy use of RSA Signature Verification: 1024 ≤ len(n) < 2048 (provides < 112 bits of security strength)

The module does not include any non-Approved algorithms allowed in the Approved mode of operations.

The module does not include any non-Approved algorithms not allowed in the Approved mode of operations.

2.3 Cryptographic Boundary

As a virtual appliance, the cryptographic module has no physical characteristics, it makes use of the physical interfaces of the server upon which the virtual appliance is installed. Figure 1 below illustrates a block diagram of a typical GPC and the module's physical perimeter.

[43] CKG – Cryptographic Key Generation

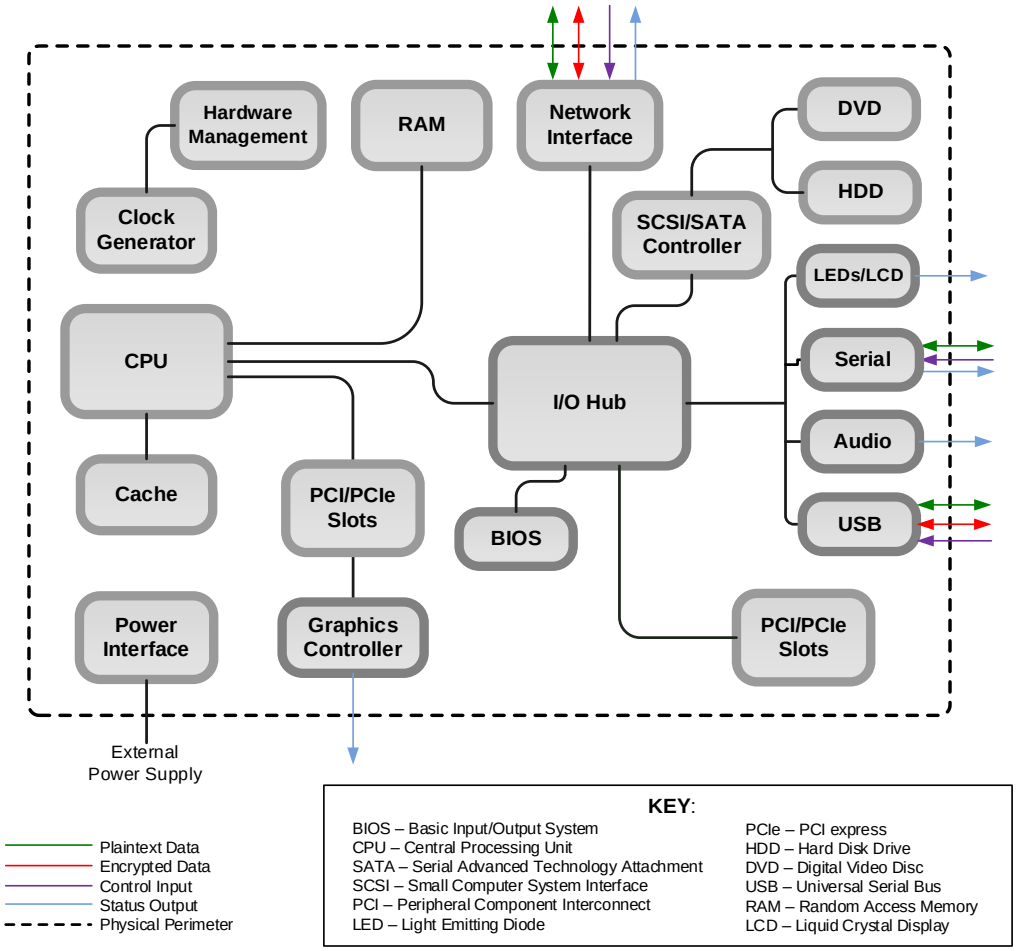

Figure 1 – GPC Block Diagram

The module consists of binary packaged into an executable that can be run in a virtual environment. The hypervisor controls and directs all interactions between the module and the physical appliance, and it is responsible for mapping the module's virtual interfaces to the host server's physical interfaces. The physical perimeter of the cryptographic module is defined by the hard enclosure around the server on which it runs.

The cryptographic boundary of the module (shown by the red dotted line in Figure 2 below) consists of the AudioCodes Mediant SBC application and AudioCodes' custom OS running in a virtual machine. The module's physical perimeter is illustrated by the black dotted line.

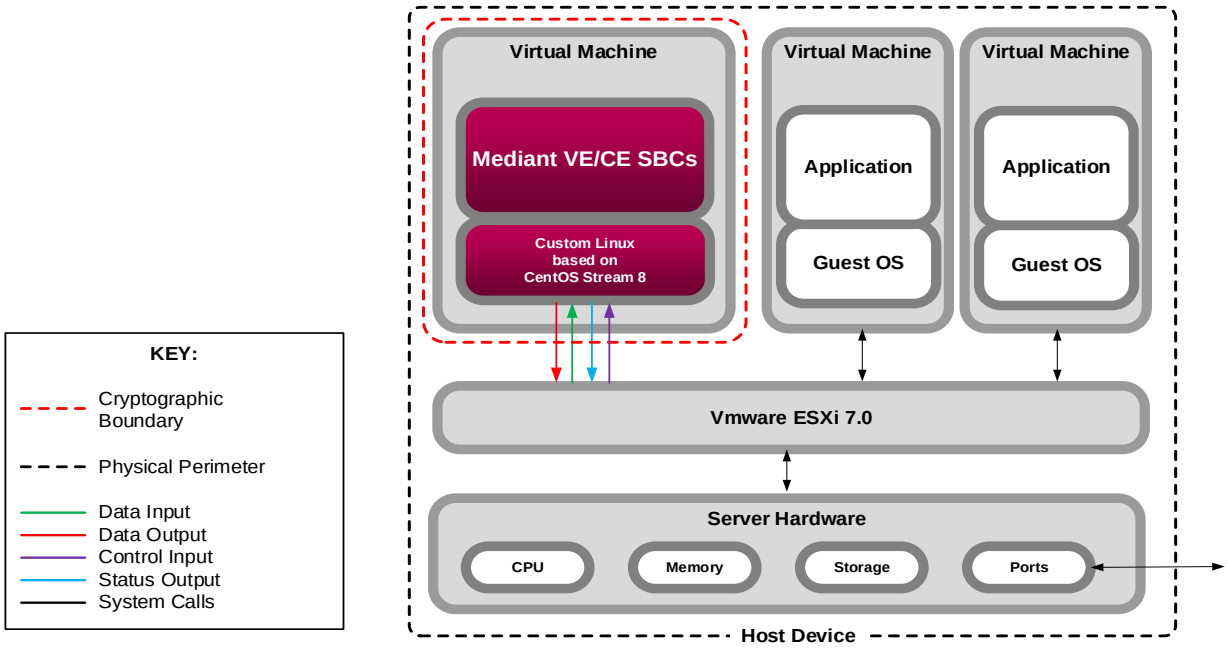

Figure 2 – AudioCodes Mediant VE and CE SBCs Cryptographic Boundary

There are no module components excluded from the requirements.

2.4 Modes of Operation

The module supports the Approved mode of operation only. When installed, configured, and operated according to this Security Policy, the module does not support a non-Approved mode of operation.

3. Cryptographic Module Interfaces

FIPS 140-3 defines the following logical interfaces for cryptographic modules:

- Data Input
- Data Output
- Control Input
- Control Output
- Status Output

Note that the module does not output control information, and thus has no specified control output interface.

As a software cryptographic module, the module has no physical characteristics. Its interfaces are logical; the hypervisor provides virtualized ports and interfaces for the module that map to the host server's physical ports and interfaces. The module relies on the physical and electrical characteristics, manual controls, and physical indicators of the host server.

The module was tested and validated on an HP ProLiant DL360 Gen10 server. The following is a list of the physical interfaces implemented on the tested host server:

- 1 GbE and 10 GbE SFP+ Ethernet ports
- USB-enabled keyboard port
- Serial port
- Video port
- LEDs[44]
- AC[45] Power port

The virtual machine hosting the module virtualizes the physical interfaces. Table 7 below provides the mapping of the FIPS-defined interfaces and the module's physical and logical interfaces.

Table 7 – Ports and Interfaces

Physical Port	Logical Interface	Data That Passes Over Port/Interface
Host server Ethernet port(s)	Virtual Ethernet port(s) • Data input • Data output • Control input • Status output	Management traffic; media and signaling traffic; operational/system status information
Host server USB-enabled keyboard port(s)	Virtual USB port(s) • Data Input • Control Input	Management traffic via CLI

[44] LED – Light-Emitting Diode
[45] AC – Alternating Current

Physical Port	Logical Interface	Data That Passes Over Port/Interface
Host platform serial port	Virtual serial port • Data input • Data output • Control input • Status output	Management traffic via CLI
Host platform video connector	Virtual video connector • Data output • Status output	CLI status information
Host server LEDs	Virtual LEDs • Status output	Operational/system status information

4. Roles, Services, and Authentication

The sections below describe the module's authorized roles, services, and operator authentication methods.

4.1 Authorized Roles

The module supports two roles that operators may assume:

- Crypto Officer (CO) role – The CO is responsible for initializing the module for first use, which includes the configuration of passwords, public and private keys, and other CSPs. The CO is also responsible for the management of all keys and CSPs, including their zeroization, and is the only operator that can configure the module for Approved mode operation. The CO has access to all User services and can also perform services via SNMPv3.

- User role – The User has read-only privileges and can show the status and statistics of the module, show the current status of the module, and connect to the module remotely using HTTPS or SSH. Users can also change their own passwords.

The CO and User roles are tied to administrative roles supported by the module. The CO role is equivalent in terms of privileges to the AudioCodes-defined "Security Administrator" and "Master" administrative role. The User role is equivalent to the AudioCodes-defined "Monitor" role. Both roles can access the Web Interface and CLI.

Table 8 below lists the supported roles, along with the services (including input and output) available to each role.

Table 8 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Show Module Versioning Information	None	Module name and version information
CO	Commission the Module	None	None
CO	Load License Key File	Command	Status output
CO	Configure the SBC System	Command and parameter	Command response/ Status output
CO	Configure VOIP Network, Media and SIP Settings, and Routing Rules	Command and parameters	Command response/ Status output
CO	Manage Users	Command and parameters	Command response/ Status output
CO	Manage User Sessions	Command and parameters	Command response/ Status output
CO	Change Password	Command and parameters	Command response/ Status output
CO, User	Change Own Password	Command and parameters	Command response/ Status output

Role	Service	Input	Output
CO	Manage Certificates/Keypairs	Command and parameters	Command response/ Status output
CO	Configure TLS Contexts	Command and parameters	Command response/ Status output
CO	Perform On-Demand Self-Tests	Command	Command response/ Status output
CO, User	Show Status	Command	Command response/ Status output
CO, User	Show System Security Status	Command	Command response/ Status output
CO, User	View Syslog	Command	Command response/ Status output
CO	Zeroize Keys and CSPs	Command	Command response/ Status output
CO	Upgrade Image	Command	Command response/ Status output
CO	Load a .ini File and Perform Automatic Updates	Command	Command response/ Status output
CO	Save a .ini File of the Module's Configuration	Command	Command response/ Status output
CO	Reset	Command	Command response/ Status output
CO User	Establish TLS Session	Command	TLS session established
CO User	Establish SSH Session	Command	SSH session established
CO	Configure SNMPv3 Users	Command and parameters	Command response/ Status output
CO	Establish SNMPv3 Session	Command and parameters	SNMP session established
CO	Establish SRTP Session	Command and parameters	SRTP session established
CO	Establish SFTP Session	Command and parameters	SFTP session established
CO	Restore Default Configuration	Command	Factory default settings restored
N/A	Perform Manual Zeroization	Reboot/power cycle host device	Status output
N/A	Perform Manual On-Demand Self-Tests	Reboot or power cycle host device	Status output
N/A	Authenticate	Command	Status output

4.2 Authentication

Each operator has their own account with a username and password which are used to authenticate to the module. Passwords are stored on non-volatile storage media (outside the module boundary but within the physical perimeter) in hashed form using SHA2-256. For SSH/SFTP, operators can also utilize RSA or ECDSA Public keys.

Note that, while the module supports authentication mechanisms, no claims are being made with regards to compliance to the Level 2/3 role-based and identity-based authentication requirements since it is being certified at Level 1.

4.3 Externally Loaded Software

The module has the capability to load software in the form of a complete image replacement from an external source. As such a replacement will constitute a new module, only FIPS-validated software may be loaded to maintain the module's validation.

Services and functions provided by the newly loaded software image are not performed until the pre-operational self-tests have executed successfully via a power-on reset. All software images are digitally signed, and a conditional self-test (using an ECDSA signature verification with P-256 curve) is performed during the reset. If the signature test fails, the new software image is ignored and the previous-loaded software image remains current.

SSP zeroization takes place prior to execution of the new image. The module's versioning information is updated to reflect the addition/update of the newly loaded software.

4.4 Services

Descriptions of the services available to authenticated module operators are provided in Table 9 below.

As allowed per section 2.4.C of *FIPS 140-3 Implementation Guidance*, the module provides indicators for the use of Approved services through a combination of an explicit indication (via a global mode indicator) and an implicit indication (via the successful completion of the service).

Please note that the keys and Sensitive Security Parameters (SSPs) listed in the table indicate the type of access required using the following notation:

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

Table 9 – Approved Services

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Show Module Versioning Information	Show the model and software version.	None	None	CO	N/A	N/A
Commission the Module	Commission the module by following the Security Policy guidelines	None	None	CO	N/A	Global Indicator (“FIPS mode: Enabled”)
Load License Key File	Load a License Key file to change or upgrade features	None	None	CO	N/A	Global Indicator (“FIPS mode: Enabled”)
Configure the SBC System	Configure IP address, Web Interface and CLI, LAN and WAN settings, and date and time; save and load configuration files; save and load CLI script files	None	None	CO, User (view only)	N/A	Global Indicator (“FIPS mode: Enabled”)
Configure VOIP Network, Media and SIP Settings, and Routing Rules	Configure IP network topology, media and SIP settings, and routing rules	None	None	CO, User (view only)	N/A	Global Indicator (“FIPS mode: Enabled”)
Manage Users	Create, edit, or delete user accounts; assign passwords and roles; import SSH public key	SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544)	SSH Public Key	CO	SSH Public Key – W	Global Indicator (“FIPS mode: Enabled”)
Manage User Sessions	Terminate specific user’s CLI session	None	None	CO	N/A	Global Indicator (“FIPS mode: Enabled”)
Change Password	Modify CO or User account passwords	SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544)	None	CO	N/A	Global Indicator (“FIPS mode: Enabled”)
Change Own Password	Modify existing login passwords	SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384	None	CO, User	N/A	Global Indicator (“FIPS mode: Enabled”)

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
		(Cert. A2544)				
Manage Certificates/ Keypairs	Generate RSA/ECDSA keypairs for certificate signing requests, generate RSA private keys, load certificates and private keys via TLS/SSH	CKG (Vendor Affirmed) Counter DRBG (Cert. A2544) ECDSA KeyGen (FIPS186-4) (Cert. A2544) ENT (NP) RSA KeyGen (FIPS186-4) (Cert. A2544) SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544) SHA3-256 (Cert. A2390)	Entropy Input String DRBG Seed DRBG 'Key' Value DRBG 'V' Value RSA Private Key RSA Public Key ECDSA Private Key ECDSA Public Key CA[46] Public Key	CO	Entropy Input String – G/E DRBG Seed – G/E DRBG 'Key' Value – G/E DRBG 'V' Value – G/E RSA Private Key – G RSA Public Key – G ECDSA Private Key – G ECDSA Public Key – G CA Public Key – W	Global Indicator ("FIPS mode: Enabled")
Configure TLS Contexts	Define TLS version and cipher suites for management and data TLS connections	None	None	CO	N/A	Global Indicator ("FIPS mode: Enabled")
Perform On-Demand Self-Tests	Perform on-demand self-tests	None	Software Integrity Test Key	CO	Software Integrity Test Key – E	Global Indicator ("FIPS mode: Enabled")
Show Status	Show the system status, Ethernet status, alarms, user activity logs, system identification and configuration settings of the module	None	None	CO, User	N/A	N/A
Show System Security Status	Show the system security status: "FIPS Approved mode"	None	None	CO, User	N/A	N/A
View Syslog	View event status messages in the syslog	None	None	CO, User	N/A	Global Indicator ("FIPS mode: Enabled")

[46] CA – Certificate Authority

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Zeroize Keys and CSPs	Zeroize keys and CSPs	None	All persistent CSPs	CO	All persistent CSPs – Z	N/A
Upgrade Image	Load new software image	ECDSA SigVer (FIPS186-4) (Cert. A2544) SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544)	Image Verification Key	CO	Image Verification Key – E	Global Indicator ("FIPS mode: Enabled")
Load a .ini File and Perform Automatic Updates	Load the module's configuration as a .ini file and perform automatic updates	None	ECDSA Private Key ECDSA Public Key RSA Private Key RSA Public Key CA Public Key SSH Private Key SSH Public Key SNMPv3 Authentication Password SNMPv3 Privacy Password	CO	ECDSA Private Key – W ECDSA Public Key – W RSA Private Key – W RSA Public Key – W CA Public Key – W SSH Private Key – W SSH Public Key – W SNMPv3 Authentication Password – W SNMPv3 Privacy Password – W	Global Indicator ("FIPS mode: Enabled")
Save a .ini File of the Module's Configuration	Save a .ini file of the module's configuration	None	None	CO	N/A	Global Indicator ("FIPS mode: Enabled")
Reset	Reset the module	None	SSPs stored in RAM	CO	SSPs stored in RAM – Z	Global Indicator ("FIPS mode: Enabled")
Establish TLS Session	Establish web session using TLS protocol	AES-CBC (Cert. A2544) AES-GCM (Cert. A2544) CKG (Vendor Affirmed) Counter DRBG (Cert. A2544) DSA KeyGen (FIPS186-4) (Cert. A2544) ECDSA KeyGen (FIPS186-4) (Cert. A2544) ENT (NP) HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544) KAS (Cert. A2544) KAS-ECC-SSC SP800-56Arev3 (Cert. A2544)	Entropy Input String DRBG Seed DRBG 'Key' Value DRBG 'V' Value DH Public Key DH Private Key DH Peer Public Key ECDH Public Key ECDH Private Key ECDH Peer Public Key TLS Private Key TLS Public Key TLS Pre-Master Secret TLS Master Secret TLS Session Key TLS Authentication Key	CO, User	Entropy Input String – G/E DRBG Seed – G/E DRBG 'Key' Value – G/E DRBG 'V' Value – G/E DH Public Key – G/R DH Private Key – G/E DH Peer Public Key – G/W/E ECDH Public Key – G/R ECDH Private Key – G/E ECDH Peer Public Key – G/W/E TLS Private Key – G/W/E TLS Public Key – G/W/R TLS Pre-Master Secret – G/R/E TLS Master Secret – G/E TLS Session Key – G/E TLS Authentication Key – G/E	Global Indicator ("FIPS mode: Enabled")

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
		KAS-FFC-SSC SP800-56Arev3 (Cert. A2544) KTS (AES-CCM) (Cert. A2544) KTS (AES-GCM) (Cert. A2544) KTS (AES-CBC/HMAC) (Cert. A2544) RSA SigGen (FIPS186-4) (Cert. A2544) RSA SigVer (FIPS186-4 (Cert. A2544) Safe Primes Key Generation (Cert. A2544) Safe Primes Key Verification (Cert. A2544) SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544) SHA3 -256 (Cert. A2390) TLS v1.2 KDF RFC 7627 (Cert. A2389) TLS v1.3 KDF (Cert. A2389)				
Establish SSH Session	Establish remote session using SSH protocol	AES-CBC (Cert. A2544) CKG (Vendor Affirmed) DRBG (Cert. A2544) DSA KeyGen (FIPS186-4) (Cert. A2544) ECDSA KeyGen (FIPS186-4) (Cert. A2544) ENT (NP) HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544) KAS (Cert. A2544)	Entropy Input String DRBG Seed DRBG 'Key' Value DRBG 'V' Value DH Public Key DH Private Key DH Peer Public Key ECDH Public Key ECDH Private Key ECDH Peer Public Key SSH Private Key SSH Public Key SSH Shared Secret SSH Session Key SSH Authentication Key	CO, User	Entropy Input String – G DRBG Seed – G/E DRBG 'Key' Value – G/E DRBG 'V' Value – G/E DH Public Key – G/R/E DH Private Key – G/E DH Peer Public Key – G/W/E ECDH Public Key – G/R/E ECDH Private Key – G/E ECDH Peer Public Key – G/W/E SSH Private Key – G/W/E SSH Public Key – G/W/R SSH Shared Secret – G/E SSH Session Key – G/E SSH Authentication Key – G/E	Global Indicator ("FIPS mode: Enabled")

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
		KAS-ECC-SSC SP800-56Arev3 (Cert. A2544) KAS-FFC-SSC SP800-56Arev3 (Cert. A2544) KDF SSH (Cert. A2389) KTS (AES-GCM) (Cert. A2544) KTS (AES-CBC/HMAC) (Cert. A2544) RSA SigGen (FIPS186-4) (Cert. A2544) RSA SigVer (FIPS186-4) (Cert. A2544) Safe Primes Key Generation (Cert. A2544) Safe Primes Key Verification (Cert. A2544) SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544) SHA3-256 (Cert. A2390)				
Configure SNMPv3 Users	Configure SNMPv3 users	AES-CFB128 (Cert. A2544) HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544) SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544)	SNMPv3 Authentication Password SNMPv3 Privacy Password SNMPv3 Privacy Key SNMPv3 Authentication Key	CO	SNMPv3 Authentication Password – W/E SNMPv3 Privacy Password – W/E SNMPv3 Session Key – W/E SNMPv3 Authentication Key – W/E	Global Indicator (“FIPS mode: Enabled”)
Establish SNMPv3 Session	Establish non-security-related monitoring session using SNMPv3 protocol	AES-CFB128 (Cert. A2544) HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544)	SNMPv3 Authentication Password SNMPv3 Privacy Password SNMPv3 Authentication Key SNMPv3 Privacy Key	CO	SNMPv3 Authentication Password – E SNMPv3 Privacy Password – E SNMPv3 Session Key – G/E SNMPv3 Privacy Key – G/E	Global Indicator (“FIPS mode: Enabled”)

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
		KDF SNMP (Cert. A2389) KTS (AES-CFB128/HMAC) (Certs. A2544) SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544)				
Establish SRTP Session	Establish session using SRTP protocol	AES-CTR (Cert. A2544) HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544) KDF SRTP (Cert. A2389) SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544)	SRTP Master Key SRTP Session Key SRTP Authentication Key	CO	SRTP Master Key – G/W SRTP Session Key – G/E SRTP Authentication Key – G/E	Global Indicator (“FIPS mode: Enabled”)
Establish SFTP Session	Establish session using SFTP protocol	AES-CBC (Cert. A2544) CKG (Vendor Affirmed) Counter DRBG (Cert. A2544) DSA KeyGen (FIPS186-4) (Cert. A2544) ECDSA KeyGen (FIPS186-4) (Cert. A2544) ENT (NP) HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544) KAS (Cert. A2544) KAS-ECC-SSC SP800-56Arev3 (Cert. A2544)	Entropy Input String DRBG Seed DRBG ‘Key’ Value DRBG ‘V’ Value DH Public Key DH Private Key DH Peer Public Key ECDH Public Key ECDH Private Key ECDH Peer Public Key SFTP Private Key SFTP Public Key SSH Shared Secret SSH Session Key SSH Authentication Key	CO	Entropy Input String – G DRBG Seed – G/E DRBG ‘Key’ Value – G/E DRBG ‘V’ Value – G/E DH Public Key – G/R/E DH Private Key – G/E DH Peer Public Key – G/W/E ECDH Public Key – G/R/E ECDH Private Key – G/E ECDH Peer Public Key – G/W/E SFTP Private Key – G/E SFTP Public Key – G/R SSH Shared Secret – G/E SSH Session Key – G/E SSH Authentication Key – G/E	Global Indicator (“FIPS mode: Enabled”)

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
		KAS-FFC-SSC SP800-56Arev3 (Cert. A2544) KDF SSH (Cert. A2389) KTS (AES-GCM) (Cert. A2544) KTS (AES-CBC/HMAC) (Cert. A2544) RSA SigGen (FIPS186-4) (Cert. A2544) RSA SigVer(FIPS186-4) (Cert. A2544) Safe Primes Key Generation (Cert. A2544) Safe Primes Key Verification (Cert. A2544) SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544) SHA3-256 (Cert. A2390)				
Restore Default Configuration	Restore settings to factory defaults	None	All persistent SSPs	CO	All persistent CSPs – Z	Global Indicator ("FIPS mode: Enabled")
Perform Manual Zeroization	Zeroize keys and CSPs	None	All ephemeral keys and CSPs	-	All ephemeral keys and CSPs – Z	N/A
Perform Manual On-Demand Self-Tests	Perform power-up self-tests on demand	None	Software Integrity Test Key All ephemeral keys and CSPs	-	Software Integrity Test Key – E All ephemeral keys and CSPs – Z	N/A
Authenticate	Use to log into the module	SHA-1 (Cert. A2544) SHA2-256 (Cert. A2544) SHA2-384 (Cert. A2544)	None	-	N/A	Global Indicator ("FIPS mode: Enabled")

Per FIPS 140-3 Implementation Guidance 2.4.C, the **Show Status, **Zeroize**, and **Show Versioning Information** services do not require an Approved security service indicator.*

The module does not provide any non-Approved services.

5. Software/Firmware Security

The module software takes the form of a single software image that includes multiple files (configuration files, executable files, packages, and other associated files). The image is verified using an approved integrity technique implemented within the cryptographic module itself. The module implements an ECDSA P-256 (SHA2-256) digital signature verification for the integrity test of the software. The approved integrity technique consists of single ECDSA signature verification; failure of the integrity check will cause the module to enter a critical error state.

The CO can initiate the pre-operational tests on demand by issuing a reset/reboot command over its management interfaces. Also, the module can be made to perform pre-operational self-tests by rebooting or power-cycling the module's VM or host device (when using this method, the operator is not required to assume an authorized role).

6. Operational Environment

The module is designed to operate within a modifiable operational environment. The module was tested and found to be compliant with FIPS 140-3 requirements on the operational environment identified in Table 2.

The cryptographic module has control over its own SSPs. The process and memory management functionality of the guest OS and the hypervisor prevents unauthorized access to plaintext private and secret keys, intermediate key generation values and other SSPs by external processes during module execution. The module only allows access to SSPs through its well-defined interfaces. The operational environment provides the capability to separate individual application processes from each other by preventing uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless of whether this data is in the process memory or stored on virtual storage within the operational environment. Processes that are spawned by the module are owned by the module and are not owned by external processes or operators.

7. Physical Security

The cryptographic module is software module and does not include physical security mechanisms. Therefore, per *ISO/IEC 19790:2021* section 7.7.1, the requirements for physical security are not applicable.

8. Non-Invasive Security

This section is not applicable. There are currently no approved non-invasive mitigation techniques referenced in *ISO/IEC 19790:2021* Annex F.

9. Sensitive Security Parameter Management

9.1 Keys and SSPs

The module supports the keys and other SSPs listed in Table 10 below.

Table 10 – SSPs

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[47]	Use & Related Keys
Keys								
Software Integrity Test Key (not an SSP)	128 bits	ECDSA SigVer (FIPS186-4) (Cert. A2544)	Hardcoded in the module image	-	-	Plaintext form in virtual RAM	Not subject to zeroization requirements	Pre-operational verification of module's software image
CA Public Key (CSP)	(ECDSA) Between 128 and 256 bits (RSA) Between 112 and 150 bits	ECDSA SigVer (FIPS186-4) (Cert. A2544) RSA SigVer (FIPS186-4) (Cert. A2544)	-	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Exported in PEM file format over TLS or SSH in encrypted form	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only)	Verification of CA signatures
RSA Private Key (CSP)	Between 112 and 150 bits	RSA SigGen (FIPS186-4) (Cert. A2544)	Generated internally via approved DRBG	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Exported in PEM file format over TLS or SSH in encrypted form	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only)	Used for certificate signing requests
RSA Public Key (PSP)	Between 112 and 150 bits	RSA SigVer (FIPS186-4) (Cert. A2544)	Generated internally via approved DRBG	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Exported in PEM file format over TLS or SSH in encrypted form	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only)	Used for certificate signing requests

[47] The indicators provided by zeroization methods specified in this column are implicit as the normal, non-error, status output of the function performing zeroization.

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[47]	Use & Related Keys
ECDSA Private Key (CSP)	Between 128 and 256 bits	ECDSA SigGen (FIPS186-4) (Cert. A2544)	Generated internally via approved DRBG	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Exported in PEM file format over TLS or SSH in encrypted form	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only)	Used for certificate signing requests
ECDSA Public Key (PSP)	Between 128 and 256 bits	ECDSA SigVer (FIPS186-4) (Cert. A2544)	Generated internally via approved DRBG	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Exported in PEM file format over TLS or SSH in encrypted form	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only)	Used for certificate signing requests
ECDH Private Key (CSP)	Between 128 and 256 bits	KAS-ECC-SSC SP800-56Arev3 (Cert. A2544)	Generated internally via approved DRBG	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Computation of KAS-ECC-SSC shared secrets during TLS/SSH key exchange
ECDH Public Key (PSP)	Between 128 and 256 bits	KAS-ECC-SSC SP800-56Arev3 (Cert. A2544)	Generated internally via approved DRBG	Never imported Exported in plaintext form	-	Plaintext form in virtual RAM	Soft reset/power cycle	Computation of KAS-ECC-SSC shared secrets during TLS/SSH key exchange
ECDH Peer Public Key (PSP)	Between 128 and 256 bits	KAS-ECC-SSC SP800-56Arev3 (Cert. A2544)	-	Imported in plaintext Never exported	-	Plaintext form in virtual RAM	Soft reset/power cycle	Computation of KAS-ECC-SSC shared secrets during TLS/SSH key exchange
DH Private Key (CSP)	112 bits	KAS-FFC-SSC SP800-56Arev3 (Cert. A2544) Safe Primes Key Generation (Cert. A2544) Safe Primes Key Verification (Cert. A2544)	Generated internally via approved DRBG	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Computation of KAS-FFC-SSC shared secrets during TLS/SSH key exchange
DH Public Key (PSP)	112 bits	KAS-FFC-SSC SP800-56Arev3 (Cert. A2544) Safe Primes Key Generation (Cert. A2544) Safe Primes Key Verification (Cert. A2544)	Generated internally via approved DRBG	Never imported Exported in plaintext form	-	Plaintext form in virtual RAM	Soft reset/power cycle	Computation of KAS-FFC-SSC shared secrets during TLS/SSH key exchange

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[47]	Use & Related Keys
DH Peer Public Key (PSP)	112 bits	KAS-FFC-SSC SP800-56Arev3 (Cert. A2544) Safe Primes Key Generation (Cert. A2544) Safe Primes Key Verification (Cert. A2544)	-	Imported in plaintext form Never exported	-	Plaintext form in virtual RAM	Soft reset/power cycle	Computation of KAS-FFC-SSC shared secrets during TLS/SSH key exchange
SSH Private Key (CSP)	112 or 128 bits	RSA SigGen (FIPS186-4) (Cert. A2544)	Generated internally via Approved DRBG	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Never exported	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only); zeroization command	Authentication during SSH session negotiation
SSH Public Key (PSP)	112 or 128 bits	RSA SigGen (FIPS186-4) (Cert. A2544)	Generated internally via Approved DRBG as part of CSR or self-signed certificate generation	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Imported by CO via CLI (over serial port) in plaintext Never exported	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only)	Authentication during SSH session negotiation
SSH Session Key (CSP)	128 and 256 bits	AES-CBC (Cert. A2544) AES-GCM (Cert. A2544) KTS (AES-GCM) (Cert. A2544) KTS (AES-CBC/HMAC) (Cert. A2544)	Derived internally via SSH KDF	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Encryption and decryption of SSH session packets Wrapping of keying material (when keys are part of the payload)
SSH Authentication Key (CSP)	Between 160 and 384 bits	HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544)	Derived internally via SSH KDF	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Authentication of SSH session packets Wrapping of keying material (when keys are part of the payload)

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[47]	Use & Related Keys
TLS Private Key (CSP)	Between 112 and 150 bits	RSA SigGen (FIPS186-4) (Cert. A2544)	Generated internally via Approved DRBG	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Imported by CO via CLI (over serial port) in plaintext form Never exported	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only); zeroization command	Authentication during TLS session negotiation
TLS Public Key (PSP)	Between 112 and 150 bits	RSA SigVer (FIPS186-4) (Cert. A2544)	Generated internally via Approved DRBG as part of CSR or self-signed certificate generation	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Never exported	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only)	Authentication during TLS session negotiation
TLS Session Key (CSP)	128 or 256 bits	AES-CBC (Cert. A2544) AES-CCM (Cert. A2544) AES-GCM (Cert. A2544) KTS (AES-CCM) (Cert. A2544) KTS (AES-GCM) (Cert. A2544) KTS (AES-CBC/HMAC) (Cert. A2544)	Derived internally using the TLS Master Secret via TLS KDF	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Encryption and decryption of TLS session packets Wrapping of keying material (when keys are part of the payload)
TLS Authentication Key (CSP)	Between 160 and 384 bits	HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544) KTS (AES-CBC/HMAC) (Cert. A2544)	Derived internally using the TLS Master Secret via TLS KDF	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Authentication of TLS session packets Wrapping of keying material (when keys are part of the payload)
SNMPv3 Privacy Key (CSP)	Between 128 and 256 bits	AES-CFB128 (Cert. A2544)	Derived internally using SNMP KDF	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Never exported	-	Plaintext form in virtual RAM	Soft reset/power cycle	Encryption and decryption of SNMPv3 session packets

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[47]	Use & Related Keys
SNMPv3 Authentication Key (CSP)	Between 160 and 384 bits	HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544)	Derived internally using SNMP KDF	Imported in PEM file format via Web Interface (over TLS) in encrypted form Imported in PEM file format via CLI (over SSH) in encrypted form Exported via TLS or SSH) in encrypted form	-	Plaintext form in virtual RAM	Soft reset/power cycle	Authentication of SNMPv3 session packets
SRTP Session Key (CSP)	128 or 256 bits	AES-CTR (Cert. A2544)	Derived internally using SRTP Master Key via the SRTP KDF	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Encryption and decryption of SRTP session packets
SRTP Authentication Key (CSP)	Between 160 and 384 bits	HMAC-SHA-1 (Cert. A2544) HMAC-SHA2-256 (Cert. A2544) HMAC-SHA2-384 (Cert. A2544)	Derived internally via SRTP KDF using SRTP Master Key	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Authentication of SRTP session packets
SFTP Private Key (CSP)	Between 112 and 150 bits	RSA SigGen (FIPS186-4) (Cert. A2544)	Generated internally via Approved DRBG	Never imported Never exported	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only); zeroization command	Authentication during SFTP session negotiation
SFTP Public Key (PSP)	Between 112 and 150 bits	RSA SigVer (FIPS186-4) (Cert. A2544)	Generated internally via Approved DRBG as part of CSR or self-signed certificate generation	Never imported Exported in plaintext form	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	Soft reset/power cycle (virtual RAM only)	Authentication during SFTP session negotiation
Image Verification Key (PSP)	128 bits	ECDSA SigVer (FIPS186-4) (Cert. A2544)	Hardcoded in the application binary	Never imported Never exported	-	Plaintext form in virtual RAM Plaintext form on virtual flash/disk	N/A	Verification of new software upgrade image
Other SSPs								
SSH Shared Secret (CSP)	Between 112 and 256 bits	KDF SSH (Cert. A2389)	Computed internally by KAS-ECC-SSC / KAS-FFC-SSC	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Input to SSH KDF for derivation of the SSH Session Key and SSH Authentication Key
TLS Pre-Master Secret (CSP)	Between 112 and 256 bits	TLS v1.2 KDF RFC 7627 (Cert. A2389) TLS v1.3 KDF (Cert. A2389)	[for KAS-ECC-SSC / KAS-FFC-SSC cipher suites] Computed internally by KAS-ECC-SSC and KAS-FFC-SSC	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Input to KAS-FFC-SSC and KAS-ECC-SSC for computation of the TLS Master Secret

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[47]	Use & Related Keys
TLS Master Secret (CSP)	384 bits	TLS v1.2 KDF RFC 7627 (Cert. A2389) TLS v1.3 KDF (Cert. A2389)	Derived internally using the TLS Pre-Master Secret via TLS KDF	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Input to TLS KDF for derivation of the TLS Session Key and TLS Authentication Key
SRTP Master Key (CSP)	128 and 256 bits	KDF SRTP (Cert. A2389)	[when module is calling side] Generated internally via Approved DRBG	[when module is calling side] Never imported; Exported via SIP/TLS in encrypted form [when module is answering side] Imported via SIP/TLS in encrypted form; Never exported	-	Plaintext form in virtual RAM	Soft reset/power cycle	Input to SRTP KDF for derivation of the SRTP Session Key and SRTP Authentication Key
Entropy Input String (CSP)	384 bits	CKG (Vendor Affirmed) SHA3-256 (Cert. A2390)	Generated internally	-	-	Plaintext form in virtual RAM	End of DRBG function, soft reset/power cycle	Random number generation
DRBG Seed (CSP)	384 bits	CKG (Vendor Affirmed) Counter DRBG (Cert. A2544)	Generated internally using entropy input string	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Random number generation
DRBG 'Key' Value (CSP)	256 bits	CKG (Vendor Affirmed) Counter DRBG (Cert. A2544)	Generated internally	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Random number generation
DRBG 'V' Value (CSP)	128 bits	CKG (Vendor Affirmed) Counter DRBG (Cert. A2544)	Generated internally	-	-	Plaintext form in virtual RAM	Soft reset/power cycle	Random number generation
SNMPv3 Authentication Password (CSP)	-	KDF SNMP (Cert. A2389)	-	Imported via Web Interface (over TLS) in encrypted form Imported via CLI (over SSH) in encrypted form Imported via CLI (over serial port) in plaintext form Imported in an INI file via Web Interface (over TLS) in encrypted form Imported in an INI file via CLI (over SSH) in encrypted form Exported in an INI file via TLS or SSH in encrypted form	-	Plaintext form in virtual RAM	Soft reset/power cycle (virtual RAM only) The CO entering an all-zero value using the Web Interface or CLI Importing a new .ini file with a zero-value SNMPv3 Authentication Password	Used to derive the SNMPv3 Authentication Key

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[47]	Use & Related Keys
SNMPv3 Privacy Password (CSP)	-	KDF SNMP (Cert. A2389)	-	Imported via Web Interface (over TLS) in encrypted form Imported via CLI (over SSH) in encrypted form Imported via CLI (over serial port) in plaintext form Imported in an INI file via Web Interface (over TLS) in encrypted form Imported in an INI file via CLI (over SSH) in encrypted form Exported in an INI file via TLS or SSH in encrypted form	-	Plaintext form in virtual RAM	Soft reset/power cycle (virtual RAM only) The CO entering an all-zero value using the Web Interface or CLI Importing a new .ini file with a zero-value SNMPv3 Privacy Password	Used to derive the SNMPv3 Privacy Key

AES GCM encryption is used in the context of several secure communications protocols. The module meets the (key/IV) pair uniqueness requirements from *NIST SP 800-38D* as follows:

- For TLS v1.2, the module supports acceptable AES GCM cipher suites from section 3.3.1.1 of *NIST SP 800-52rev2*.

  The mechanism for IV generation falls into scenario 1 in *FIPS 140-3 IG* C.H and is compliant with *RFC 5288*. The counter portion of the IV is strictly increasing. When the IV exhausts the maximum number of possible values for a given session key, a failure in encryption will occur and a handshake to establish a new encryption key will be required. It is the responsibility of the module operator (i.e., the first party, client, or server) to trigger this handshake in accordance with *RFC 5246* when this condition is encountered.

- For TLS v1.3, the module supports acceptable AES GCM cipher suites from section 3.3.1.2 of *NIST SP 800-52rev2*. The protocol's implementation is contained within the boundary of the module, and the generated IV is only used in the context of the AES GCM encryption executing the provisions of the TLS 1.3 protocol.

  The mechanism for IV generation falls into scenario 5 in *FIPS 140-3 IG* C.H and is compliant with *RFC 8446*. Each session employs a "per-record nonce", a 64-bit sequence number (or IV) maintained separately for reading and writing records. Each sequence number is set to 0 at the beginning of a connection and whenever the key is changed (the first record transmitted under a particular traffic key uses sequence number 0), and the appropriate sequence number is incremented by one after reading or writing each record. Because the size of sequence numbers is 64 bits, they should not wrap. If a sequence number needs to wrap, it is the responsibility of the module operator to either rekey or terminate the connection.

- For SSH v2, the mechanism for IV generation falls into scenario 1 in *FIPS 140-3 IG* C.H and is compliant with *RFC 5647*.

  A new IV parameter is generated by the module for each AES GCM encryption. The IV consists of a 4-byte fixed field and an 8-byte invocation counter. The fixed field of the IV remains the same for the duration of

the session, while the invocation counter is treated as a 64-bit integer and is incremented by one when performing an encryption of a new binary packet. If the invocation counter reaches its maximum value $2^{64} – 1$, the next encryption is performed with the invocation counter set to either 0 or 1. No more than $2^{64} – 1$ encryptions are performed in the same session. When a session is terminated for any reason, it is the responsibility of the module operator to derive a new key and a new initial IV.

The module also complies with the following RFCs:

- RFC 4252
- RFC 4253
- RFC5647

9.2 RGB Entropy Sources

Table 11 below specifies the module's entropy sources.

Table 11 – Non-Deterministic Random Number Generation Specification

Entropy Source(s)	Minimum Number of Bits of Entropy	Details
CPU Time Jitter Based Non-Physical TRNG	384 bits	The min-entropy (per 4 bits of data) of the test was 3.597905 bits. As long as there is at least one bit of entropy per four bits of raw noise data, the entropy provided by each call to CPU Jitter entropy can be considered to contain full entropy. When the DRBG requests 384 bits of entropy for seeding, the function is called four times and returns 384 bits of entropy, thus exceeding the FIPS requirement of at least 112 bits of entropy.

10. Self-Tests

Both pre-operational and conditional self-tests are performed by the module. Pre-operational tests are performed between the time a cryptographic module is powered on and before the module transitions to the operational state. Conditional self-tests are performed by the module during module operation when certain conditions exist. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

10.1 Pre-Operational Self-Tests

Pre-operational self-tests are executed automatically at module power-up without action from the module operator.

The module performs the following pre-operational self-test(s):

- Software Integrity Test on the module software image (using ECDSA P-256 with SHA2-256 digital signature verification)

10.2 Conditional Self-Tests

The module performs the following conditional self-tests:

- Conditional cryptographic algorithm self-tests (CASTs)
    - Crypto Library:
        - AES ECB encrypt KAT[48] (128-bit length)
        - AES ECB decrypt KAT (128-bit length)
        - AES CCM encrypt KAT (128-bit length)
        - AES CCM decrypt KAT (128-bit length)
        - AES GCM encrypt KAT (256-bit length)
        - AES GCM decrypt KAT (256-bit length)
        - CTR DRBG instantiate/generate/reseed KAT (AES, 256-bit, with derivation function)
        - ECDSA sign KAT (P-256 curve)
        - ECDSA verify KAT (P-256 curve)
        - HMAC KATs (SHA-1, SHA2-256, SHA2-384)
        - RSA sign KAT (2048-bit; SHA2-256; PKCS#1.5 scheme)
        - RSA verify KAT (2048-bit; SHA2-256; PKCS#1.5 scheme)
        - SHA-2 KATs (SHA2-224, SHA2-512)
        - SHA-3 KATs (SHA3-256)
        - FFC DH Shared Secret “Z” Computation KAT (2048-bit)
        - ECC CDH Shared Secret “Z” Computation KAT (P-256 curve)
    - Entropy Library:
        - SHA3-256 KAT

[48] KAT – Known Answer Test

        - Entropy “Stuck” Test
        - Entropy Repetition Count Test (performed over 1024 samples)
        - Entropy Adaptive Proportion Test (performed over 1024 samples)

    - KDF Library:
        - TLS v1.2 KDF KAT
        - TLS v1.3 KDF KAT
        - SSH KDF KAT

    To ensure all conditional CASTs are performed prior to the first operational use of the associated algorithm, all CASTs are performed during the module’s initial power-up sequence. The CASTs for algorithms used in the pre-operational software integrity test are performed prior to the integrity test itself; all other CASTs are executed immediately after the successful completion of the software integrity test.

- Conditional pair-wise consistency tests (PCTs)
    - ECDSA key generation PCT (upon generation of a key pair for ECDSA digital signature functions)
    - RSA sign/verify PCT (upon generation of a key pair for RSA digital signature functions)
    - DH key generation PCT (upon generation of a key pair for DH key agreement functions)
    - ECDH key generation PCT (upon generation of a key pair for ECDH key agreement functions)

- Conditional manual SSP entry test (upon direct entry of an SSP)

- Conditional software load test using ECDSA P-256 signature verification (upon loading of a new image)

10.3 Self-Test Failure Handling

Upon failure of a pre-operational self-test, conditional CAST, or conditional PCT , the module enters a “Fatal” error state, keys are zeroized, and the module is automatically reset, with reset reason of “FIPS Failure”. An error is written to syslog. All access to the cryptographic functionality and CSPs is disabled. All data outputs via data output interfaces are inhibited (with the exception of syslog status messages) and the management interfaces will not respond to any commands while the module is in this state. A successful reboot is needed to clear the error condition and return to a normal operational state.

Upon failure of the conditional image verification test, the module enters a “Soft Error” state and with error status logged in syslog and the load process aborted. The error state is then automatically cleared, and the module resumes normal operation.

11. Life-Cycle Assurance

The sections below describe how to ensure the module is operating in its validated configuration, including the following:

- Procedures for secure installation, initialization, startup, and operation of the module
- Maintenance requirements
- Administrator and non-Administrator guidance

Operating the module without following the guidance herein (including the use of undocumented services) will result in non-compliant behavior and is outside the scope of this Security Policy.

11.1 Secure Installation

The module is available as a file containing the virtual appliance image. The Crypto Officer is responsible for all initial setup activities, including configuring the virtual machine, installing the guest operating system, and installing the Mediant SBC application software. For detailed guidance regarding these activities, please see the *AudioCodes Installation Manual, Mediant Virtual Edition (VE) SBC.*

To setup the module, the CO must follow the instructions found under the document entry "Installing Mediant VE SBC on VMware vSphere ESXi" for the Virtual Edition.

Once the module is installed with network settings properly configured, the Crypto Officer must then enable Approved mode operation.

11.2 Initialization

The CO shall configure the module for Approved mode. operation This ensures that the system will use only Approved cryptographic algorithms and key strengths. To configure the module for operation in the Approved mode, the CO may use the CLI or the Web Interface. Please refer to the following documents for general information on the use of the module's management interfaces:

- *AudioCodes Reference Guide, Command-Line Interface for Media Gateways & SBCs, Version 7.6*
- *AudioCodes User's Manual, Mediant Software SBC, Virtual (VE), Cloud (CE), and Server (SE) Editions, Version 7.6*

To configure the module for operation in the Approved mode, the CO must perform the following actions:

- The CO must enable Approved mode. Using the CLI, the CO must issue the `FIPSmode enable` command. Using the Web Interface, the module's mode can be set on the **Security Settings** page (**Setup** menu -> **IP Network** tab -> **Security** folder -> **Security Settings)** and clicking the **<Enable FIPS>** button.

- General information for configuring TLS contexts (settings that define the TLS parameters used for management and other TLS applications) using the Web Interface is addressed in the "Configuring TLS Certificates" chapter of the *AudioCodes User's Manual*.

  For operation in the Approved mode, the CO shall open the TLS Contexts table on the **TLS Contexts** page (**Setup** menu -> **IP Network** tab -> **Security** folder > **TLS Contexts**) and ensure that the contexts are configured according to the following guidance:

  - For the "DH Key Size" parameter, the CO may select any supported size except 1024.

  - For "Cipher Server" and "Cipher Client" parameters (applicable to TLS versions 1.0 – 1.2), the CO shall ensure that only Approved ciphers are used by adding the following to the cipher string to the cipher string list:

    !RC4:!aNULL:!eNULL:!AECDH:!ADH:!CAMELLIA:!ARIA128:!SEED:!kRSA:!3DES

  - For "Cipher Server TLS1.3" and "Cipher Client TLS 1.3" parameters (applicable to TLS version 1.3), the CO shall ensure that only Approved ciphers are used by removing the following cipher string from the cipher string list:

    TLS_CHACHA20_POLY1305_SHA256

- General information for configuring SRTP is addressed in the "Configuring SRTP" chapter of each of the *AudioCodes User's Manual*. For operation in the Approved mode , the CO shall open the **Media Security** page (**Setup** menu -> **Signaling & Media** tab -> **Media** folder -> **Media Security**) and ensure that the settings are configured according to the following guidance:

  - For the "Media Security Behavior" parameter, the CO shall select "Mandatory" from the drop-down list.

  - For the "Aria Protocol Support" parameter, the CO shall ensure it is set to "Disable".

- For secure key transfer, the CO shall ensure that derived session keys are transferred to endpoints using TLS (i.e., force TLS). The CO shall click "New" or "Edit" on the **SIP Interfaces** table (**Setup** menu -> **Signaling & Media** tab -> **Core Entities** folder -> **SIP Interfaces**) and ensure that the settings on the UDP and TCP ports of each SIP interface are configured according to the following guidance:

  - For the "UDP Port" parameter, the CO shall enter "0".

  - For the "TCT Port" parameter, the CO shall enter "0".

- General information for configuring remote management is addressed in the ''Configuring Secured (HTTPS) Web'' chapter of the User's Manual. For securing RADIUS[49] connections for operation in the Approved mode, the CO shall open the **Web Settings** page (**Setup** menu -> **Administration** tab -> **Web & CLI** folder -> **Web Settings**) and ensure that the settings are configured according to the following guidance:

[49] RADIUS – Remote Authentication Dial In User Service

- For the "'Secured Web Connection (HTTPS)" parameter, the CO shall select "HTTPS Only" from the drop-down list.

Configuring the module into Approved mode will zeroize all persistent CSPs and reset the module.

11.3 Startup

No additional startup steps are required to be performed by end-users.

11.4 Administrator Guidance

The Crypto Officer is responsible for initialization and security-relevant configuration and management of the module.

Once installed, commissioned, and configured, the CO is responsible for maintaining the status of the module to ensure that it is running in its Approved mode. The Crypto Officer shall monitor the module's status regularly. If any irregular activity is noticed, or the module is consistently reporting errors, customers should contact AudioCodes Customer Support. Please refer to section 11 for guidance that the Crypto Officer must follow for the module to be considered running in an Approved mode of operation.

11.4.1 Default Login Password

The module provides a default login password for first-time module access for the CO only. The CO is required to change the default login password as part of the initial configuration.

11.4.2 On-Demand Self-Tests

The pre-operational self-tests are automatically performed at power-up. The CO may initiate the pre-operational self-tests by issuing the reset command over the module's management interfaces or power-cycling the host server or VM.

Using the CLI, resetting the module is accomplished by issuing the `reload now` command. Using the Web interface, resetting the module is accomplished from the **Maintenance Actions** page (**Setup** menu -> **Administration** tab -> **Maintenance** folder -> **Maintenance Actions**) and clicking the **<Reset>** button on the toolbar.

11.4.3 Zeroization

There are many CSPs within the module's cryptographic boundary including symmetric keys, private keys, public keys, and login password hashes. CSPs reside in virtual RAM, as well as on virtual storage media within the VM. All ephemeral keys used by the module are zeroized on reset and power cycle. Private keys and CSPs on the virtual machine's flash and hard disk can be zeroized by using a CLI command. The public key used for the image verification test is stored in the virtual machine's flash and hard disk and cannot be zeroized.

Using the CLI, keys and CSPs are zeroized using the `clear security-files` command. Successful return from this command indicates the completion of the zeroization process.

The SNMPv3 Authentication Password and SNMPv3 Privacy Password may be zeroized by the CO entering an all-zero value using the Web Interface or CLI or importing a new .ini file with a zero value. Both methods will overwrite and zeroize these CSPs. Completion of the manual entry process or of the .ini file load process indicates the completion of the zeroization process.

11.4.4 Status and Versioning Information

On the first power up, the module is, by default, in an unconfigured operational state. During initial configuration and setup, the module is explicitly set to operate in the Approved mode of operation. Authorized operators can access the module via the CLI and determine the mode of the module.

- Using the CLI, the mode status can be viewed by issuing the `show system security status` command. When the module is properly configured per this Security Policy, the command will return the following message:

```
FIPS mode: Enabled
```

- Using the Web Interface, the module's operational status can also be viewed on the **Security Settings** page (**Setup** menu -> **IP Network** tab -> **Security** folder -> **Security Settings**).

Module operators can also access the module's versioning information and correlate it to the versioning information shown on the module's FIPS validation certificate.

- Using the CLI, the module version can be viewed by issuing the `show system version` command.

- Using the Web Interface, the version information can be viewed on the **Device Information** page (**Monitor** menu -> **Monitor** tab -> **Summary** folder -> **Device Information**).

When executing on an on-prem virtual environment, the module name will be reported as "Mediant Virtual Edition". When executing in a cloud-based environment, the module name will be reported as "Mediant Cloud Edition".

11.4.5 Additional Administrator Guidance

The list below provides additional guidance for module administrators:

- The CO shall re-instantiate the module if the module has encountered a fatal error and becomes non-operational. If power-cycling the module does not correct the error condition, the module is considered to be compromised or malfunctioned and should be sent back to AudioCodes for repair or replacement.

- The module allows for the loading of new software and employs a digital signature verification technique to test its integrity. All SSPs must be zeroized prior to the loading and subsequent execution of new software via the following CLI command:

```
write factory clear-keys-and-certs
```

This can also be accomplished via the Software Upgrade wizard. When using the wizard, ensure that the "Use existing configuration" checkbox on the **Load *ini* file** wizard page is cleared and do not select a file to load. This will restore the module configuration back to factory default settings.

- To maintain an Approved mode of operation, the CO must ensure that only FIPS-validated software is loaded. Any operation of the module after loading non-validated software constitutes a departure from this Security Policy.

11.5 Non-Administrator Guidance

The User does not have the ability to configure sensitive information on the module, with the exception of their password. The User must be diligent to pick strong passwords and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret or private keys in their possession.

The following list provides additional policies below that must be followed by module operators:

- In the event that the module's power is lost and then restored, a new key for use with the AES GCM encryption shall be established.

- In order to comply with the key entry requirements described in section 9.5.A of the *Implementation Guidance for FIPS PUB 140-3 and the CMVP*, entry of plaintext private keys and CSPs using the CLI via the serial port must be accomplished using a non-networked general-purpose computing device.

- The module implements the KAS-FFC-SSC and KAS-ECC-SSC key agreement schemes specified in *NIST SP 800-56Arev3*. This specification requires that certain checks are performed to provide assurance regarding the keys being used. The following assurance checks are performed by the cryptographic module:

    - Assurances of domain parameter validity (section 5.5.2 of *NIST SP 800-56Arev3*)
    - Assurances required by the key pair owner (section 5.6.2.1 of *NIST SP 800-56Arev3*)
    - Assurances required by the public key recipient (section 5.6.2.2 of *NIST SP 800-56Arev3*)

12. Mitigation of Other Attacks

The module does not claim to mitigate any attacks beyond the FIPS 140-3 Level 1 requirements for this validation. Therefore, per *ISO/IEC 19790:2021* section 7.12, requirements for this section are not applicable.

Appendix A. Acronyms and Abbreviations

Table 12 provides definitions for the acronyms and abbreviations used in this document.

Table 12 – Acronyms and Abbreviations

Term	Definition
AC	Alternating Current
ACL	Access Control List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
B2BUA	Back-to-Back User Agent
CA	Certificate Authority
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CSR	Certificate Signing Request
CTR	Counter
CVL	Component Validation List
DC	Direct Current
DDOS	Distributed Denial-of-Service
DES	Data Encryption Standard
DOS	Denial-of-Service
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DSP	Digital Signal Processing
DTLS	Datagram Transport Layer Security
EC	Elliptical Curve
ECC	Elliptical Curve Cryptography
ECC CDH	Elliptical Curve Cryptography Cofactor Diffie Hellman

Term	Definition
ECDSA	Elliptical Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FFC DH	Finite Field Cryptography Diffie-Hellman
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet
Gbps	Gigabits per second
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HA	High Availability
HDD	Hard Disk Drive
HMAC	(Keyed-) Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
ICE	Interactive Connectivity Establishment
IEEE	Institute of Electrical and Electronics Engineers
iLO	Integrated Lights Out
IP	Internet Protocol
IV	Initialization Vector
KAS	Key Agreement Scheme
KAS ECC SSC	Key Agreement Scheme - Elliptical Curve Cryptography - Shared Secret Computation
KAS FFC SSC	Key Agreement Scheme - Finite Field Cryptography - Shared Secret Computation
KAT	Known Answer Test
KDF	Key Derivation Function
LED	Light Emitting Diode
MAC	Message Authentication Code
Mbps	Megabits per second
MOS	Mean Opinion Score
N/A	Not Applicable
NAT	Network Address Translation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OAMP	Operations, Administration, Maintenance, and Provisioning
OS	Operating System
PBKDF2	Password-Based Key Derivation Function 2
PBX	Private Branch Exchange

Term	Definition
PEM	Privacy Enhanced Mail
PKCS	Public-Key Cryptography Standards
PUB	Publication
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SAS	Serial Attached Small Computer System Interface
SBC	Session Border Controller
SDES	Session Description Protocol Security Descriptions
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Small Form-Factor Pluggable
SFTP	SSH (or Secure) File Transfer Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SRTP	Secure Real-Time Transport Protocol
SSD	Solid State Drive
SSH	Secure Shell
TCP	Transport Control Protocol
TDM	Time-Division Multiplexing
TLS	Transport Layer Security
U	Rack Unit
UDP	User Datagram Protocol
U.S.	United States
USB	Universal Serial Bus
VGA	Video Graphics Array
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com