

AudioCodes Ltd.

Mediant Session Border Controllers

Hardware Models: Mediant 4000 SBC and Mediant 9080 SBC

Firmware Version: 7.4

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1

Document Version: 1.1

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.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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

Table of Contents

1. Introduction	4
1.1 Purpose	4
1.2 References	4
1.3 Document Organization	4
2. Mediant Session Border Controllers	5
2.1 Overview	5
2.2 Module Specification	8
2.3 Module Ports and Interfaces	12
2.4 Roles and Services	18
2.4.1 Authorized Roles	18
2.4.2 Operator Services	19
2.4.3 Additional Services	22
2.5 Operational Environment	23
2.6 Cryptographic Key Management	23
2.7 EMI / EMC	34
2.8 Self-Tests	34
2.8.1 Power-Up Self-Tests	34
2.8.2 Conditional Self-Tests	35
2.8.3 Critical Functions Self-Tests	35
2.8.4 Self-Test Failure Handling	35
2.9 Mitigation of Other Attacks	36
3. Secure Operation	37
3.1 Installation and Setup	37
3.1.1 Initial Setup	37
3.1.2 FIPS-Approved Mode Configuration	37
3.2 Crypto Officer Guidance	38
3.2.1 Management	38
3.2.2 Default Password	38
3.2.3 On-Demand Self-Tests	38
3.2.4 Zeroization	39
3.3 User Guidance	39
3.4 Additional Guidance and Usage Policies	39
3.5 Non-Approved Mode of Operation	40
4. Acronyms	41

List of Tables

Table 1 – Security Level per FIPS 140-2 Section	7
Table 2 – Cryptographic Algorithm Providers	9
Table 3 – FIPS-Approved Algorithm Implementations	10
Table 4 – FIPS-Approved Key Derivation Functions	12
Table 5 – Allowed Algorithms.....	12
Table 6 – FIPS 140-2 Logical Interface Mappings for the Mediant 4000 SBC.....	13
Table 7 – FIPS 140-2 Logical Interface Mappings for the Mediant 9080 SBC.....	16
Table 8 – Authorized Operator Services.....	19
Table 9 – Additional Services.....	22
Table 10 – Cryptographic Keys, Cryptographic Key Components, and CSPs.....	24
Table 11 – Acronyms	41

List of Figures

Figure 1 – Mediant 4000 SBC	5
Figure 2 – Mediant 9080 SBC	6

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Mediant Session Border Controllers from AudioCodes Ltd. (AudioCodes). This Security Policy describes how the Mediant Session Border Controllers meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.¹ and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the U.S. National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at <https://csrc.nist.gov/projects/cryptographic-module-validation-program>.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Mediant Session Border Controllers are referred to in this document as the SBC, SBCs, module, or modules. The Mediant Session Border Controllers are also referred to individually as the Mediant 4000 and the Mediant 9080.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 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.

1.3 Document Organization

The Security Policy document is organized into two primary sections. Section 2 provides an overview of the validated module. This includes a general description of the module's capabilities and its use of cryptography as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions, management methods, and applicable usage policies.

¹ U.S. – United States

2. Mediant Session Border Controllers

2.1 Overview

AudioCodes Ltd. (hereafter referred to as AudioCodes) is a leading vendor of advanced networking and media processing solutions for the digital workplace. The AudioCodes Mediant family of Session Border Controllers (SBCs) offers a line of versatile IP² communications platforms that connect VoIP³ and TDM⁴ 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 SIP⁵ trunk and hosted telephony services.

The Mediant Session Border Controllers form 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. They can function as a peering SBC, access SBC, or enterprise SBC.

- The Mediant 4000 SBC (see Figure 1) is a mid-to-high scale capacity SBC designed for deployment in large organizations and as an access SBC for service providers. It supports up to 5000 SBC sessions.
- The Mediant 9080 SBC (see Figure 2) is a high-capacity SBC designed for deployment in large enterprise and contact center locations, and as access and peering SBCs for service provider environments. It supports up to 70,000 SBC sessions.



Figure 1 – Mediant 4000 SBC

² IP – Internet Protocol

³ VoIP – Voice Over Internet Protocol

⁴ TDM – Time-Division Multiplexing

⁵ SIP – Session Initiation Protocol



Figure 2 – Mediant 9080 SBC

The SBCs are 1U⁶ IP encryption appliances with proven performance, resiliency, and security featuring real-time encryption (VoIP signaling and media traffic), DSP⁷-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 B2BUA⁸
- SIP Interworking
- Extensive PBX⁹ interoperability
- Transport Mediation between SIP over UDP¹⁰/TCP¹¹/TLS¹²/WebSocket, IPv4/IPv6, RTP¹³/SRTP¹⁴ SDES¹⁵/DTLS¹⁶
- Header Manipulation
- Local and far-end NAT¹⁷ traversal
- Integrated WebRTC gateway with support for WebSocket, Opus, VP8¹⁸ video coder, lite ICE¹⁹, DTLS, RTP multiplexing, and secure RTCP²⁰ with feedback
- Denial of service protection with DoS²¹/DDoS²² line rate protection,
- VOIP firewall and deep packet inspections with rogue RTP detection and prevention
- Encryption and authentication with support for TLS, DTLS, SRTP, HTTPS²³, SSH²⁴, SFTP²⁵, and SNMP²⁶
- Topology hiding and user privacy

⁶ U – Rack Unit

⁷ DSP – Digital Signal Processing

⁸ B2BUA – Back-to-Back User Agent

⁹ PBX – Private Branch Exchange

¹⁰ UDP – User Datagram Protocol

¹¹ TCP – Transport Control Protocol

¹² TLS – Transport Layer Security

¹³ RTP – Real-time Transport Protocol

¹⁴ SRTP – Secure Real-time Transport Protocol

¹⁵ SDES – Session Description Protocol Security Descriptions

¹⁶ DTLS – Datagram Transport Layer Security

¹⁷ NAT – Network Address Translation

¹⁸ VP8 – Video coding format developed by Google

¹⁹ ICE – Interactive Connectivity Establishment

²⁰ RTCP – Real-Time Transport Control Protocol

²¹ DoS – Denial of Service

²² DoS/DDoS – Denial-of-Service/Distributed Denial-of-Service

²³ HTTPS – Hypertext Transfer Protocol Secure

²⁴ SSH – Secure Shell

²⁵ SFTP – SSH (or Secure) File Transfer Protocol

²⁶ SNMP – Simple Network Management Protocol

- Traffic separation with VLAN²⁷/physical interface separation for multiple media, control and OAMP²⁸ interfaces
- Call Admission Control
- Full Quality of Experience (QoE) monitoring: Jitter, Packet Loss, Delay and MOS²⁹

Management of the SBCs 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 (Mediant 9080 SBC only)
- 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 Mediant 4000 SBC and Mediant 9080 SBC.

The Mediant Session Border Controllers are validated at the FIPS 140-2 section levels shown in Table 1 below.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A ³⁰
7	Cryptographic Key Management	1

²⁷ VLAN – Virtual Local Area Network

²⁸ OAMP – Operations, Administration, Maintenance, and Provisioning

²⁹ MOS – Mean Opinion Score

³⁰ N/A – Not applicable

Section	Section Title	Level
8	EMI/EMC ³¹	1
9	Self-tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The SBC is a hardware cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The cryptographic boundary is defined by the physical enclosure of the SBC and includes all internal hardware as well as the SBC 7.4 firmware.

The main hardware components consist of integrated circuits, processors, memories, SSD³², SAS³³ HDD³⁴, flash, DSP cards, power supplies, fans, and the enclosure containing all of these components.

Figure 3 below depicts the logical diagram of the Mediant SBC firmware. The following undefined acronyms appear in Figure 3:

- CPU – Central Processing Unit
- LED – Light Emitting Diode
- NIC – Network Interface Card
- USB – Universal Serial Bus

³¹ EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

³² SSD – Solid State Drive

³³ SAS – Serial Attached Small Computer System Interface

³⁴ HDD – Hard Disk Drive

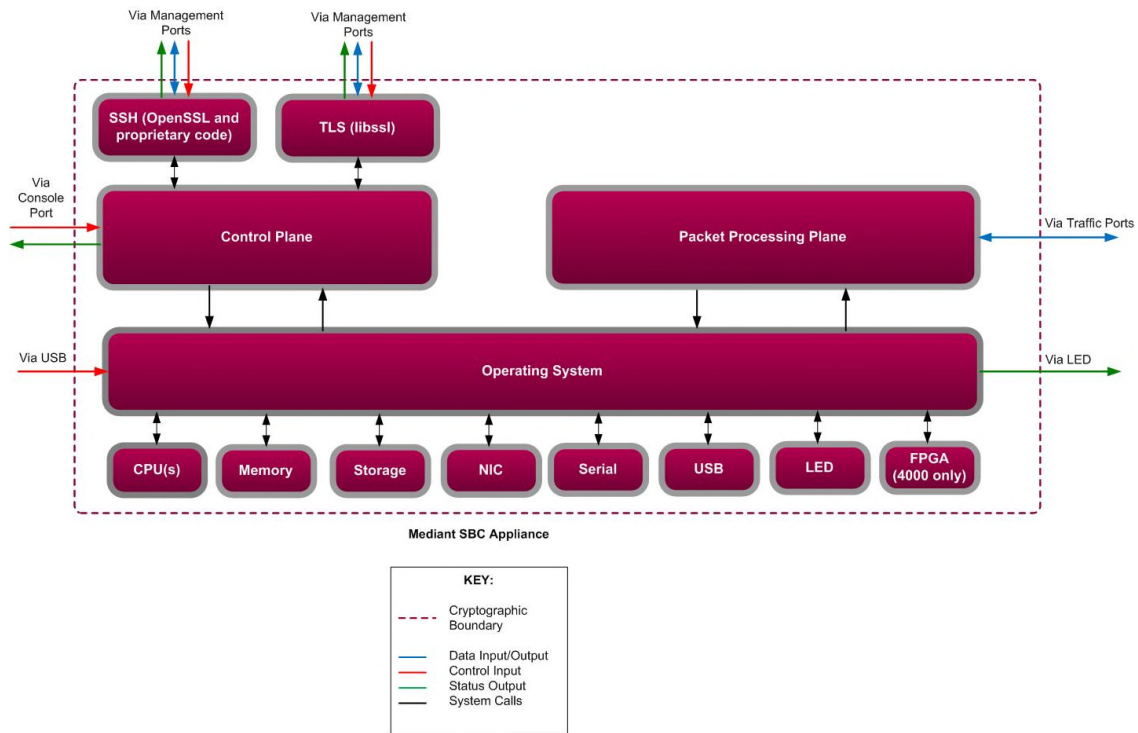


Figure 3 – Mediant 4000 SBC and Mediant 9080 SBC Logical Block Diagram

The module includes the cryptographic algorithm providers listed in Table 2 below.

Table 2 – Cryptographic Algorithm Providers

Implementation Name	Version	Module Model		Use
		4000	9080	
AudioCodes Mediant SBC Cryptographic Library	1.0	#C941	#C941	Firmware-based cryptographic primitives (based on OpenSSL 1.1.1)
AudioCodes Mediant SBC Cryptographic Accelerator Module	1.0	#C940	-	Hardware-accelerated implementations of cryptographic primitives
AudioCodes Mediant SBC KDF ³⁵	1.0	#C974	-	KDF implementations for SNMP, SRTP, and TLS
AudioCodes Mediant SBC Cryptographic Accelerator KDF	1.0	#C1006	-	Hardware-accelerated implementations of SNMPv3, SRTP, SSHv2, and TLS KDFs
AudioCodes Mediant SBC KDF	1.0	-	#C973	KDF implementations for SNMP, SRTP, SSH, and TLS

The module implements the FIPS-Approved algorithms listed in Table 3 below.

³⁵ KDF – Key Derivation Function

Table 3 – FIPS-Approved Algorithm Implementations

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use	
Crypto Library (4000/9080)	Crypto Accelerator (4000)						
-	#C940	AES ³⁶	FIPS PUB ³⁷ 197	CBC ³⁸ , CTR ³⁹	128, 256	Encryption/decryption	
				CFB128 ⁴⁰	128, 192, 256	Encryption/decryption	
				ECB ⁴¹	128	Encryption/decryption <i>ECB mode is used in self-test only</i>	
#C941	-	AES	FIPS PUB 197	CBC, CTR	128, 256	Encryption/decryption	
				CFB128	128, 192, 256	Encryption/decryption	
				ECB	128	Encryption/decryption <i>ECB mode is used in self-test only</i>	
				NIST SP ⁴² 800-38C	CCM ⁴³	128, 256	Encryption/decryption
				NIST SP 800-38D	GCM ⁴⁴	128, 256	Encryption/decryption
Vendor Affirmed	-	CKG ⁴⁵	NIST SP 800-133	-	-	Symmetric key generation <i>Symmetric keys and generated seeds are produced using unmodified output from the Approved DRBG.</i>	
#C941	-	CVL ⁴⁶	NIST SP 800-56Arev2	ECC CDH ⁴⁷ Primitive	P-224, P-256, P-384, P-521	Shared secret computation <i>P-224 curve used in self-test only.</i>	
#C941	-	DRBG ⁴⁸	NIST SP 800-90Arev1	CTR-based	256	Deterministic random bit generation	
#C941	-	ECDSA ⁴⁹	FIPS PUB 186-4	PKG	P-224, P-256, P-384, P-521	Key pair generation	
#C941	-	HMAC ⁵⁰	FIPS PUB 198-1	SHA-1 ⁵¹ , SHA-256, SHA-384	-	Message authentication <i>The module also supports HMAC SHA-1-32 and HMAC SHA-1-80.</i>	

³⁶ AES – Advance Encryption Standard

³⁷ PUB – Publication

³⁸ CBC – Cipher Block Chaining

³⁹ CTR – Counter

⁴⁰ CFB – Cipher Feedback

⁴¹ ECB – Electronic Codebook

⁴² SP – Special Publication

⁴³ CCM – Cipher Block Chaining - Message Authentication Code

⁴⁴ GCM – Galois Counter Mode

⁴⁵ CKG – Cryptographic Key Generation

⁴⁶ CVL – Component Validation List

⁴⁷ ECC CDH – Elliptic Curve Cryptographic Cofactor Diffie Hellman

⁴⁸ DRBG – Deterministic Random Bit Generator

⁴⁹ ECDSA – Elliptic Curve Digital Signature Algorithm

⁵⁰ HMAC – (keyed-) Hashed Message Authentication Code

⁵¹ SHA – Secure Hash Algorithm

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
Crypto Library (4000/9080)	Crypto Accelerator (4000)					
#C941	-	KTS	NIST SP 800-38F	AES (unauthenticated mode) with HMAC	[AES] 128, 192, 256	Key transport (TLS, SSH, SRTP, SNMP) <i>Key establishment methodology provides between 128 and 256 bits of encryption strength</i>
				AES (authenticated mode)	[AES] 128, 192, 256	Key transport (TLS) <i>Key establishment methodology provides between 128 and 256 bits of encryption strength.</i>
				Triple-DES (unauthenticated mode) with HMAC	[Triple-DES] 168	Key transport (TLS, SNMP) <i>Key establishment methodology provides 112 bits of encryption strength</i>
-	#C940	RSA	FIPS PUB 186-4	SigGenPKCS1.5 ⁵²	2048, 3072, 4096	Digital signature generation
				SigVerPKCS1.5	1024, 2048, 3072	Digital signature verification
#C941	-	RSA	FIPS PUB 186-4	KeyGen	2048, 3072	Key pair generation
				SigGenPKCS1.5	2048, 3072, 4096	Digital signature generation
				SigVerPKCS1.5	1024, 2048, 3072	Digital signature verification
-	#C940	SHS ⁵³	FIPS PUB 180-4	SHA-1, SHA-256	-	Message digest
#C941	-	SHS	FIPS PUB 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	-	Message digest <i>The module implements SHA-224, but does not use it operationally.</i>
-	#C940	Triple-DES ⁵⁴	NIST SP 800-67rev2	TCBC	Keying option 1	Encryption/decryption
#C941	-	Triple-DES	NIST SP 800-67rev2	TCBC	Keying option 1	Encryption/decryption

The vendor affirms the following cryptographic security methods:

- As per *NIST SP 800-133*, the module uses its FIPS-Approved counter-based DRBG to generate cryptographic keys. The resulting symmetric key or generated seed is an unmodified output from the DRBG. The module’s DRBG is seeded via `/dev/random`, a non-deterministic random number generator (NDRNG) internal to the module.

The module implements the Approved key derivation functions listed in Table 4 above.

⁵² PKCS – Public Key Cryptography Standard
⁵³ SHS – Secure Hash Standard
⁵⁴ DES – Data Encryption Standard

Table 4 – FIPS-Approved Key Derivation Functions

Certificate Number			Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
KDF (4000)	KDF (9080)	KDF Accelerator (4000)					
#C974	-	-	CVL	NIST SP 800-135rev1	SNMPv3, SRTP, TLSv1.0/1.1/1.2	-	Key derivation
-	#C973	-	CVL	NIST SP 800-135rev1	SNMPv3, SRTP, SSHv2, TLSv1.0/1.1/1.2	-	Key derivation
-	-	#C1006	CVL	NIST SP 800-135rev1	SNMPv3, SRTP, SSHv2, TLSv1.0/1.1/1.2	-	Key derivation

**No parts of the SNMP, SRTP, SSH, and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.*

The module implements the non-Approved but allowed algorithms shown in Table 5.

Table 5 – Allowed Algorithms

Algorithm	Caveat	Use
Diffie-Hellman	Key establishment methodology provides 112 bits of encryption strength	Key agreement
Elliptic Curve Diffie-Hellman (ECDH) #C941 , #C973 , #C974 , #C1006	Key establishment methodology provides between 128 and 256 bits of encryption strength	Key agreement
MD5 ⁵⁵	-	TLS protocol handshake Hashed operator passwords for validation by RADIUS server
NDRNG ⁵⁶	-	Seeding for the FIPS-Approved SP 800-90A CTR_DRBG
RSA	Key establishment methodology provides between 112 and 150 bits of encryption strength	Key transport
SHA-1	Legacy-use	RSA signature verification

2.3 Module Ports and Interfaces

The module’s design separates the physical ports and interfaces into four logically distinct and isolated categories. They are:

- Data Input Interface
- Data Output Interface

⁵⁵ MD5 – Message Digest 5

⁵⁶ NDRNG – Non Deterministic Random Number Generator

- Control Input Interface
- Status Output Interface

The Mediant 4000 SBC contains the physical ports and interfaces shown in Figure 4 and Figure 5

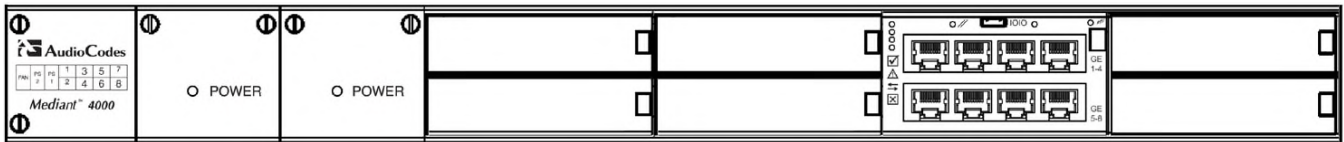


Figure 4 – Mediant 4000 SBC SBC Ports and Interfaces (Front)

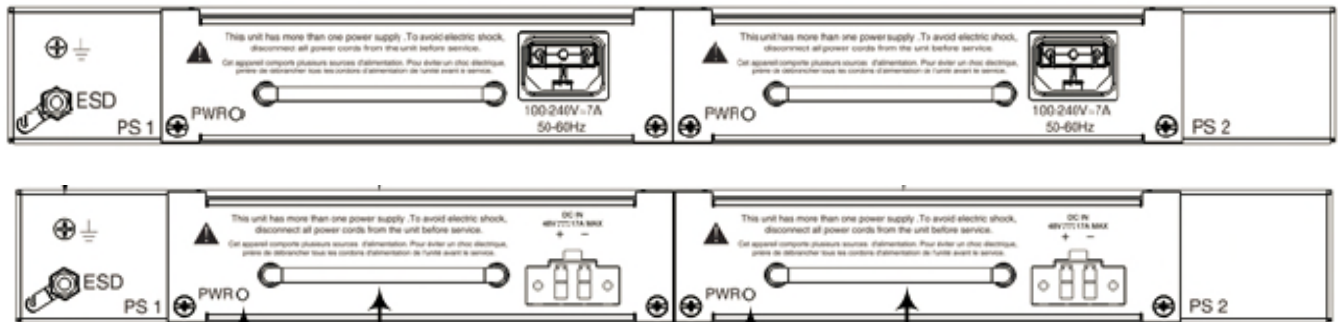


Figure 5 – Mediant 4000 SBC Ports and Interfaces (Rear)

The Mediant 9080 SBC contains the physical ports and interfaces shown in Figure 6 and Figure 7.

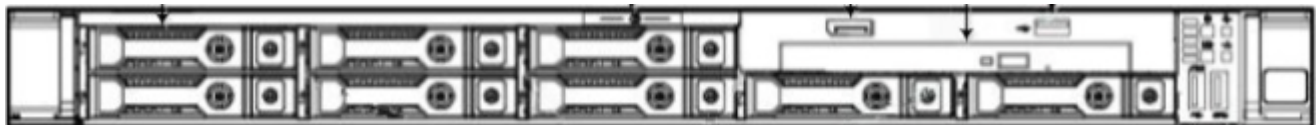


Figure 6 – Mediant 9080 SBC Ports and Interfaces (Front)

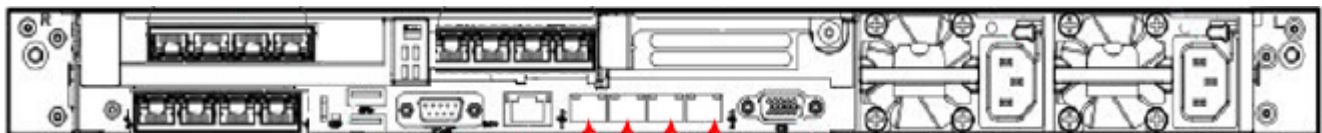





Figure 7 – Mediant 9080 SBC Ports and Interfaces (Rear)

Table 6 provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2 for the Mediant 4000.

Table 6 – FIPS 140-2 Logical Interface Mappings for the Mediant 4000 SBC

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Front Panel			
CPU Module LEDs			
<input checked="" type="checkbox"/> Module Service LED	1	Module Service indicator: <ul style="list-style-type: none"> • Solid green = Module in service • Off = Module out of service 	Status Output
 Module Fault LED	1	Module Fault indicator: <ul style="list-style-type: none"> • Solid green = Normal operation • Red = Booting up phase / fault detected in module • Off = During booting up state 	Status Output
 Module HA State LED	1	Module HA State indicator: <ul style="list-style-type: none"> • Solid green = Application running in Standalone state • Flashing green = Application running in HA Active state • Off = During booting up state • Solid yellow = Application is starting Boot / synchronizing • Flashing yellow = Application is running in HA Redundant state 	Status Output
<input checked="" type="checkbox"/> Module Operational State LED	1	Module Operational State indicator: <ul style="list-style-type: none"> • Solid red = Out of service • Off = Normal operation 	Status Output
Left Ethernet Port LED	1	Module Left Ethernet Port indicator: <ul style="list-style-type: none"> • Solid green = Ethernet link established • Flashing green = Data is being received or transmitted (activity) on the Ethernet port • Off = No Ethernet link 	Status Output
Right Ethernet Port LED	1	Module Right Ethernet Port indicator: <ul style="list-style-type: none"> • Solid orange = 100Base-T (Gigabit) Ethernet link established • Off = No Ethernet link or 100Base-Tx link established 	Status Output
 Module Hot-Swap AMC LED	1	Module Hot-Swap AMC indicator: <ul style="list-style-type: none"> • Solid blue = Blue hot-swap LED indicating that the AMC module can be fully removed or inserted • Off = Module insertion process is complete 	Status Output
Fan Tray Module LEDs			

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Fan Tray Module LED	2 (one for each of two Fan Tray Modules)	Module Fan Tray indicator: <ul style="list-style-type: none"> • Green = Fan Tray module and corresponding Power Supply module are operating normally • Red = Indicates one or both of the following: <ul style="list-style-type: none"> ○ Fan Tray Module failure ○ Power failure due to any of the following: <ul style="list-style-type: none"> ▪ Failure in corresponding Power Supply Module ▪ Failure in power source (e.g., disconnected power cord) ▪ Corresponding Power Supply Module not installed in the chassis • Off = Indicates one or both of the following: <ul style="list-style-type: none"> ○ No power received by the chassis. This indicates a problem related to both Power Supply Modules. This could be due to a failure in both Power Supply Modules or a failure in the power source (e.g., disconnected power cords) to which the modules are connected. ○ Fan Tray Module not receiving power due to a failure in the module or module not inserted correctly. 	Status output
Media Processing Module LEDs			
Module Service LED	1	Module Service indicator: <ul style="list-style-type: none"> • Solid green = Module in service • Off = Module out of service 	Status output
Module Operational LED	1	Module Operational indicator: <ul style="list-style-type: none"> • Solid green = Normal operation • Red = Booting up phase 	Status output
Module Application State LED	1	Module Application State indicator: <ul style="list-style-type: none"> • Solid green = Application running • Off = During booting up state • Solid yellow = Application is starting boot up 	Status Output
Module Service LED	1	Module Service indicator: <ul style="list-style-type: none"> • Solid red = Out of service • Off = Normal operation 	Status Output
CPU Module Ports and Buttons			
Ethernet Ports (1000Base-T GbE)	8	Data ports for management, media and signaling traffic, or HA configuration	Management: Control Input, Status Output, Data Input, Data Output Media and Signaling traffic: Data Input, Data Output HA configuration: Data Input, Data Output, Control Input, Status Output

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
RS-232 Serial Port (Micro-USB)	1	Used to access the CLI for serial communication	Data Input, Data Output, Control Input, Status Output
Reset Pinhole Button	1	Button used to reset the module	Control Input
Rear Panel			
Power Status LED	1	Module power supply indicator: <ul style="list-style-type: none"> • Solid green: power supply is operating correctly • Off = Failure / disruption in the power supply, or the power is currently not being supplied to the device through the power supply entry 	Status Output

Table 7 provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2 for the Mediant 9080.

Table 7 – FIPS 140-2 Logical Interface Mappings for the Mediant 9080 SBC

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Front Panel			
Power On/Standby Button/LED and System Power LED	1	Power status indicator: <ul style="list-style-type: none"> • Solid green = System on • Flashing green = Performing power on sequence • Solid amber = System in standby • Off = No power present 	Control Input Status Output
Health LED	1	Module health indicator: <ul style="list-style-type: none"> • Solid green = Normal • Flashing green = iLO is rebooting • Flashing amber = System degraded • Flashing red = System critical 	Status Output
NIC Status LED	1	Module NIC status indicator: <ul style="list-style-type: none"> • Solid green = Link to network • Flashing green = Network active • Off = No network activity 	Status Output
UID ⁵⁷ LED/Button	1	Module UID indicator: <ul style="list-style-type: none"> • Solid blue = activated • Flashing blue = Remote management or firmware upgrade in progress <ul style="list-style-type: none"> ○ 1 Hz = Remote management or firmware upgrade in progress ○ 4 Hz = iLO manual reboot sequence initiated ○ 8 Hz = iLO manual reboot sequence in progress • Off = deactivated 	Status Output

⁵⁷ UID – Unit Identification

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
USB 2.0 Port	1	Used to access the CLI via USB-enabled keyboard	Data Input, Control Input
USB 3.0 Port	1	Used to access the CLI via USB-enabled keyboard	Data Input, Control Input
Display Port	1	Analog video output port	Data Output, Status Output
iLO Service Port	1	Used for field service only	N/A
Rear Panel			
Slot 1: Quad 1-GbE copper ports	4	4 Quad 1 GbE for management or media and signaling traffic	Management: Control Input, Status Output, Data Input, Data Output Media and Signalling traffic: Data Input, Data Output
Slot 2: Quad 10-GbE SFP+ ports	4	4 Quad 10 GbE SFP+ for management or media and signaling traffic	Management: Control Input, Status Output, Data Input, Data Output Media and Signalling traffic: Data Input, Data Output
Slot 3	Unused	Unused slot	N/A
NIC Ports	Unused (dust covered)	Unused NIC ports	N/A
Video (VGA) Port	1	Analog video output port	Data Output, Status Output
iLO Management Port	1	Used for field service only	N/A
Serial Port	1	Used to access the CLI for serial communication	Data Input, Data Output Control Input, Status Output
USB 3.0 ports	2	Used to access the CLI via USB-enabled keyboard	Data Input, Control Input
1 GbE copper ports	1	Used for management or media and signaling traffic	Management: Control Input, Status Output, Data Input, Data Output Media and Signalling traffic: Data Input, Data Output
1 GbE copper ports	3	Used for media and signaling traffic	Data Input, Data Output

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
UID LED	1	Module UID indicator: <ul style="list-style-type: none"> • Solid blue = Identification is activated • Flashing blue = System is being managed remotely • Off = Identification is deactivated 	Status Output
iLO 5/Standard LED	1	Module iLO 5 indicator: <ul style="list-style-type: none"> • (Right LED) NIC activity status: <ul style="list-style-type: none"> ○ Solid green = Activity exists ○ Flashing green = Activity exists ○ Off = No activity exists • (Left LED) NIC link status: <ul style="list-style-type: none"> ○ Solid green = Link exists ○ Off = No link exists 	Status Output
Power Supply 1 LED	1	Module power supply indicator: <ul style="list-style-type: none"> • Solid green = Normal • Off = One or more of the following conditions exists: <ul style="list-style-type: none"> ○ AC power unavailable ○ Power supply failed ○ Power supply in standby mode ○ Power supply exceeded current limit 	Status Output
Power Supply 2 LED	1	Module power supply indicator: <ul style="list-style-type: none"> • Solid green = Normal • Off = One or more of the following conditions exists: <ul style="list-style-type: none"> ○ AC power unavailable ○ Power supply failed ○ Power supply in standby mode ○ Power supply exceeded current limit 	Status Output

2.4 Roles and Services

The sections below describe the module's roles and services.

2.4.1 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. Lastly, the CO is the only operator that can configure the module into the FIPS-Approved mode of operation. The CO also has access to all User services. The CO 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.

The CO and User roles are tied to administrative roles supported by the Mediant Session Border Controllers. 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. Each operator has their own account with a username and password which are used to authenticate to the module. Note that while the module supports authentication, since it is being certified at Level 1, no claims are being made with regards to compliance to the Level 2/3 role-based and identity-based authentication requirements.

2.4.2 Operator Services

Descriptions of the services available to the Crypto Officer role and User role are provided in the Table 8 below. The keys and CSPs listed in Table 8 indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 8 – Authorized Operator Services

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Commission the module	✓		Commission the module by following the Security Policy guidelines	None	None	None
Load License Key file	✓		Load a License Key file to change or upgrade features	Command	Status output	None
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	Command and parameter	Command response/ Status output	None
Configure VOIP network, media and SIP settings, and routing rules	✓		Configure IP network topology, media and SIP settings, and routing rules	Command and parameters	Command response/ Status output	None
Manage users	✓		Create, edit, or delete user accounts; assign passwords and roles; import SSH public key	Command and parameters	Command response/ Status output	Crypto Officer Password – R/W/X User Password – R/W/X SSH RSA Public Key – R/W/X
Manage user sessions	✓		Terminate specific user’s CLI session	Command and parameters	Command response/ Status output	SSH Session Key – W

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Change password	✓		Modify CO or User account passwords	Command and parameters	Command response/ Status output	Crypto Officer Password – R/W User Password – R/W
Change own password	✓	✓	Modify existing login passwords	Command and parameters	Command response/ Status output	Crypto Officer Password – R/W User Password – R/W
Manage Certificates/ Keypairs	✓		Generate RSA keypairs for certificate signing requests, generate RSA private keys, load certificates and private keys	Command and parameters	Command response/ Status output	RSA Private Key – R/W/X RSA Public Key – R/W/X Certificate Load Key – W/X CA ⁵⁸ Public Key – R/W TLS Peer Public Key – R/W SSH Peer Public Key – R/W
Configure TLS Contexts	✓		Define TLS version and ciphersuites for management and data TLS connections	Command and parameters	Command response/ Status output	None
Perform Self-Tests	✓		Perform on-demand self-tests	Command	Command response/ Status output	All ephemeral keys and CSPs – W
Show Status	✓	✓	Show the system status, Ethernet status, alarms, user activity logs, system identification and configuration settings of the module	Command	Command response/ Status output	None
Show system security status	✓	✓	Show the system security status: FIPS Approved mode	Command	Command response/ Status output	None
View Syslog	✓	✓	View event status messages in the syslog	Command	Command response/ Status output	None
Zeroize keys	✓		Zeroize keys and CSPs	Command	Command response/ Status output	All persistent private keys/CSPs – W
Upgrade firmware	✓		Load new firmware and perform an integrity test using an RSA digital signature	Command	Command response/ Status output	Firmware Load Authentication Key – R/X

⁵⁸ CA – Certificate Authority

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Load a .ini file and perform automatic updates	✓		Load the module's configuration as a .ini file and perform automatic updates	Command	Command response/ Status output	RSA Private Key – R/W RSA Public Key – R/W CA Public Key – R/W TLS Peer Public Key – R/W SSH Peer Public Key – R/W SSH Private Key – R/W SSH Public Key – R/W Radius Shared Secret – R/W SNMPv3 Authentication Password – R/W SNMPv3 Privacy Password – R/W Crypto Officer Password – R/W User Password – R/W
Save a .ini file of the module's configuration	✓		Save a .ini file of the module's configuration	Command	Command response/ Status output	Radius Shared Secret – R/W SSH Peer Public Key – R/W Crypto Officer Password – R/W User Password – R/W
Reset	✓		Reset the module	Command	Command response/ Status output	CSPs stored in RAM – W
Establish TLS session	✓	✓	Establish web session using TLS protocol	Command	Command response/ Status output	Diffie-Hellman Public Key – R/X Diffie-Hellman Private Key – X ECDH Public Component – R/X ECDH Private Component – X TLS Private Key – W/X TLS Public Key – W/X TLS Peer Public Key – R/X TLS Pre-Master Secret – W/X TLS Master Secret – W/X TLS Session Key – R/W/X TLS Authentication Key – W/X
Establish SSH session	✓	✓	Establish remote session using SSH protocol	Command	Command response/ Status output	Diffie-Hellman Public Key – R/X Diffie-Hellman Private Key – X ECDH Public Component – R/X ECDH Private Component – X SSH Private Key – W/X SSH Public Key – W/X SSH Peer Public Key – R/X SSH Shared Secret – W/X SSH Session Key – R/W/X SSH Authentication Key – W/X
Configure SNMPv3 users	✓		Configure SNMPv3 users	Command and parameters	Command response/ Status output	SNMPv3 Authentication Password – W SNMPv3 Privacy Password – W SNMPv3 Session Key – W/X SNMPv3 Authentication Key – W/X

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Perform SNMPv3 services	✓		Perform actions over SNMPv3	Command and parameters	Command response/ Status output	SNMPv3 Authentication Password – W SNMPv3 Privacy Password – W SNMPv3 Session Key – W/X SNMPv3 Authentication Key – W/X
Encrypt/Decrypt SNMP data	✓		Encrypt / decrypt SNMP data	Establish SNMP protocol session	SNMP session established	SNMPv3 Session Key – R/X SNMPv3 Privacy Password – R/X
Authenticate SNMP data	✓		Authenticate SNMP data	Establish SNMP protocol session	SNMP session established	SNMPv3 Authentication Key – R/X SNMPv3 Authentication Password – R/X

2.4.3 Additional Services

The module provides a limited number of services for which the operator is not required to assume an authorized role. Table 9 lists the services for which the operator is not required to assume an authorized role. None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

Table 9 – Additional Services

Service	Description	Input	Output	CSP and Type of Access
Zeroize	Zeroize keys and CSPs	Power cycling using power connectors, power button (Mediant 9080 SBC only) or reset pinhole button (Mediant 4000 SBC only)	Status output	All ephemeral keys and CSPs – W
Perform on-demand self-tests	Perform power-up self-tests on demand	Power cycling using power connectors, power button (Mediant 9080 SBC only) or reset pinhole button (Mediant 4000 SBC only)	Status output	All ephemeral keys and CSPs – W
Authenticate	Use to log into the module	Command	Status output	Crypto Officer Password – X User Password – X RADIUS Shared Secret – W/X TLS Public Key – X

2.5 Operational Environment

The module employs a non-modifiable operating environment. The SBC firmware is executed by the module's processor as indicated below:

- Mediant 4000 SBC (one Cavium OCTEON II series processor)
- Mediant 9080 SBC (two Intel Xeon Gold series processors)

This operational environment does not provide a general-purpose OS to the operator. The operational environment is not modifiable by the operator, and only the module's signed image can be executed. All firmware upgrades are digitally-signed, and a conditional self-test (RSA signature verification) is performed during each upgrade. If the signature test fails, the new firmware is ignored and the current firmware remains loaded.

NOTE: Only FIPS-validated firmware may be loaded to maintain the module's validation.

2.6 Cryptographic Key Management

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

- RSA private key file – plaintext base64 encoded PEM⁵⁹ format.
- X.509 certificate file with a public key matching the private key in the RSA private key file – plaintext base64 encoded PEM format
- 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 certificate 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 via the Web Interface, CLI, or Automated Update mechanism are indicated as such in Table 10.

The module supports the CSPs described in Table 10 below.

⁵⁹ PEM – Privacy Enhanced Mail

Table 10 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
CA Public Key	2048 or 3072 bit RSA key	Generated externally and imported in Base64 encoded (PEM) file format via Web Interface or CLI	Exported in Base64 encoded (PEM) file format via Web Interface or CLI	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only)	Verification of CA signatures
ECDH Private Component	Private component of ECDH protocol: P-256, P-384, P-521	Generated internally	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Establishment of TLS session keys
ECDH Public Component	Public component of ECDH protocol: P-256, P-384, P-521	[for the module] Generated internally [for a peer ⁶⁰] Generated externally and entered in plaintext	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in RAM	Soft reset/power cycle	Establishment of TLS session keys
Diffie-Hellman Private Key	256-bit DH key	Generated internally	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Generation of SSH/TLS shared secrets
Diffie-Hellman Public Key	2048-bit DH key	[for the module] Generated internally [for a peer] Generated externally and entered in plaintext	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in RAM	Soft reset/power cycle	Generation of SSH/TLS shared secrets

⁶⁰ Peer refers to either a SIP User Agent or the management workstation.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SSH Private Key	2048 or 3072-bit RSA key	Generated internally via FIPS-Approved DRBG OR Generated externally and imported in Base64 encoded (PEM) file format via Web Interface or CLI	Never exits the module	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only); zeroization command	Authentication during SSH session negotiation
SSH Public Key	2048 or 3072-bit RSA key	Generated internally via FIPS-Approved DRBG as part of CSR or self-signed certificate generation OR Generated externally and imported in textual PEM format via Web Interface or CLI (over SSH) OR Generated externally and imported in plaintext via CLI (over serial port)	Exits the module in plaintext form	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only)	Authentication during SSH session negotiation

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SSH Peer Public Key	1024 or 2048-bit RSA key	Generated externally and entered as hexadecimal digits via CLI OR Generated externally and imported in ciphertext in an INI file via Web Interface or CLI (over SSH)	Exported in an INI file via Web Interface or CLI	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only)	Client authentication 1024-bit key may be used for signature verification only
SSH Shared Secret	Shared secret 256-bits	Derived internally via DH shared secret computation	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Derivation of the SSH Session Key and SSH Authentication Key
SSH Session Key	AES-CTR 128-bit key	Derived internally via SSH KDF	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Encryption and decryption of SSH session packets
SSH Authentication Key	160-bit HMAC key or 256-bit HMAC key	Derived internally via SSH KDF	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Authentication of SSH session packets

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Private Key	2048 or 3072-bit RSA key	Generated internally via FIPS-Approved DRBG OR Generated externally and imported in Base64 encoded (PEM) file format via Web Interface or CLI OR Generated externally and entered by CO in plaintext via CLI (over serial port)	Never exits the module	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only); zeroization command	Authentication and possible key exchange during TLS key negotiation
TLS Public Key	2048 or 3072-bit RSA key	Generated internally via FIPS-Approved DRBG as part of CSR or self-signed certificate generation OR Generated externally and imported in textual PEM format via Web Interface or CLI	Exits the module via digital certificate in plaintext form	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only)	Authentication during TLS key negotiation
TLS Peer Public Key	2048 or 3072-bit RSA key	Generated externally and input via incoming TLS handshake	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Certificate-based authentication during TLS key negotiation

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Pre-Master Secret	[for RSA cipher suites] 384-bit random value [for DH/ECDH cipher suites] 256, 384, or 528-bit DH/ECDH shared secret)	[for RSA cipher suites and module acting as client] Generated internally via FIPS-Approved DRBG [for RSA cipher suites and module acting as server] Generated externally and imported in encrypted form via RSA key transport [for DH/ECDH cipher suites] Derived internally via DH/ECDH shared secret computation	[for RSA cipher suites and module acting as client] Exits the module in encrypted form via RSA key transport [for RSA cipher suites and module acting as server] Never exits the module [for DH/ECDH cipher suites] Never exits the module	Plaintext in RAM	Soft reset/power cycle	Derivation of the TLS Master Secret
TLS Master Secret	[for TLSv1.2] 256 or 384-bit shared secret [TLSv1.0/1.1] 160-bit shared secret	Derived internally using the TLS Pre-Master Secret via TLS KDF	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Derivation of the TLS Session Key and TLS Authentication Key
TLS Session Key	128 or 256-bit AES key or 168-bit Triple-DES key	Derived internally using the TLS Master Secret via TLS KDF	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Encryption and decryption of TLS session packets
TLS Authentication Key	160, 256, or 384-bit HMAC key	Derived internally using the TLS Master Secret via the TLS KDF	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Authentication of TLS session packets
SRTP Master Key	128 or 256-bit shared secret	[when module is placing a call] Generated internally via FIPS-Approved DRBG [when module is answering side] Generated externally by peer and imported in ciphertext via SIP/TLS	[when module is offering side] Exits in encrypted form via SIP/TLS [when module is answering side] Never exits the module	Plaintext in RAM	Soft reset/power cycle	Peer Authentication, Session and Authentication keys derivation for SRTP session

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SRTP Session Key	128 or 256-bit AES-CTR key	Derived internally using SRTP Master Key	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Encryption or decryption during SRTP session
SRTP Authentication Key	160-bit HMAC key	Derived internally using SRTP Master Key	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Authentication of SRTP session packets
RADIUS Shared Secret	Shared secret (alpha-numeric string) Up to 48 characters	Entered by CO in ciphertext via Web Interface or CLI (over SSH) OR Entered by CO in plaintext via CLI (over serial port) OR Imported in ciphertext in an INI file via Web Interface or CLI (over SSH)	Exported in an INI file via TLS or SSH	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only) OR The CO entering an all-zero value using the Web Interface or CLI OR Importing a new INI file with a zero-value RADIUS shared secret	Peer authentication of RADIUS messages
DRBG Seed	384-bit value	Generated internally using entropy input string	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Random number generation
Entropy Input String	384 bits	Generated internally	Never exits the module	Plaintext in RAM	End of DRBG function, soft reset, Power cycle	Random number generation
DRBG Key Value	Internal DRBG state value 256 bits	Generated internally	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Random number generation

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG 'V' Value	Internal DRBG state value 128 bits	Generated internally	Never exits the module	Plaintext in RAM	Soft reset/power cycle	Random number generation
SNMPv3 Session Key	128-bit AES-CFB key or 168-bit Triple-DES key	Derived internally using SNMP KDF	Never output from module	Plaintext in RAM	Soft reset/power cycle	Encrypting SNMPv3 packets
SNMPv3 Authentication Key	160-bit HMAC key	Derived internally using SNMP KDF	Never output from module	Plaintext in RAM	Soft reset/power cycle	Authenticating SNMPv3 packets
SNMPv3 Authentication Password	Passphrase Minimum of eight (8) characters	Input electronically in ciphertext via Web Interface or CLI (over SSH) OR Input electronically in plaintext via CLI (over serial port) OR Imported in ciphertext in an INI file via Web Interface or CLI (over SSH)	Output in an INI file via TLS or SSH	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only) The CO entering an all-zero value using the Web Interface or CLI OR Importing a new INI file with a zero-value SNMPv3 Authentication Password	Deriving the SNMPv3 Authentication Key

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Privacy Password	Passphrase Minimum of eight (8) characters	Input electronically in ciphertext via Web Interface or CLI (over SSH) OR Input electronically in plaintext via CLI (over serial port) OR Imported in ciphertext in an INI file via Web Interface or CLI (over SSH)	Output in an INI file via TLS or SSH	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only) The CO entering an all-zero value using the Web Interface or CLI OR Importing a new INI file with a zero-value SNMPv3 Privacy Password	Deriving the SNMPv3 Session Key
Crypto Officer Password	Alphanumeric string Minimum of eight (8) characters	Input electronically in ciphertext via Web Interface or CLI (over SSH) OR Input electronically in plaintext via CLI (over serial port) OR Imported in ciphertext in an INI file via Web Interface or CLI (over SSH)	Output in an INI file via TLS or SSH	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only) The CO entering an all-zero value using the Web Interface or CLI OR Importing a new INI file with a zero-value Crypto Officer password	Authenticating the Crypto Officer to the module

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
User Password	Alphanumeric string Minimum of eight (8) characters	Input electronically in ciphertext via Web Interface or CLI (over SSH) OR Input electronically in plaintext via CLI (over serial port) OR Imported in ciphertext in an INI file via Web Interface or CLI (over SSH)	Output in an INI file via TLS or SSH	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only) The CO entering an all-zero value using the Web Interface or CLI OR Importing a new INI file with a zero-value User password	Authenticating the User to the module
Firmware Load Authentication Key	2048-bit RSA public key	Hardcoded/embedded in the application's firmware image	Never exits the module	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	N/A	Verifying the RSA signature of the digest of a new software load package
SFTP Private Key	2048 or 3072-bit RSA private key	Generated internally via FIPS-Approved DRBG OR Generated externally and imported in Base64 encoded (PEM) file format via Web Interface or CLI	Never exits the module	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only); zeroization command	Authentication during SFTP session negotiation

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SFTP Public Key	2048 or 3072-bit RSA key	Generated internally via FIPS-Approved DRBG as part of CSR or self-signed certificate generation OR Generated externally and imported in textual PEM format via Web Interface or CLI	Exits the module in plaintext form	[for the 4000 and 9080] Plaintext in RAM [for the 4000] Plaintext in non-volatile flash [for the 9080] Plaintext in non-volatile hard disk	Soft reset/power cycle (RAM only)	Authentication during SFTP session negotiation
AES GCM IV ⁶¹	96-bit IV	Generated internally deterministically in compliance with TLS 1.2 GCM Cipher Suites for TLS and Section 8.2.1 of NIST SP 800-38D via FIPS-Approved DRBG	Never output from module	Plaintext in RAM	Soft reset/power cycle	IV input to AES-GCM function. Used in the TLS protocol.

⁶¹ IV – Initialization Vector

The AES-GCM IV is used in the TLS protocol. The AES-GCM IV is internally generated deterministically in compliance with TLSv1.2 GCM cipher suites as specified in RFC 5288 and Section 8.2.1 of NIST SP 800-38D. Per RFC 5246, when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key.

The module is compatible with TLSv1.2 and supports acceptable GCM ciphersuites from Section 3.3.1 of SP 800-52 Rev 2.

2.7 EMI / EMC

The module was tested and found to be conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.8 Self-Tests

The module performs power-up self-tests, conditional self-tests, and critical function tests. These tests are described in the sections that follow.

2.8.1 Power-Up Self-Tests

The SBC performs the following self-tests at power-up to verify the integrity of the firmware images and the correct operation of the FIPS-Approved algorithm implementations:

- Firmware Integrity Test on Mediant SBC firmware components and crypto library using 2048-bit RSA digital signature with SHA-256
- Crypto accelerator algorithm tests:
 - AES ECB encrypt KAT⁶²
 - AES ECB decrypt KAT
 - SHA-1, SHA-256 KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
 - RSA signature generation KAT
 - RSA signature verification KAT
 - FFC DH Primitive “Z” Computation KAT
- Crypto Library algorithm tests:
 - AES ECB encrypt KAT
 - AES ECB decrypt KAT
 - AES CCM encrypt KAT
 - AES CCM decrypt KAT
 - AES GCM encrypt KAT
 - AES GCM decrypt KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
 - HMAC SHA-1, HMAC SHA-256, and HMAC SHA-384 KAT
 - SHA-224, SHA-512 KAT

⁶² KAT – Known Answer Test

- CTR_DRBG KAT
- RSA signature generation KAT
- RSA signature verification KAT
- ECC CDH Primitive “Z” Computation KAT
- FFC DH Primitive “Z” Computation KAT

Note: For the Crypto Library, HMAC KATs with SHA-1, SHA-256, and SHA-384 utilize (and thus test) the full functionality of the SHA-1, SHA-256, and SHA-384 algorithms; therefore, no independent KATs for SHA-1, SHA-256, and SHA-384 implementations are required.

The CO can run the module’s power-up self-tests at any time by issuing a reset command over the module’s Management interfaces.

Also the power-up self-tests can be initiated via power-cycling the module (power button with Mediant 9080 SBC or reset pinhole button with Mediant 4000 SBC) or by disconnecting and reconnecting power connectors to the module. For these services, an operator is not required to assume an authorized role.

2.8.2 Conditional Self-Tests

The SBC performs the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for the DRBG (Crypto Library)
- CRNGT for the NDRNG entropy source (Crypto Library)
- Firmware Load Test using RSA signature verification with SHA-256
- RSA Pair-wise Consistency Test using SHA-256 (Crypto Library)

2.8.3 Critical Functions Self-Tests

The SBC implements the counter-based DRBG (specified in *NIST SP 800-90Arev1*) as its random number generator. The DRBG specification requires that certain critical functions be tested conditionally to ensure the security of the DRBG. Therefore, the following critical function tests are implemented by the cryptographic module:

- Instantiate Critical Function Test
- Generate Critical Function Test
- Reseed Critical Function Test
- Uninstantiate Critical Function Test

2.8.4 Self-Test Failure Handling

If the module fails any power-up self-test, 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 firmware load test, the module enters a “Soft Error” state and with error status logged in syslog and the load process aborted.

On failure of any conditional cryptographic self-test or critical function test, the module goes into 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.

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3. Secure Operation

The SBC meets overall Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-approved mode of operation.

3.1 Installation and Setup

The CO shall be responsible for receiving, installing, initializing, and maintaining the SBC module. To operate the module in the Approved mode, the CO shall configure the module via the Web Interface or the CLI as directed by this Security Policy. The following sections provide the CO with important instructions and guidance for the secure installation and configuration of the SBC.

3.1.1 Initial Setup

Upon receiving the SBC hardware, the CO shall check that the system is not damaged and that all required parts and instructions are included. The CO shall refer to the following documents for initial setup instructions:

- *AudioCodes Hardware Installation Manual, Mediant 9000 SBC Series, Mediant 9000 Rev. B, Mediant 9030, Mediant 9080, Version 7.4, May 19, 2019*
- *AudioCodes Hardware Installation Manual, Mediant 4000 SBC, Version 7.4, April 29, 2019*

After the CO has finished installation of the module, the management interfaces can be accessed to configure the module in the FIPS-Approved mode of operation, which is outlined in section 3.1.2 below.

3.1.2 FIPS-Approved Mode Configuration

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

- *AudioCodes Reference Guide, Command-Line Interface for Media Gateways & SBCs Version 7.4, May 19, 2019*
- *AudioCodes User's Manual, Mediant 9000 SBC Series, Mediant 9000 Rev. B / Mediant 9030 / Mediant 9080, Version 7.4, May 19, 2019*
- *AudioCodes User's Manual, Mediant 4000 SBC, Version 7.4, May 16, 2019*

To configure the SBC into FIPS mode, the CO must perform the following actions:

- The CO must enable FIPS mode by issuing the command `FIPSmode enable` using the CLI.

- The CO must configure “TLS contexts”, which are settings that define the TLS parameters used for management and other TLS applications. Configuring TLS contexts is addressed in the “Configuring SSL/TLS Certificates” and “Security” chapters of the AudioCodes User’s Manuals. The CO must ensure that all TLS contexts are configured according to the following guidance:
 - For RSA keys, the CO must only import RSA keys that are equal to 2048 or 3072 bits in length.
 - For TLS versions, the CO must select version 1.0, 1.1, or 1.2. The CO must not select SSLv3.
 - For supported TLS ciphersuites only FIPS-Approved algorithms must be used. To ensure that only FIPS-Approved algorithms are during ciphersuite negotiations, add the following to the ciphersuite strings: **!RC4:!aNULL:!eNULL:!AECDH:!ADH:!CAMELLIA:!ARIA128:!SEED**.
 - For SRTP parameters, ensure the Media Security Behavior is set to “Mandatory” (instead of the default “Preferable”) and the Aria Protocol Support is set to “Disable” (the default).
 - For secure key transfer, ensure derived session keys are transferred to endpoints using TLS (i.e., force TLS) by configuring ‘0’ on the UDP and TCP port of each SIP interface
 - For secure RADIUS connections, enable HTTPS for RADIUS by configuring the 'Secured Web Connection (HTTPS)' parameter to **HTTPS Only** (see "Configuring Secured (HTTPS) Web" section of the *AudioCodes User’s Manual*).

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

3.2 Crypto Officer Guidance

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

3.2.1 Management

Once installed, commissioned, and configured, the CO is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. Please refer to Section 3.1.2 for guidance that the CO must follow for the module to be considered running in a FIPS-Approved mode of operation.

3.2.2 Default Password

The Mediant 4000 SBC and Mediant 9080 SBC provide a default password for module access for the CO only. The CO is required to change the default password as part of the initial configuration.

3.2.3 On-Demand Self-Tests

The power-up self-tests are automatically performed at power-up. The CO may initiate the power-up self-tests by issuing the reset command or power-cycling the module.

Using the CLI, resetting the module is accomplished by issuing the following command:

```
# reload now
```

Using the Web interface, resetting the module is accomplished by navigating to **Setup -> Administration -> Maintenance -> Maintenance Actions** and clicking the Reset button.

3.2.4 Zeroization

There are many CSPs within the module's cryptographic boundary including symmetric keys, private keys, public keys, and login passwords hashes. CSPs reside in multiple storage media including the RAM, non-volatile flash, and hard disk. All ephemeral keys used by the module are zeroized on reset and power cycle. Private keys and CSPs on the non-volatile flash and hard disk of the module can be zeroized by using a CLI command. The public key used for the firmware load test is stored in non-volatile flash and hard disk and cannot be zeroized.

Using the CLI, keys and CSPs are zeroized using the following command:

```
# clear security-files
```

The RADIUS Shared Secret, SNMPv3 Authentication Password, SNMPv3 Privacy Password, Crypto Officer password, and User 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.

3.3 User 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.

3.4 Additional Guidance and Usage Policies

This section notes 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.
- The CO shall power-cycle 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 firmware, and employs an Approved message authentication technique to test its integrity. However, to maintain an Approved mode of operation, the CO must ensure that only FIPS-validated firmware is loaded. Any operation of the module after loading non-validated firmware constitutes a departure from this Security Policy.
- The CO shall ensure that the module performs no more than 2^{16} encryptions with a given Triple-DES key.

- In order to comply with the key entry requirements described in section 7.7 of the *Implementation Guidance for FIPS PUB 140-2 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.

3.5 Non-Approved Mode of Operation

When initialized and configured according to the guidance in section 3.1.2 of this Security Policy, the module does not support a non-Approved mode of operation.

4. Acronyms

Table 11 provides definitions for the acronyms used in this document.

Table 11 – Acronyms

Acronym	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	ECC Cofactor Diffie Hellman

Acronym	Definition
ECDSA	Elliptical Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
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
KAT	Known Answer Test
KDF	Key Derivation Function
LED	Light Emitting Diode
MAC	Message Authentication Code
Mbps	Megabits per second
MD5	Message Digest 5
MOS	Mean Opinion Score
N/A	Not Applicable
NAT	Network Address Translation
NDRNG	Non-Deterministic Random Number Generator
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
PEM	Privacy Enhanced Mail

Acronym	Definition
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.



13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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

