

Sonus Networks, Inc.

SBC 7000 Session Border Controller

Hardware Model: SBC 7000; Firmware Version: 5.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1

Document Version: 0.8

Prepared for:



Sonus Networks, Inc.
4 Technology Park Drive

Westford, MA 01886
United States of America

Phone: +1 855 GO SONUS
www.sonus.net

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. Introduction4**
 - 1.1 Purpose4
 - 1.2 References4
 - 1.3 Document Organization4
- 2. SBC 7000 Session Border Controller5**
 - 2.1 Overview5
 - 2.2 Module Specification8
 - 2.3 Module Interfaces 10
 - 2.4 Roles and Services 13
 - 2.4.1 Authorized Roles 13
 - 2.4.2 Operator Services 13
 - 2.4.3 Additional Services 16
 - 2.4.4 Authentication 17
 - 2.5 Physical Security 18
 - 2.6 Operational Environment 18
 - 2.7 Cryptographic Key Management 18
 - 2.8 EMI / EMC 23
 - 2.9 Self-Tests 23
 - 2.9.1 Power-Up Self-Tests 23
 - 2.9.2 Conditional Self-Tests 24
 - 2.9.3 Critical Functions Self-Tests 24
 - 2.9.4 Self-Test Failure Handling 24
 - 2.10 Mitigation of Other Attacks 24
- 3. Secure Operation25**
 - 3.1 Initial Setup 25
 - 3.1.1 SBC Hardware Installation and Commissioning 25
 - 3.1.2 SBC Firmware Installation and Configuration 25
 - 3.1.3 SBC FIPS-Approved Mode Configuration and Status 26
 - 3.2 Crypto Officer Guidance 26
 - 3.2.1 Management 27
 - 3.2.2 Zeroization 27
 - 3.2.3 Status Monitoring 27
 - 3.3 User Guidance 27
 - 3.4 Additional Usage Policies 28
 - 3.5 Non-FIPS-Approved Mode 28
- 4. Acronyms29**

List of Tables

Table 1 – Security Level per FIPS 140-2 Section	8
Table 2 – FIPS-Approved Algorithm Implementations	8
Table 3 – FIPS 140-2 Logical Interface Mappings	11
Table 4 – SBC 7000 Session Border Controller LEDs Description	12
Table 5 – Authorized Operator Services.....	14
Table 6 – Additional Services.....	16
Table 7 – Authentication Mechanism Used by the Module.....	17
Table 8 – Cryptographic Keys, Cryptographic Key Components, and CSPs.....	19
Table 9 – Non-Approved Services	28
Table 10 – Acronyms	29

List of Figures

Figure 1 – Front View of SBC 7000	5
Figure 2 – Rear View of SBC 7000.....	6
Figure 3 – A Typical Deployment Scenario of SBC.....	8
Figure 4 – Rear Panel Ports of SBC 7000	11

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the SBC 7000 Session Border Controller from Sonus Networks, Inc. (Sonus). This Security Policy describes how the SBC 7000 Session Border Controller meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. 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 Canada's Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at <http://csrc.nist.gov/groups/STM/cmvp>.

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 SBC 7000 Session Border Controller is referred to in this document as the SBC, or the module.

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 Sonus website (www.sonus.net) contains information on the full line of products from Sonus.
- The CMVP website (<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Sonus. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Sonus and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Sonus.

2. SBC 7000 Session Border Controller

2.1 Overview

Sonus Networks, Inc. (hereafter referred to as Sonus) is a leader in IP¹ networking with proven expertise in delivering secure, reliable and scalable next-generation infrastructure and subscriber solutions. The Sonus line of Session Border Controllers (SBC) help mid-sized and large enterprises take advantage of cost-saving SIP² trunking services by securing their network from IP-based attacks, unifying SIP-based communications and controlling traffic in the network.

Sonus's SBC 7000 Session Border Controller features a unique architecture design that differs from other SBCs on the market today by aggregating all of the session border functionality – security, encryption, transcoding, call routing, and session management – into a single device and distributing those functions to embedded and modular hardware within the device. For example, media transcoding on the SBC is performed on a modular DSP³ farm while much of the encryption is handled via embedded cryptographic hardware, thereby, providing optimal performance during real-world workloads, overloads, and attacks.

The SBC 7000 Session Border Controller is a high-performance air-cooled, 5U, IP encryption appliance that provides secure SIP-based communications with robust security, reduced latency, real-time encryption (VOIP⁴ signaling and media traffic), media transcoding, flexible SIP session routing and policy management.

Figure 1 and Figure 2 below show a picture of the front and rear panels of the SBC 7000 Session Border Controller respectively.



Figure 1 – Front View of SBC 7000

¹ IP – Internet Protocol

² SIP – Session Initiation Protocol

³ DSP – Digital Signal Processor

⁴ VOIP – Voice Over Internet Protocol



Figure 2 – Rear View of SBC 7000

The SBC is designed to fully address the next-generation need of SIP communications by delivering embedded media transcoding, robust security and advanced call routing in a high-performance, medium form-factor device. The SBC 7000 is designed to accommodate upto 150,000 call sessions. Some of the network and security features provided by the module include:

- Session-aware firewall, split DMZ⁵, bandwidth & QoS⁶ theft protection, topology hiding, DoS⁷/DDoS⁸ detection/blocking, rogue RTP⁹ protection, IPsec¹⁰ and TLS¹¹ encryption
- Embedded media transcoding hardware
- H.323 and SIP-I/T interworking
- Stateful call-handling even during overload/attack/outages
- Embedded localized or centralized call-routing options
- Far-end NAT¹² traversal
- TLS, IPsec (IKEv1¹³) for signaling encryption
- Secure RTP/RTCP¹⁴ for media encryption
- Support for large number of protocols including IPv4, IPv6, IPv4/IPv6 interworking, SSH¹⁵, SFTP¹⁶, SNMP¹⁷, HTTPS¹⁸, RTP/RTCP, UDP¹⁹, TCP²⁰, DNS²¹, and ENUM²²
- Exceptional scalability even under heavy workloads
- Device management using encrypted and authenticated device management messages

⁵ DMZ – Demilitarized Zone

⁶ QoS – Quality of Service

⁷ DoS – Denial of Service

⁸ DoS/DDoS – Denial-of-Service/Distributed Denial-of-Service

⁹ RTP – Real-time Transport Protocol

¹⁰ IPsec – Internet Protocol Security

¹¹ TLS – Transport Layer Security

¹² NAT – Network Address Translation

¹³ IKEv1 – Internet Key Exchange version 1

¹⁴ RTCP – RTP Control Protocol

¹⁵ SSH – Secure Shell

¹⁶ SFTP – SSH File Transport Protocol

¹⁷ SNMP – Simple Network Management Protocol

¹⁸ HTTPS – Hypertext Transfer Protocol Secure

¹⁹ UDP – User Datagram Protocol

²⁰ TCP – Transmission Control Protocol

²¹ DNS – Domain Name System

²² ENUM – E.164 Number Mapping

- Controlled menu access and comprehensive audit logs
- Integrated Baseband Management Controller (BMC)

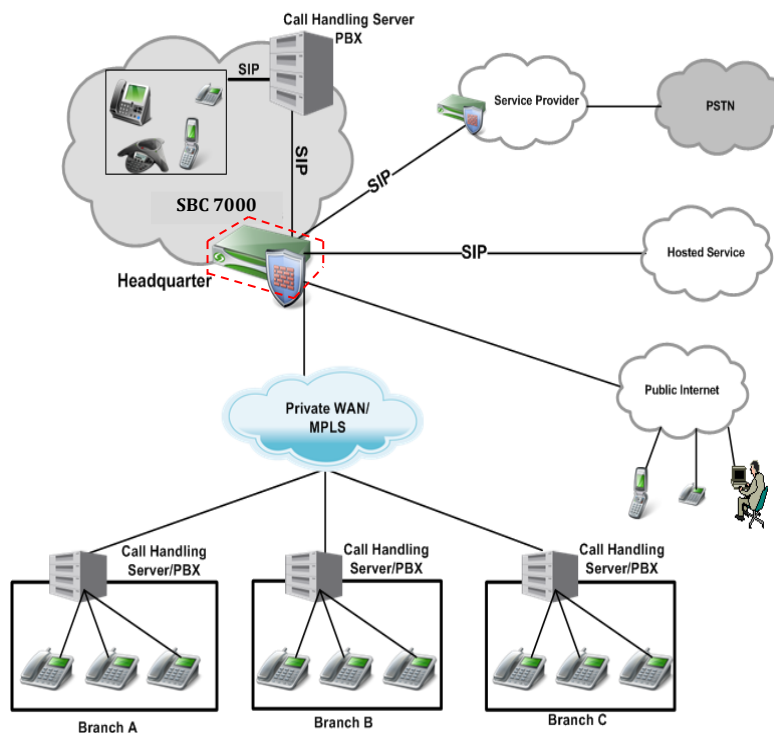
The validated module is a solution that delivers end-to-end SIP session control and a networkwide view of SIP traffic and policy management. The module can be deployed as peering SBCs, access SBCs, or enterprise-SBCs (e-SBCs).

Management of the SBC 7000 Session Border Controller is accomplished via:

- SNMPv3 traps and polling, which are used only for non-security relevant information about the module's state and statistics
- Command Line Interface (CLI), which is accessible remotely via SSH over Ethernet Management ports
- Web-based Graphical User Interface (GUI), which is accessible remotely via HTTPS (using EMA²³ and PM²⁴) over Ethernet management ports

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.

Figure 3 below illustrates a typical deployment scenario of the SBC and the cryptographic boundary is shown by the red-colored dotted line.



²³ EMA – Embedded Management Application

²⁴ PM – Platform Manager

Figure 3 – A Typical Deployment Scenario of SBC

The SBC 7000 Session Border Controller is 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	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A ²⁵
7	Cryptographic Key Management	1
8	EMI/EMC ²⁶	1
9	Self-tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The SBC 7000 Session Border Controller is a hardware cryptographic module with a multiple-chip standalone embodiment. The cryptographic module consists of firmware and hardware components enclosed in a secure, production-grade metal case. The main hardware components consist of integrated circuits, processors, memories, SSD²⁷, flash, DSP, power supplies, fans, and the enclosure containing all of these components. The overall security level of the module is 1. The cryptographic boundary of the SBC is defined by the SBC device enclosure, which encompasses all the hardware and firmware components.

The other component that is excluded from the boundary and, therefore, from the FIPS 140-2 requirements is the Small Form-Factor Pluggable (SFP) transceivers that can be connected to the media and the HA interfaces of the module. These are merely adapters to interface the module's ports to either copper-based or fiber-based wiring, depending on the customer need.

The SBC 7000 Session Border Controller uses the FIPS-Approved algorithm implementations in hardware (Network Processor) and firmware (Crypto Library) as listed in Table 2 below.

Table 2 – FIPS-Approved Algorithm Implementations

²⁵ N/A – Not applicable

²⁶ EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

²⁷ SSD – Solid State Drive

Algorithm	Certificate Number	
	Network Processor	Crypto Library
AES ²⁸ in CBC ²⁹ , CTR modes (128-bit key)	#3482	-
AES in CBC, CFB ³⁰ modes (128, 256-bit keys)	-	#3483
AES in ECB ³¹ mode (128, 192, 256-bit keys)	-	#3483
AES in GCM ³² mode (128, 256-bit keys)	-	#3483
Triple-DES ³³ in CBC, ECB modes (keying option 1, 2)	-	#1964
Triple-DES in CBC mode (keying option 1, 2)	#1963	-
SHA ³⁴ -1	#2876	#2877
HMAC ³⁵ -SHA-1	#2224	#2225
SHA-224, SHA-256, SHA-384, SHA-512		#2877
HMAC using SHA-224, SHA-256, SHA-384, SHA-512	-	#2225
RSA key generation (2048-bit)	-	#1788
RSA (PKCS ³⁶ #1 v1.5) signature generation (2048-bit), signature verification (1024, 2048-bit)	-	#1788
ECDSA (FIPS 186-4) PKV/SigVer for all P, K, and B curves; PKG/SigGen for all P, K, and B curves except P-192, K-163, and B-163	-	#709
SP ³⁷ 800-90A CTR_DRBG ³⁸	-	#860
CVL ³⁹ for KDF ⁴⁰ (TLS – SP 800-135, Section 4.2)	-	#559
CVL for KDF (SSH – SP 800-135, Section 5.2)	-	#559
CVL for KDF (SNMP – SP 800-135, Section 5.4)	-	#559
CVL for KDF (SRTP – SP 800-135, Section 5.3)	#557	-
CVL for EC ⁴¹ Diffie-Hellman SP800-56A All NIST-Defined Curves except P-192, K-163, and B-163.	-	#558

Note: The TLS, SSH, SNMP, and SRTP protocols have not been reviewed or tested by the CAVP or CMVP.

The module uses the FIPS-Approved SP 800-90A CTR_DRBG to generate cryptographic keys. The module does not receive seed value for the DRBG from outside; rather, it is seeded via `/dev/random`, a Non-Deterministic Random Number Generator (NDRNG) internal to the module.

²⁸ AES – Advanced Encryption Standard

²⁹ CBC – Cipher Block Chaining

³⁰ CFB – Cipher Feedback

³¹ ECB – Electronic Codebook

³² GCM – Galois/Counter Mode

³³ DES – Data Encryption Standard

³⁴ SHA – Secure Hash Algorithm

³⁵ HMAC – Keyed-Hash Message Authentication Code

³⁶ PKCS – Public-Key Cryptography Standards

³⁷ SP – Special Publication

³⁸ DRBG – Deterministic Random Bit Generator

³⁹ CVL – Component Validation List

⁴⁰ KDF – Key Derivation Function

⁴¹ EC – Elliptical Curve

The module implements the following non-Approved algorithms that are allowed to be used in FIPS-Approved mode of operation:

- RSA (key encapsulation; key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (used for key establishment) (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- NDRNG (used for seeding the DRBG)
- MD5 (used for firmware integrity test during power-up self-test)

Additional information concerning DSA, ECDSA, SHA-1, Diffie-Hellman key establishment, RSA, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

2.3 Module Interfaces

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

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

Data input/output are the packets utilizing the services provided by the module. These packets enter and exit the module through the Ethernet Media, Management, and HA⁴² interfaces. Control input consists of configuration or administration data entered into the module through the Command Line Interface (CLI) and Web GUI over Ethernet management interfaces, USB, and HA ports. Status output consists of the status provided over Ethernet Management interfaces, HA ports, and also displayed via LEDs⁴³ and log information.

The physical ports and interfaces of the SBC 7000 Session Border Controller are depicted in Figure 1, Figure 2, and marked in Figure 4 below. Table 3 lists the physical ports/interfaces available in the SBC, and also provides the mapping from the physical ports/interfaces to logical interfaces as defined by FIPS 140-2.

⁴² HA – High Availability

⁴³ LED – Light Emitting Diode

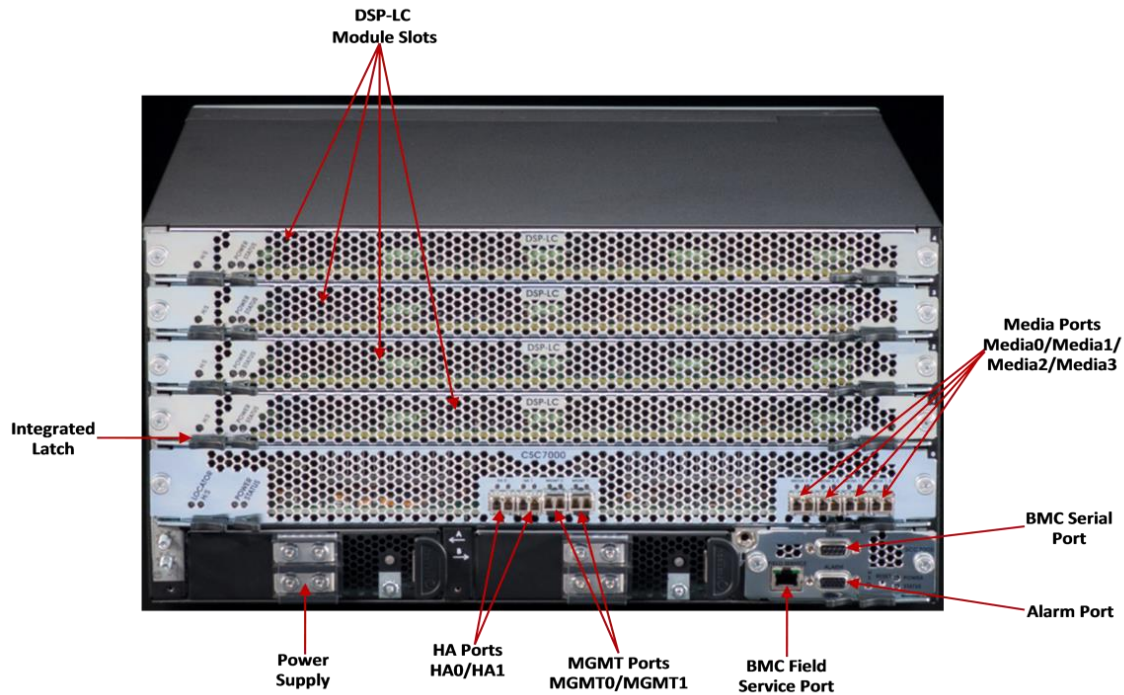


Figure 4 – Rear Panel Ports of SBC 7000

Physical interfaces for the SBC are described in Table 3 below.

Table 3 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity		FIPS 140-2 Logical Interface
	SBC 7000		
Ethernet Media Port	BP ⁴⁴	4	Data in, Data out
Ethernet Management Port	BP	2	Data in, Data out Control in, Status out
Ethernet HA Port	BP	2	Data in, Data out Control in, Status out
USB Port	FP ⁴⁵	1	Control in
Power LED	FP	1	Status out
	BP	2	
Status LED	FP	1	Status out
	BP	2	
Active LED	FP	1	Status out
Alarm LED	FP	1	Status out

⁴⁴ BP – Back Panel

⁴⁵ FP – Front Panel

Physical Port/Interface	Quantity		FIPS 140-2 Logical Interface
	SBC 7000		
Locator LED	FP	1	Status out
	BP	1	
H/S ⁴⁶ LED	BP	2	Status out
Power Supply LED	BP	2	Status out
AC/DC ⁴⁷ Power Input Connector	BP	2	Control in

NOTE: Each module also includes a back panel alarm port. This port is not operational, and provides no facility for input or output.

Each SFP⁴⁸ port and Ethernet port on the SBC 7000 has LEDs associated with it, which indicate the status of the port. The LED is OFF if the cable is not connected and link is not established. The LED turns GREEN if a cable is connected and the link is established, and flashes when activity is present.

As shown in Figure 1 and Figure 4 above, the module has number of LEDs that indicate the state of the module. The descriptions for the LEDs are listed in the Table 4 below.

Table 4 – SBC 7000 Session Border Controller LEDs Description

LED	Description	Color	Definition
FP Power LED	Indicator of power status for all voltages generated on the module	OFF	The module is not powered.
		GREEN	The module is all powered on.
		AMBER	The module’s BMC power good.
BP Power LED	Indicator of power status of swappable modules	OFF	The swappable module is off when 48V is not applied to it.
		GREEN	The swappable module is on when 48V is applied to it.
FP Status LED	Indicator of module Status	OFF	The module application is not running.
		GREEN	The module is powered and the application is running normally.
		AMBER	The module application startup has not completed, or the application has been shutdown.
BP Status LED	Indicator of operational status of swappable modules	OFF	The swappable module is not running.
		GREEN	The swappable module has completely started and running.
FP Active LED	Indicator of module redundancy State	OFF	The module is in standby mode.
		GREEN	The module is active and protected.
		Blinking GREEN	The module is active but unprotected.
		AMBER	The module is core dumping.

⁴⁶ H/S – Hot Swappable

⁴⁷ AC/DC – Alternating Current/Direct Current

⁴⁸ SFP – Small Form-factor Pluggable

LED	Description	Color	Definition
FP Alarm LED	Indicator of module Critical/Major Failure	OFF	The module is in no alarm condition state.
		AMBER	The module is in major alarm condition state.
		RED	The module is in critical alarm state.
FP Locator LED	Indicator of module Identifier	OFF	The module is not being identified.
		ON or Blinking	The module is being user identified.
BP Locator LED	Indicator of module Identifier	OFF	The swappable module is not being identified.
		ON or Blinking	The swappable module is being user identified.
BP H/S LED	Indicator of operations status of the hotswappable module when chassis management software brings down the module.	OFF	The hotswappable module is running normal.
		SOLID BLUE	The hotswappable module is completely down and safe for removal.
		FLASHING BLUE	The hotswappable module is shutting down or going offline.
Power Supply LED	Indicator of state of the power supply	OFF	The power supply is not working.
		GREEN	The power supply is operational.
Ethernet and SFP Port LEDs	Indicator of link and activity status	GREEN	A cable is connected and the link is up.
		Blinking GREEN	Activity is present on the link.

Apart from these indicators, the alarms events are also logged into log file.

2.4 Roles and Services

The sections below describe the module’s roles and services, and define any authentication methods employed.

2.4.1 Authorized Roles

As required by FIPS 140-2, the module supports two roles that operators may assume:

- **Crypto Officer** – 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 FIPS-Approved mode of operation. The CO also has access to all User services.
- **User** – 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 and SSH.

2.4.2 Operator Services

Descriptions of the services available to the Crypto Officer role and User role are provided in the Table 5 below. The keys and CSPs listed in Table 5 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 5 – 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
Manage SBC License	✓		Installs the license to enable SBC features; delete or update license; view current license status	Command	Status output	None
Configure the SBC system	✓		Define network interfaces and settings; set protocols; configure authentication information; define policies and profiles	Command and parameter	Command response/ Status output	None
Configure routing policy and control services	✓		Configure IP network parameters and profiles for signaling, media, call routing, call services, zone, IP ACL ⁴⁹ rules, NTP ⁵⁰ and DNS ⁵¹ servers	Command and parameters	Command response/ Status output	None
Configure Crypto Suite Profile	✓		Select crypto suites for SRTP, SRTCP, and SIP communication	Command and parameters	Command response/ Status output	None
Configure Call Data Record (CDR)	✓		Configure log file behavior	Command and parameters	Command response/ Status output	None
Manage users	✓		Create, edit and delete users; define user accounts and assign permissions.	Command and parameters	Command response/ Status output	Password – R/W/X
Manage user sessions	✓		Terminate User sessions	Command and parameters	Command response/ Status output	TLS Session Key – W

⁴⁹ ACL – Access Control List

⁵⁰ NTP – Network Time Protocol

⁵¹ DNS – Domain Name System

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Change password	✓	✓	Modify existing login passwords	Command and parameters	Command response/ Status output	Password – R/W
Load certificate	✓		Loads new certificates	Command	Command response/ Status output	CA ⁵² Public Keys – R/W Peer Public Keys – R/W
Run script	✓		Run a script file (a text file containing a list of CLI commands to execute in sequence)	Command	Command response/ Status output	None (service may potentially access CSPs indirectly via scripted CLI commands)
Perform Self Tests	✓		Perform on-demand Self-Tests	Command	Command response/ Status output	All ephemeral keys and CSPs – W
Perform Network Diagnostics (e.g. ping)	✓	✓	Monitor connections	Command	Command response/ Status output	None
Show Status	✓	✓	Show the system status, Ethernet status, FIPS Approved mode, alarms, system identification and configuration settings of the module	Command	Command response/ Status output	None
View Event Log	✓		View event status messages	Command	Command response/ Status output	None
Zeroize Keys	✓		Zeroize all keys and CSPs	Command	Command response/ Status output	All CSPs – W
Upgrade Firmware	✓		Load new firmware and performs an integrity test using an RSA digital signature	Command	Command response/ Status output	RSA Public Key – R/X
Perform Keying of CDB ⁵³ key	✓		Generate CDB key	Command and parameters	Command response/ Status output	CDB key – W/X
Reboot/Reset	✓		Reboot or reset the module	Command	Command response/ Status output	CSPs stored in SDRAM – W

⁵² CA – Certificate Authority⁵³ CDB – Configuration Database

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Establish TLS Session	✓	✓	Establish web session using TLS protocol	Command	Command response/ Status output	Password – X RSA Public key – R/X RSA Private key – X HMAC Key – W/X ECDSA Public key – R/X ECDSA Private key – X TLS Session key – R/W/X TLS Authentication Key – R/W/X
Establish SSH Session	✓	✓	Establish remote session using SSH protocol	Command	Command response/ Status output	Password – X SSH Authentication Key – R/W/X SSH Session Key – R/W/X RSA Public key – R/X RSA Private Key – X HMAC Key – W/X
SNMPv3 Traps		✓	Provides system condition information	None	Status output	SNMPv3 Session Key – R/W/X SNMPv3 HMAC Key – R/W/X
Encryption/ Decryption service	✓	✓	Encrypt or decrypt user data, keys, or management traffic	Command and parameters	Command response	TLS Session Key – X SSH Session key – X
Authentication service	✓	✓	Authenticate user data or management traffic	Command and parameters	Command response	TLS Authentication Key – X SSH Authentication key – X

All services listed above require the operator to assume a role, and the module authenticates the role before providing any of these services.

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 6 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 6 – Additional Services

Service	Description	Input	Output	CSP and Type of Access
Zeroize	Zeroize keys and CSPs	Power cycling using power connectors	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	Status output	All ephemeral keys and CSPs – W

Service	Description	Input	Output	CSP and Type of Access
Authenticate	Use to log into the module	Command	Status output	Password – X

2.4.4 Authentication

The module supports role-based authentication. All module operators authenticate using a username and password. Password complexities can be configured by the Crypto Officer. The module requires a minimum of 8 characters and allows a maximum of 24 characters for a password. The password must contain any combination of at least one uppercase letter and one lowercase letter, one number, and a special character, allowing a choice from a total of 95 possible characters. The strength calculation below provides minimum strength based on password policy.

Table 7 lists the authentication mechanisms used by the module.

Table 7 – Authentication Mechanism Used by the Module

Authentication Type	Strength
Password	<p>The minimum length of the password is eight characters, with 95 different case-sensitive alphanumeric characters and symbols possible for usage.</p> <p>The chance of a random attempt falsely succeeding is 1: (95⁸), or 1: 6,634,204,312,890,625.</p> <p>The fastest network connection over Ethernet Interface supported by the module is 1000 Mbps.</p> <p>Hence, at most (10 × 10⁸ × 60 = 6 × 10¹⁰ =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is 1 : [95⁸ possible passwords / ((6 × 10¹⁰ bits per minute) / 64 bits per password)]</p> <p>1: (95⁸ possible passwords / 937,500,000 passwords per minute)</p> <p>1: 7,076,484;</p> <p>which is less than 1:100,000 as required by FIPS 140-2.</p>
Public Key Certificates	<p>The module supports RSA digital certificate authentication of users during Web GUI/HTTPS (TLS) access. Using conservative estimates and equating a 2048 bit RSA key to a 112 bit symmetric key, the probability for a random attempt to succeed is 1:2¹¹² or 1: 5.19 × 10³³.</p> <p>The fastest network connection supported by the module over Ethernet interfaces is 1000 Mbps.</p> <p>Hence at most (100 × 10⁷ × 60 = 6 × 10¹⁰ =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is</p> <p>1: (2¹¹² possible keys / ((6 × 10¹⁰ bits per minute) / 112 bits per key))</p> <p>1: (2¹¹² possible keys / 535,714,285 keys per minute)</p> <p>1: 96.92 × 10²³;</p> <p>which is less than 100,000 as required by FIPS 140-2.</p>

The feedback of authentication data to a user is obscured during authentication. The module provides feedback by displaying a “rounded dot” (●) symbol when an operator is entering his password over EMA and Platform Manager login while no feedback is provided for CLI login.

The module provides the ability for an operator to change roles and requires re-authentication of an operator to assume a new role. In order to change roles, an operator is required to first log out and then log in with an account with appropriate permissions for the desired role.

The module does not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. The authenticated CO can modify their own authentication credentials as well as the credentials of the Users, while the Users have the ability to modify their own authentication data only.

2.5 Physical Security

All CSPs are stored and protected within the SBC 7000 Session Border Controller’s production-grade enclosure. The entire enclosure consists of two parts: the main chassis and the removable upper cover. The removable upper cover is secured to the main enclosure with screws.

All of the components within the module are production grade with standard passivation.

2.6 Operational Environment

The operational environment of the module does not provide a general-purpose operating system (OS) to the user. The SBC’s processors run Sonus’s proprietary Linux-based kernel in a non-modifiable operational environment. The operating system 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.

2.7 Cryptographic Key Management

The module supports the CSPs described in Table 8 below.

Table 8 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Config Database (CDB) Key	Triple-DES 192-bit key	Generated internally via FIPS-Approved DRBG	Never exits the module	Plaintext in SSD	Re-keyed over CLI or EMA , when appliance is re-imaged, or over management command	Encryption of RSA and ECDSA Private key, preshared secrets for RADIUS in CDB
SSH Session Key	AES 128, 256-bit or Triple-DES 192-bit key	Generated internally via Diffie-Hellman key agreement	Never exits the module	Plaintext in RAM	Reboot or session termination	Encryption or decryption during SSH
TLS Session Key	AES 128, 256-bit key	Generated internally via FIPS-Approved DRBG or entered into the module in encrypted form	Never exits the module	Plaintext in RAM	Reboot or session termination	Encryption or decryption of TLS communication
HMAC Key	160-bit (minimum) HMAC key	Generated internally via Diffie-Hellman key agreement	Never exits the module	Plaintext in RAM	Reboot or session termination	TLS and SSH session packet authentication
SRTP Master Key	128-bit shared secret	Generated externally, imported in encrypted form via a secure SIP/TLS session	Exits in encrypted form	Plaintext in RAM	Reboot or session termination	Peer Authentication, Session and Authentication keys derivation for SRTP session
SRTP Symmetric Key	AES-CTR 128-bit key	Generated internally using Master Key	Never exits the module	Plaintext in RAM	Reboot or session termination	Encryption or decryption during SRTP session
SRTP Authentication Key	160-bit HMAC key	Generated internally using Master Key	Never exits the module	Plaintext in RAM	Reboot or session termination	Authentication of SRTP session packets
RADIUS Shared Secret	Shared secret (alpha-numeric string)	Entered electronically by Crypto Officer	Never exits the module	Encrypted in the CDB on SSD	Command via CLI or EMA	Peer Authentication of RADIUS messages
DRBG Seed	256-bit value	Generated internally using entropy input string	Never exits the module	Plaintext in RAM	Reboot or session termination	Generation of random number

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Entropy Input String	512-bit value	Continually polled from various system resources to accrue entropy by NDRNG	Never exits the module	Plaintext in RAM	Reboot or session termination	Generation of random number
RSA Private Key	2048-bit	Generated internally via FIPS-Approved DRBG	Never exit the module	Stored in the CDB on SSD – encrypted for the certificates; stored outside CDB on SSD – plaintext for SSH	Command via CLI or EMA	Used for SSH and SFTP key negotiation; TLS authentication and certificate generation
RSA Public Key	1024, 2048-bit	The module’s 2048-bit public key is generated internally; public key of a peer enters the module in plaintext	The module’s 2048-bit public key exits the module in plaintext form; public key of a peer never exits the module	Plaintext in the CDB on SSD	Command via CLI or EMA	Used for SSH and SFTP key negotiation; TLS authentication and certificate generation; 1024-bit key is used for legacy purposes for signature verification only
ECDSA Private Key	All NIST defined Approved Curves	Generated internally via FIPS-Approved DRBG	Never exit the module	Stored in the CDB on SSD – encrypted for the certificates	Command via CLI or EMA	TLS authentication and certificate generation
ECDSA Public Key	All NIST defined Approved Curves	The module’s public key is generated internally; public key of a peer enters the module in plaintext	The module’s public key exits the module in plaintext form; public key of a peer never exits the module	Plaintext in the CDB on SSD	Command via CLI or EMA	TLS authentication and certificate generation
Diffie-Hellman Public Key	2048-bit	The module’s public key is generated internally; public key of a peer enters the module in plaintext	The module’s public key exits the module in plaintext form; public key of a peer never exits the module	Plaintext in RAM	Reboot or session termination	Generation of SSH Session key
Diffie-Hellman Private Key	2048-bit	Generated internally	Never exits the module	Plaintext in RAM	Reboot or session termination	Generation of SSH Session key

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
EC DH public component	Public components of EC DH protocol	The module's public key is generated internally; public key of a peer enters the module in plaintext	The module's public key exits the module in plaintext; public key of a peer never exits the module	Plaintext in RAM	Reboot or session termination	Generation of SSH Session key
EC DH private component	Private exponent of EC DH protocol	Generated internally	Never exits the module	Plaintext in RAM	Reboot or session termination	Generation of SSH Session key
SNMPv3 Privacy Key	AES-CFB 128-bit or Triple-DES 192-bit	Generated externally, imported in encrypted form via a secure TLS or SSH session	Exits in encrypted form (over TLS session) within configuration data when performing configuration backup	Plaintext in the CDB on SSD	Command via CLI or EMA	Encrypting SNMPv3 packets
SNMPv3 HMAC Key	160-bit HMAC key	Generated externally, imported in encrypted form via a secure TLS or SSH session	Exits in encrypted form (over TLS session) within configuration data when performing configuration backup	Plaintext in the CDB on SSD	Command via CLI or EMA	Authenticating SNMPv3 packets
Crypto Officer password	Minimum of eight characters of alphanumeric string	Initial password generated internally using FIPS-Approved DRBG, password changes entered into module via a console port or over SSH	Initially generated password provided to the CO on CLI/EMA over encrypted session, changed password never exits the module	Plaintext (hashed ⁵⁴) on SSD and in RAM	Zeroized when the password is updated with a new one	Authenticating the Crypto Officer

⁵⁴ Passwords are hashed by the operating system and stored on the SSD. They are temporarily loaded into the memory in hashd form for comparison during a login.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
User password	Minimum of eight characters of alphanumeric string	Initial password generated internally using DRBG, password changes entered into module via a console port or over SSH	Initially generated password provided to the User on CLI/EMA over encrypted session, changed password never exits the module	Plaintext (hashed) on SSD and in RAM	Zeroized when the password is updated with a new one	Authenticating the User
Firmware Load Authentication Key	Hardcoded RSA 2048-bit key with SHA-256	Embedded in release image	Never exits the module	Image in Flash memory	The Flash location is write protected in hardware at the factory (i.e. not writeable by end user) and is not zeroized.	Verify RSA signature of firmware image digest

2.8 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).

2.9 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.

2.9.1 Power-Up Self-Tests

The SBC 7000 Session Border Controller 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 tests using MD5 and HMAC-SHA 256
- Network Processor driver algorithm tests:
 - AES encrypt KAT⁵⁵
 - AES decrypt KAT
 - HMAC SHA-1 KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
- Crypto Library algorithm tests:
 - AES encrypt KAT
 - AES decrypt KAT
 - AES GCM encrypt KAT
 - AES GCM decrypt KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
 - HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512 KAT
 - SP 800-90A CTR_DRBG KAT
 - RSA signature generation KAT
 - RSA signature verification KAT
 - ECDSA Pair-wise Consistency Test
 - ECC CDH KAT

Note: HMAC KATs with SHA-1 and SHA-2 utilize (and thus test) the full functionality of the SHA-1 and SHA-2 algorithms; thus, no independent KATs for SHA-1 and SHA-2 implementations are required.

The CO or User can perform the power-up self-tests at any time by power-cycling the module or issuing a reboot command over the module's Management interface over SSH or HTTPS. Also, the module can be made to perform power-up self-tests by disconnecting and reconnecting power connectors to the module; and for this service, an operator is not required to assume an authorized role.

⁵⁵ KAT – Known Answer Test

2.9.2 Conditional Self-Tests

The SBC 7000 Session Border Controller 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 (for OS, SonusDB, EMA, and SBC)
- RSA Pair-wise Consistency Test (Crypto Library)
- ECDSA Pair-wise Consistency Test (Crypto Library)
- EC Diffie-Hellman pairwise consistency test (Crypto Library)

2.9.3 Critical Functions Self-Tests

The SBC 7000 Session Border Controller implements the SP 800-90A CTR_DRBG as its random number generator. The SP 800-90A 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:

- SP 800-90A CTR_DRBG Instantiate Critical Function Test
- SP 800-90A CTR_DRBG Generate Critical Function Test
- SP 800-90A CTR_DRBG Reseed Critical Function Test
- SP 800-90A CTR_DRBG Uninstantiate Critical Function Test

2.9.4 Self-Test Failure Handling

Upon failure of the conditional firmware load test, the module enters a “Soft Error” state and disables all access to cryptographic functions and CSPs. This is a transitory error state, during which the error status is recorded to the system log file and/or event audit log file. Upon failure of this self-test, the CO may choose to reject or continue with the firmware load. Rejecting the load will abort the load process, clear the error condition, and the module continues normal operations with the currently-loaded firmware. Choosing to continue will load the firmware, clear the error condition, and the module continues operating with the currently-loaded firmware until the next reboot.

Upon any other self-test failure, the module goes into “Critical Error” state and disables all access to cryptographic functions and CSPs. All data outputs are inhibited, and a permanent error status will be recorded to the system log file and/or event audit log file. The task that invoked the failed self-test will be suspended, and the current operation will not complete. The management interfaces will not respond to any commands while the modules are in this state. The CO must reboot the module to clear the error condition and return to a normal operational state.

2.10 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 7000 Session Border Controller meets overall Level 1 requirements for FIPS 140-2. The sections below describe how to ensure that the module is running securely. Please note that physical access to the module shall be limited to authorized operators only.

3.1 Initial Setup

The module is delivered in an uninitialized factory state, and requires first-time configuration in order to operate in its FIPS-Approved mode. Physical access to the module shall be limited to the Crypto Officer, and the CO shall be responsible for putting the module into the Approved mode. The following sections provide the necessary step-by-step instructions for the secure installation of the SBC device, as well as the steps necessary to configure the module for its FIPS-Approved mode of operation.

3.1.1 SBC Hardware Installation and Commissioning

In order to setup the SBC, the following steps should be performed by an authorized CO:

1. Before unpacking the SBC from the shipping container, examine the shipping container for evidence of damage. If any such damage exists, indicate that on the shipping document of the carrier and contact Sonus Networks, Inc. immediately for instructions.
2. Retain the packing list. Make sure all the items on the list are present including all the components of the universal rack mount kit that is shipped with the module.
3. Follow the instructions in *"Sonus SBC 7000 Series 5.0 Hardware Install Guide"* to install Rack Mount Kits, SBC Chassis, Front Bezel, and Cables.

Once these steps have been completed, the SBC hardware is considered to be installed and commissioned.

3.1.2 SBC Firmware Installation and Configuration

The next steps are to configure the firmware and management ports and to install the SBC application software. Please follow the detailed instructions in *"Sonus SBC 5000 & 7000 Software Installation Guide"* for configuring, installing, and upgrading the SBC 7000 application, or the following instructions shall be followed by the CO:

1. Connect your PC/Laptop via an Ethernet cable to the Ethernet Field Service Port (FSP) provided by the BMC of the appliance.
2. Configure your PC with an IP address on the "169.254.77.x" subnet.
3. Type the pre-configured IP address "169.254.77.1" in a web browser to connect to the BMC.
4. Configure the real BMC IP address in BMC configuration screen to replace the initial address "169.254.77.1".
5. Disconnect the PC/Laptop from FSP. Connect the FSP port to the router on LAN segment for out-of-band management.
6. Connect a PC to the IP network that can access the BMC IP address.

7. Configure the network management interface from the BMC GUI and connect the management cables to the router. Disconnect your PC from the BMC and connect to the IP network that can reach the management IP address range.
8. Launch the Platform Manager (PM) from the BMC either by clicking the link from the BMC or by typing the ***https://<mgtport_ip>:444*** in the web browser.
9. Install the SBC 7000 Series application software using the Platform Manager. For stand-alone installation and configuration guide, see section "*Sonus SBC Portfolio 5.0 Documentation Set*".

After successful installation, configure the module per the configuration instructions in the "*Sonus SBC Portfolio 5.0 Documentation Set*" document. Once the network settings are correctly configured for the module, continue to Section 3.1.3 in this document to configure SBC module for the FIPS-Approved mode.

3.1.3 SBC FIPS-Approved Mode Configuration and Status

During the initial setup of the SBC, as described in section 3.1 above, it is the responsibility of the Crypto Officer to enable FIPS mode during the SBC initial configuration. To set the FIPS mode to enabled via CLI after logging in, the CO shall run the set of CLI commands documented in "*Sonus SBC Portfolio 5.0 Documentation Set*" where it ends with commands:

- a. *set system admin <system name> fips-140-2 mode enabled*
- b. *commit*

After completion of the above steps the system will reboot. After this reboot, and on all subsequent reboots, the module is in its FIPS-Approved mode of operation.

At any point of time, the status of the module (i.e. FIPS Mode status) can be viewed on the CLI management interfaces by performing the following steps:

- a. *show configuration system admin <systemName> fips-140-2 mode -> "mode enabled"*

The status of the module can also be viewed using EMA GUI navigator.

3.2 Crypto Officer Guidance

The Crypto Officer shall receive the module from Sonus via trusted couriers (e.g. United Parcel Service, Federal Express, and Roadway). On receipt, the Crypto Officer should check the package for any irregular tears or openings. Prior to use, the Crypto Officer shall perform physical inspection of the unit in accordance with the procedure described in section 3.1.1 and if there are any signs of damage, the Crypto Officer should immediately contact Sonus.

The SBC supports multiple Crypto Officers. This role is assigned when the first CO logs into the system using the default username and password. The CO is required to change the default password as part of initial configuration. Only the CO can create other operators and configure the SBC module to operate in FIPS-Approved mode.

3.2.1 Management

Once installed, commissioned, and configured, the Crypto Officer 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 3.1.3 and Section 3.2 above for guidance that the Crypto Officer must follow for the module to be considered running in a FIPS-Approved mode of operation. The Crypto Officer should monitor the module's status regularly. If any irregular activity is noticed, or the module is consistently reporting errors, customers should consult "*Sonus SBC Portfolio 5.0 Documentation Set*" document to resolve the issues. If the problems cannot be resolved through these resources, Sonus customer support should be contacted. The CO must ensure that the key type and size requirement matches those specified in Table 8 above and the CO password is at least 8 characters in length.

For details regarding the management of the module, please refer to the "*Sonus SBC Portfolio 5.0 Documentation Set*".

3.2.2 Zeroization

There are many CSPs within the module's cryptographic boundary including symmetric key, private keys, public keys, and login passwords hashes. All ephemeral keys used by the module are zeroized on reboot, power cycle, or session termination. CSPs reside in multiple storage media including the SDRAM and system SSD. Ephemeral keys are zeroized when the module is rebooted or sessions are terminated. Other keys and CSPs, such as CDB-key, that is stored on the SSD of the module can be zeroized by using commands via EMA or CLI. The zeroization of the CDB-key renders other keys and CSPs stored in the non-volatile memory of the CDB useless, thereby, effectively zeroizing them. The public key used for the firmware load test is stored in a file in the flash file system, and cannot be zeroized. Reinstallation of the firmware also erases all the volatile and non-volatile keys and CSPs from the module.

The commands that can be used over CLI and EMA to zeroize keys and CSPs are:

CLI: *request system admin <systemName> zeroizePersistenKeys*

EMA: *All -> System ->Admin -> <systemName>-> Admin Commands-> zeroizePersistenKeys*

3.2.3 Status Monitoring

On the first power up, the module is, by default, in non-Approved mode of operation. During initial configuration and setup, the module is explicitly set to operate in the FIPS-Approved mode of operation. An authorized user can access the module via the CLI or the EMA and determine the FIPS-Approved mode of the module.

Detailed steps and procedure required to determine whether the module is operating in FIPS-Approved mode or not can be found in the "*Sonus SBC Portfolio 5.0 Documentation Set*", which is made available through a secure customer portal after purchase.

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 Usage Policies

This sections notes additional policies below that must be followed by module operators:

- As noted above, operator access to the BMC is provided over two external ports: an RS-232 serial port and a 1Gbps Ethernet port (called the BMC Field Service Port). The CO must use this port in order to accomplish the module’s initial setup and configuration as described in section 3.1.1 above. Beyond this, the BMC’s external ports shall not be used while the module is operational; use of the BMC’s external ports is prohibited while the module is operating in its FIPS-Approved mode. The CO shall ensure that operators do not directly access the module via the BMC’s external ports for any purpose.
- EC Diffie-Hellman with encryption strength less than 112 bits and Triple-DES keying option 2 shall not be used in the FIPS Approved mode of operation.
- In case the module’s power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- 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.

3.5 Non-FIPS-Approved Mode

During operation, the module can switch modes on a service-by-service basis between an Approved mode of operation and a non-Approved mode of operation. The module will transition to the non-Approved mode of operation when the “Establish SSH Session” service is invoked using the curves P-192, K-163, or B-163. The module transitions back to the Approved mode of operation upon the utilization of an Approved security function.

The module supports the Crypto Officer and User roles while in the non-Approved mode of operation. Table 9 below lists the service(s) available in the non-Approved mode of operation.

Table 9 – Non-Approved Services

Service	Operator		Description	Input	Output
	CO	User			
Establish SSH Session (non-compliant)	✓	✓	Establish remote session using SSH protocol	Command	Command response/ Status output

4. Acronyms

Table 10 provides definitions for the acronyms used in this document.

Table 10 – 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
BMC	Baseboard Management Controller
CA	Certificate Authority
CBC	Cipher Block Chaining
CDR	Call Data Record
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DC	Direct Current
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DNS	Domain Name System
DOS	Denial of Service
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
EC	Elliptical Curve
ECB	Electronic Codebook
ECC	Elliptical Curve Cryptography
ECDSA	Elliptical Curve Digital Signature Algorithm

Acronym	Definition
EMA	Embedded Management Application
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ENUM	E.164 NUmber Mapping
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HA	High Availability
HMAC	(Keyed-) Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IKE v1	Internet Key Exchange version1
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
KAT	Known Answer Test
KDF	Key Derivation Function
LED	Light Emitting Diode
MAC	Message Authentication Code
Mbps	Mega-bits per second
MD5	Message Digest 5
MKEK	Master Key Encrypting Key
N/A	Not Applicable
NAT	Network Address Translation
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PKCS	Public-Key Cryptography Standards
PM	Platform Manager
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Riverst, Shamir, and Adleman
RTCP	Real-time Transport Control Protocol

Acronym	Definition
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Small Form-Factor Pluggable
SFTP	SSH (or Secure) File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-Time Transport Protocol
SSD	Solid State Drive
SSH	Secure Shell
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Packet
USB	Universal Serial Bus
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>

