Sonus Networks, Inc.

SBC 5110 and 5210 Session Border Controllers

Hardware Version: SBC 5110 and SBC 5210
Firmware Version: 4.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.11

Prepared for:

Sonus Networks, Inc.
4 Technology Park Drive
Westford, MA 01886
United States of America

Phone: +1 855 GO SONUS
Email: sales@sonusnet.com
http://www.sonusnet.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the SBC 5110 and 5210 Session Border Controllers from Sonus Networks, Inc. This Security Policy describes how the SBC 5110 and 5210 Session Border Controllers (Hardware Version: SBC 5110 and SBC 5210 respectively; Firmware Version: 4.0) meet 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 National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the modules in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the modules. The SBC 5110 and 5210 Session Border Controllers are referred to in this document as the SBC, the cryptographic module, the module, or the modules. The SBC 5110 Session Border Controller is also referred as SBC 5110; the SBC 5210 Session Border Controller is also referred as SBC 5210.

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 (http://www.sonusnet.com/) contains information on the full line of products from Sonus Networks, Inc.
- 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 5110 and 5210 Session Border Controllers

2.1 Module Overview

Sonus Networks, Inc. (hereafter referred to as Sonus) is a leader in IP[1] networking with proven expertise in delivering secure, reliable and scalable next-generation infrastructure and subscriber solutions. The Sonus line of Session Border Controllers (SBCs) help mid-sized and large enterprises take advantage of cost-saving SIP[2] trunking services by securing their network from IP-based attacks, unifying SIP-based communications and controlling traffic in the network.

Sonus's SBC 5110 and 5210 Session Border Controllers feature 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 hardware within the device. For example, media transcoding on the SBCs is performed on an embedded DSP[3] 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 5110 and 5210 Session Border Controllers are high-performance air-cooled, 2U, IP encryption appliances that provide secure SIP-based communications with robust security, reduced latency, real-time encryption (VOIP[4] signaling and media traffic), media transcoding, flexible SIP session routing & policy management.

Figure 1 and Figure 2 below shows a picture of the SBC 5110 and 5210 Session Border Controllers respectively.

Figure 1 – Front View of SBC 5110

Figure 2 – Front View of SBC 5210

[1] IP – Internet Protocol
[2] SIP – Session Initiation Protocol
[3] DSP – Digital Signal Processor
[4] VOIP – Voice Over Internet Protocol

Note that the front panel of the SBC shows "SBC 5100" and "SBC 5200" to indicate that it is a member of the 5100 and 5200 family of products. An accompanying label affixed to the top rear corner of each chassis identifies a given SBC specifically as "SBC 5110"(shown in Figure 3) and "SBC 5210" (shown in Figure 4).

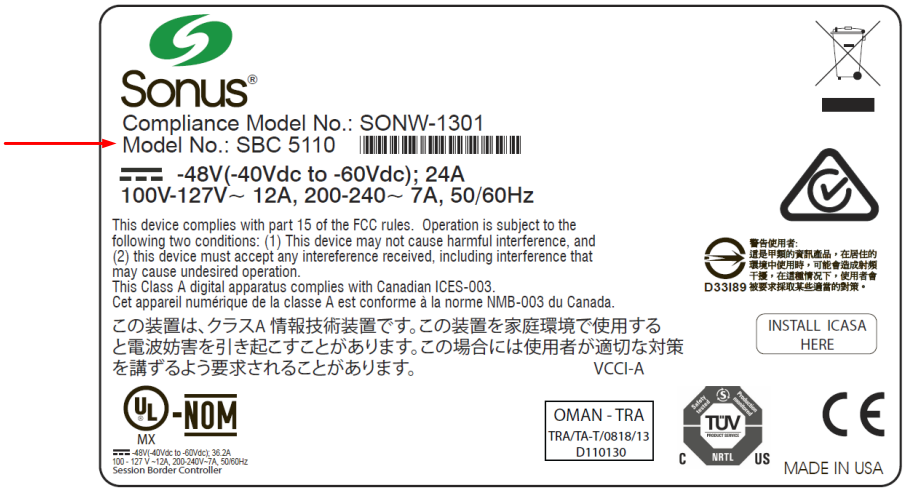


Figure 3 – Identifying Label for SBC 5110

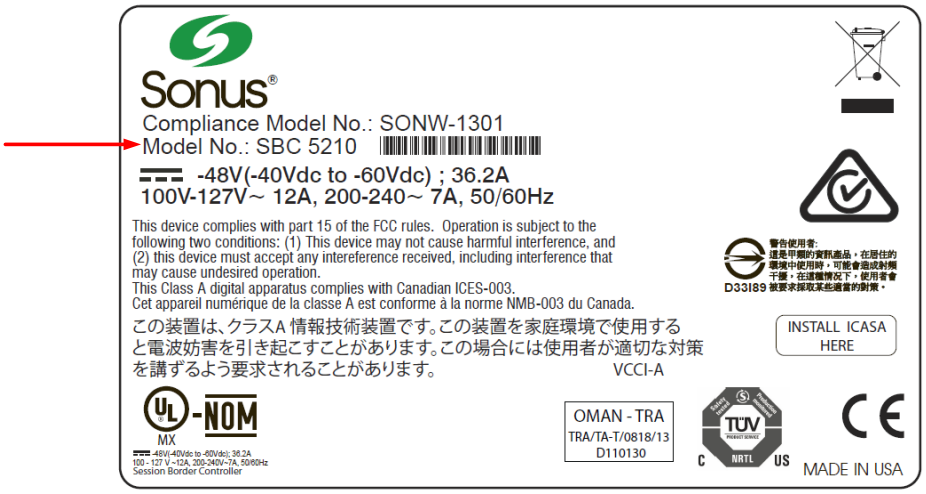


Figure 4 – Identifying Label for SBC 5210

The SBC is designed to fully address the next-generation needs of SIP communications by delivering embedded media transcoding, robust security and advanced call routing in a high-performance, small form-factor devices. The SBC 5110 can accommodate 250-10,000 call sessions while SBC 5210 can accommodate 500-64,000 call sessions. Some of the network and security features provided by the modules include:

- Session-aware firewall, split DMZ[5], bandwidth & QoS[6] theft protection, topology hiding, DoS[7]/DDoS[8] detection/blocking, rogue RTP[9] protection, IPsec[10] and TLS[11] encryption

[5] DMZ – Demilitarized Zone

- 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 NAT[12] traversal
- TLS, IPsec (IKEv1[13]) for signaling encryption
- Secure RTP/RTCP[14] for media encryption
- Support for large number of protocols including IPv4, IPv6, IPv4/IPv6 interworking, SSH[15], SFTP[16], SNMP[17], HTTPS[18], RTP/RTCP, UDP[19], TCP[20], DNS[21], ENUM[22], etc.
- Exceptional scalability even under heavy workloads
- Device management using encrypted and authenticated device management messages
- Controlled menu access and comprehensive audit logs
- Integrated Baseband Management Controller (BMC)

2.1.1 SBC Deployment

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 modules can be deployed as peering SBCs, access SBCs, or enterprise-SBCs (e-SBCs).

Management of the SBC 5110 and 5210 Session Border Controllers is accomplished via:

- SNMPv3[23] traps and polling, which is 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 EMA[24] and PM[25]) over Ethernet Management ports

These management interfaces provide authorized operators access to the modules for configuration and management of all facets of the modules 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 SBCs.

[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 Secuirty
[11] TLS – Transport Layer Secuirty
[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 – Domian Name System
[22] ENUM – E.164 NUmber Mapping
[23] SNMPv3 – Simple Network Management Protocol version 3
[24] EMA – Embedded Management Application
[25] PM – Platform Manager

Figure 5 below illustrates a typical deployment scenario of SBCs and the cryptographic boundary is shown by the red-colored dotted line.

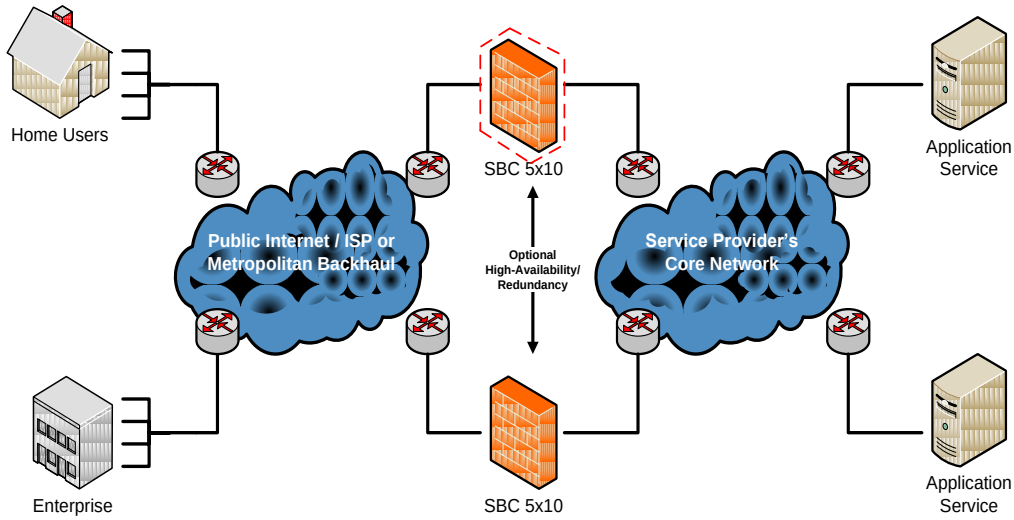


Figure 5 – Typical Deployment of SBCs in a Network

2.1.2 SBC FIPS 140-2 Validation

The SBC 5110 and 5210 Session Border Controllers are validated at the FIPS 140-2 section levels as 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	1
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[27]

[26] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[27] N/A – Not applicable

2.2 Module Specification

The SBC 5110 and 5210 Session Border Controllers are hardware cryptographic modules with a multiple-chip standalone embodiment. The cryptographic modules consist of firmware and hardware components enclosed in a secure, production grade metal case. The main hardware components consist of integrated circuits, processors, memories, SSD[28], flash, DSP, power supplies, fans, and the enclosure containing all of these components . The overall security level of the modules is 1. The cryptographic boundary of the SBC is defined around the SBC device which includes all the hardware components, firmware, and the metal case.

The SBC 5110 and 5210 Session Border Controllers use the FIPS-Approved algorithm implementations in firmware and hardware as listed in Table 2 below.

Table 2 – FIPS-Approved Algorithm Implementations in Hardware and Firmware

Algorithm	Certificate Number		
	Crypto Accelerator	Network Processor	Crypto Library
AES[29] in CBC[30], CTR modes (128-bit key)	-	#2644	-
AES in CBC, CFB[31] modes (128, 256-bit keys)	-	-	#2643
Triple-DES[32] in CBC mode (Three-Key)	-	-	#1586
SHA[33]-1	-	#2218	#2217
HMAC[34] using SHA-1	-	#1636	#1635
SHA-224, SHA-256, SHA-384, SHA-512	#2216	-	#2217
HMAC using SHA-224, SHA-256, SHA-384, SHA-512	-	-	#1635
RSA key generation (2048-bit)	-	-	#1354
RSA PKCS[35]#1 v1.5 signature generation (2048-bit), signature verification (1024, 2048-bit)	#1353	-	#1354
SP[36] 800-90A CTR_DRBG[37]	-	-	#412
CVL for Key Derivation Function	-	#125	#124
EC[38] Diffie-Hellman SP800-56A All NIST-Defined Curves	-	-	#124

NOTE: The EC Diffie-Hellman implementation includes support for curves (P-192, B-163, K163) that are non-compliant and disallowed for use in a FIPS-Approved mode of operation. Please refer to NIST SP 800-131A for details.

The modules use the FIPS-Approved SP 800-90A CTR_DRBG to generate cryptographic keys. The modules do 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 modules.

[28] SSD – Solid State Drive
[29] AES – Advanced Encryption Standard
[30] CBC – Cipher Block Chaining
[31] CFB – Cipher Feedback
[32] DES – Data Encryption Standard
[33] SHA – Secure Hash Algorithm
[34] HMAC – Keyed-Hash Message Authentication Code
[35] PKCS – Public-Key Cryptography Standards
[36] SP – Special Publication
[37] DRBG – Deterministic Random Bit Generator
[38] EC – Elliptical Curve

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

- RSA (key wrapping; 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)
- MD5 (used for firmware integrity test during power-up self-test)

Additional information concerning DSA, 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.

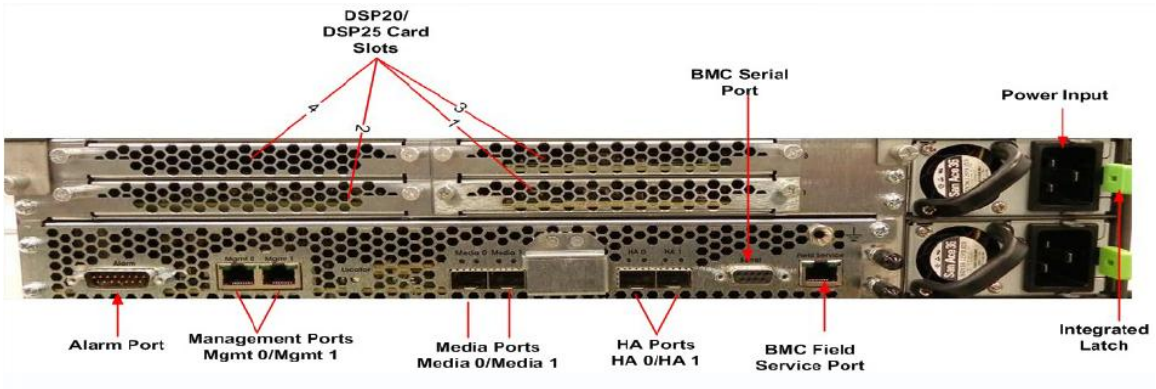
2.3 Module Interfaces

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 modules. These packets enter and exit the modules through the Ethernet Media, Management, and HA[39] interfaces. Control input consists of configuration or administration data entered into the modules 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 LEDs[40] and log information.

The physical ports and interfaces of the SBC 5110 and 5210 Session Border Controllers are depicted in Figure 1, Figure 2, Figure 6, and Figure 7. Table 3 lists the physical ports/interfaces available in the SBCs, and also provides the mapping from the physical ports/interfaces to logical interfaces as defined by FIPS 140-2.



[39] HA – High Availability
[40] LED – Light Emitting Diode

Figure 6 – Back Panel View of SBC 5110

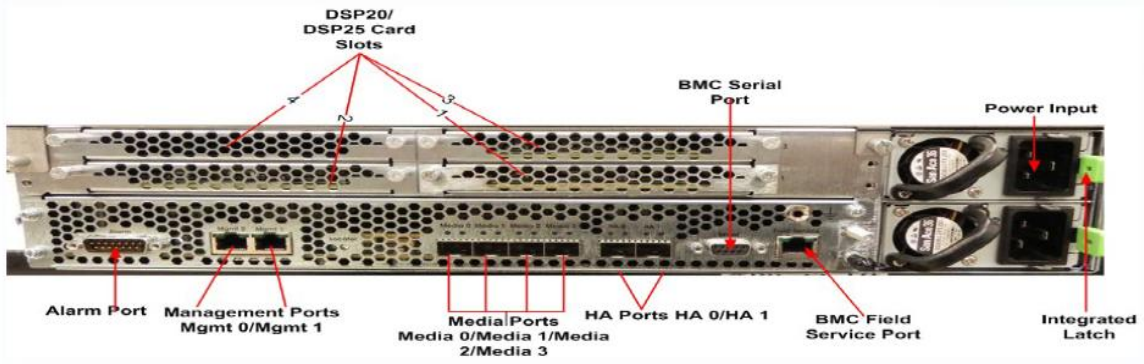


Figure 7 – Back Panel View of SBC 5210

Table 3 – Logical Interface Mapping

Physical Port/Interface	Quantity				FIPS 140-2 Logical Interface
	SBC 5110		SBC 5210		
Ethernet Media Port	BP[41]	2	BP	4	Data in, Data out
Ethernet Management Port	BP	2	BP	2	Data in, Data out Control in, Status out
Ethernet HA Port	BP	2	BP	2	Data in, Data out Control in, Status out
USB Port	FP[42]	1	FP	1	Data in
Power LED	FP	1	FP	1	Status out
Status LED	FP	1	FP	1	Status out
Active LED	FP	1	FP	1	Status out
Alarm LED	FP	1	FP	1	Status out
Locator LED	FP BP	1 1	FP BP	1 1	Status out
Power Supply LED	BP	2	BP	2	Status out
AC/DC[43] Power Input Connector	BP	2	BP	2	Control in
BMC Electrical	Internal	Various	Internal	Various	Control in, Status out

[41] BP – Back Panel
[42] FP – Front Panel
[43] AC/DC – Alternating Current/Direct Current

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

Each SFP[44] and Ethernet port on the SBC 5110 and SBC 5210 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, Figure 2, Figure 6, and Figure 7 above, both the modules have number of LEDs that indicate the state of the modules. The descriptions for the LEDs are listed in the Table 4 below.

Table 4 – SBC 5110 and 5210 Session Border Controllers LEDs Description

LED	Description	Color	Definition
Power LED	Indicator of power status for all voltages generated on the modules	OFF	The module is not powered.
		GREEN	The module is all powered on.
		AMBER	The module's BMC powers on and off when all power is off.
Status LED	Indicator of modules status	OFF	The module is not powered.
		GREEN	The module is powered and is healthy and operating normally.
		AMBER	The module is powered but unhealthy, one or more errors have occurred.
Active LED	Indicator of modules redundancy state	OFF	The module is in standby mode.
		GREEN	The module is active and protected.
		Blinking GREEN	The module is active and not protected.
		AMBER	The module is core dumping
Alarm LED	Indicator of modules 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.
Locator LED	Indicator of module Identifier	OFF	The module is not being identified.
		Blinking WHITE	The module is being user identified.
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.

[44] SFP – Small Form-factor Pluggable

2.4 Roles and Services

As required by FIPS 140-2, the modules support two roles that operators may assume: a Crypto-Officer (CO) role and a User role. The modules support role-based operator authentication. The keys and Critical Security Parameters (CSPs) listed in the 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.

2.4.1 Authorized Roles

There are two authorized roles in the module that an operator may assume: a Crypto-Officer (CO) role and a User role.

- Crypto-Officer – The CO is the administrator of the modules. Only a CO is authorized to use the default password of the module and can create other COs and Users and provision the SBC to operate in FIPS-Approved mode. The Crypto-Officers have access to all configuration, one or more CSPs, and the module's services. The CO services are provided remotely via the Web GUI over HTTPS and CLI over SSH.
- User – The User is limited to the read-only information and status activities which are a subset of CO services. The User cannot configure the modules except read system status and statistics.

2.4.2 Operator Services

Descriptions of the services available to the CO and the User are provided in Table 5.

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
Authenticate	✓	✓	Used to log into the module	Command	Status output	Password – X
Install, delete, and view 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

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Configure routing policy and control services	✓		Configure IP network parameters and profiles for signaling, media, call routing, call services, zone, IP ACL[45] rules, NTP[46] and DNS[47] 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
Add/Delete/Modify 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	None
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[48] 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
Perform Self Tests	✓		Perform on-demand self-tests	Command	Command response/ Status output	None
Network Diagnostics (e.g. ping)	✓	✓	Monitor connections	Command	Command response/ Status output	None

[45] ACL – Access Control List
[46] NTP – Network Time Protocol
[47] DNS – Domain Name System
[48] CA – Certificate Authority

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
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
Event Log	✓		View event status messages	Command	Command response/ Status output	None
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
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
Keying of CDB[49] key	✓		Generate CDB key	Command and parameters	Command response/ Status output	CDB key – W/X
Reset	✓		Reset the module	Command	Command response/ Status output	CSPs stored in SDRAM – W
TLS	✓	✓	Login to the module via Web interface and perform any of the services listed above	Command	Command response/ Status output	Password – X RSA Public key – R/X RSA Private key – X TLS Session key – R/W/X TLS Authentication Key – R/W/X
SSH	✓	✓	Login to the module remotely using SSH protocol and perform any of the services listed above	Command	Command response/ Status output	Password – R SSH Authentication Key – R/W/X SSH Session Key – R/W/X RSA Public key – R/X RSA Private Key – X

[49] CDB – Configuration Database

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
SNMPv3 Traps		✓	Provides system condition information	None	Status output	SNMPv3 Session Key – R/W/X SNMPv3 Authentication 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 list above require the operator to assume a role, and the module authenticates the role before providing any services.

2.4.3 Additional Services

In Approved mode, the modules 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 modules.

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 ephermeral 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
Data Processing	Encryption/decryption and authentication of media, signaling, and network traffic	None	None	RSA Private Keys – R/W/X TLS Session Key – R/W/X TLS Authentication Key – R/W/X SRTP[50] Session Key – R/W/X SRTP Authentication Key – R/W/X SRTCP[51] Session Key – R/W/X SRTCP Authentication Key – R/W/X

2.4.4 Authentication Mechanism

The modules support 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 atleast one upper-case and one lower-case letters, one numbers, and a special characters, allowing 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 modules.

[50] SRTP – Secure Real-time Transport Protocol
[51] SRTCP – Secure Real-time Control Protocol

Table 7 – Authentication Mechanism Used by the Module

Authentication Type	Strength
Password	The minimum length of the password is eight characters, with 95 different case-sensitive alphanumeric characters and symbols possible for usage. The chance of a random attempt falsely succeeding is 1: (95^8), or 1: 6,634,204,312,890,625. The fastest network connection over Ethernet Interface supported by the module is 100 Mbps. Hence, at most ($10 \times 10^7 \times 60 = 6 \times 10^9$ =) 6,000,000,000 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 : [95^8 possible passwords / ((6×10^9 bits per minute) / 64 bits per password)] 1: (95^8 possible passwords / 93,750,000 passwords per minute) 1: 70,764,846; which is less than 1:100,000 as required by FIPS 140-2.
Public Key Certificates	The modules support 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 1:2^{112} or 1: 5.19×10^{33}. The fastest network connection supported by the modules over Ethernet interfaces is 100 Mbps. Hence at most ($100 \times 10^6 \times 60 = 6 \times 10^9$ =) 6,000,000,000 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: (2^{112} possible keys / ((6×10^9 bits per minute) / 112 bits per key)) 1: (2^{112} possible keys / 53,571,428 keys per minute) 1: 96.92×10^{24}; which is less than 100,000 as required by FIPS 140-2.

2.4.4.1 Authentication Data Protection

The modules do 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 5110 and 5210 Session Border Controllers' production-grade enclosures. 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 modules are production grade with standard passivation.

2.6 Operational Environment

The operational environment of the modules 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 modules' 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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Config Database (CDB) Key	Triple-DES-CBC 168-bit key	Generated internally using DRBG	Never exits the module	Plaintext in SSD	Re-keyed over CLI or EMA , when appliance is reimaged, or over management command	Encryption of RSA Private key, Preshared secrets for RADIUS in CDB
SSH Symmetric Key	AES 128, 256-bit or Triple-DES 168-bit key	Diffie-Hellman key agreement	Never exits the module	Plaintext in RAM	Reboot or session termination	Encryption or decryption during SSH
TLS Session Key	AES-CBC 128, 256-bit key	Generated internally via FIPS-Approved DRBG or enters the module encrypted	Never exits the module	Plaintext in RAM	Reboot or session termination	Encryption or decryption of TLS communication
HMAC Key	Shared key generated via Diffie-Hellman key agreement	Generated internally via FIPS-Approved DRBG	Never exits the module	Plaintext in RAM	Reboot or session termination	TLS and SSH session packet authentication
SRTP Master Key	128-bit Shared secret	Externally generated, imported in encrypted form via a secure SIP/TLS session	Exits in encrypted format	Plaintext in RAM	Reboot or session termination	Peer Authentication, Session and Authentication keys derivation for SRTP session
SRTP Symmetric Key	AES-CM 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	32, 80-bit HMAC SHA1key	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)	Electronically entered by Crypto-Officer	Never exits the module	Stored in the CDB on SSD - encrypted	Command via CLI or EMA	Peer Authentication of RADIUS messages

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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
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	Internally generated using 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 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	Stored in the CDB on SSD - plaintext	Command via CLI or EMA	Used for SSH and SFTP key negotiation; 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; 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
EC DH public component	Public components of EC DH protocol	Internally generated	Output electronically in plaintext	Plaintext in volatile memory	Power cycle or host reboot	Used by calling application
EC DH private component	Private exponent of EC DH protocol	Internally generated	Never exits the module	Plaintext in volatile memory	Power cycle or host reboot	Used by calling application

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Privacy Key	AES-CFB 128-bit or Triple-DES 168-bit	Externally generated, imported in encrypted form via a secure TLS or SSH session	Never exits the module	Stored in the CDB on SSD - plaintext	Command via CLI or EMA	Encrypting SNMPv3 packets.
SNMPv3 Authentication Key	HMAC-SHA-1-96	Externally generated, imported in encrypted form via a secure TLS or SSH session	Exits in encrypted format when performing configuration backup	Stored in the CDB on SSD - plaintext	Command via CLI or EMA	Authenticating SNMPv3 packets.
Crypto-Officer 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 CO on CLI/EMA over encrypted session, changed password never exits the module	Plaintext (hashed[52]) on SSD and in RAM	Zeroized when the password is updated with a new one	Authenticating the Crypto-Officer
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 CO 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

[52] Passwords are hashed by the operating system and stored on the SSD. They are temporarily loaded into the memory for comparison during a login.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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 modules implement cryptographic algorithms using firmware (Crypto Library) as well as in the software and drivers that operate the hardware accelerators (Network Processor and Crypto Accelerator); and the modules perform various Self-Tests (Power-Up Self-Tests, Conditional Self-Tests, and Conditional Critical Function Tests) to verify their functionality and correctness. Upon any power-up self-test, conditional self-test, or critical function test failure, the modules go into "Critical Error" state and it disables all access to cryptographic functions and CSPs. All data outputs are inhibited upon a power-up, conditional, critical function self-test failure. 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 do not respond to any commands until the module is operational. The CO must reboot the modules to clear the error condition and return to a normal operational state.

2.9.1 Power–Up Self–Tests

The SBC 5110 and 5210 Session Border Controllers perform the following self-tests at power-up to verify the integrity of the firmware images and the correct operation of the FIPS-Approved algorithm implementation in the modules:

- Firmware integrity self-test using MD5 and HMAC-SHA-256
- Crypto Library with Crypto Accelerator algorithm tests:
  - RSA signature generation KAT
  - RSA signature verification KAT
- Network Processor driver algorithm tests:
  - AES encrypt KAT[53]
  - AES decrypt KAT
  - HMAC SHA-1 KAT
- Crypto Library algorithm tests:
  - AES encrypt KAT
  - AES 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
  - 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 modules' Management interface over SSH or HTTPS. Also, the modules can be

[53] KAT – Known Answer Test

made to perform power-up self-tests by disconnecting and reconnecting power connectors to the modules; and for this service, an operator is not required to assume an authorized role.

2.9.2 Conditional Self–Tests

The SBC 5110 and 5210 Session Border Controllers implement the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for the SP 800-90A CTR_DRBG (Crypto Library)
- Continuous Random Number Generator Test (CRNGT) for the NDRNG Entropy source (Crypto Library)
- RSA Pair-wise Consistency Test (Crypto Library with Crypto Accelerator)
- RSA Pair-wise Consistency Test (Crypto Library)
- Firmware Load Test using RSA signature verification (for OS, SonusDB, EMA, and SBC)
- EC Diffie-Hellman pairwise consistency test (Crypto Library)

2.9.3 Critical Function Tests

The SBC 5110 and 5210 Session Border Controllers implement 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 modules:

- 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

2.10 Mitigation of Other Attacks

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

3 Secure Operation

The SBC 5110 and 5210 Session Border Controllers meet overall Level 1 requirements for FIPS 140-2. The sections below describe how to ensure that the modules are running securely. Please note that physical access to the modules shall be limited to authorized operators only.

3.1 Initial Setup

The modules are delivered in an uninitialized factory state, and require first-time configuration in order to operate in their 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 "*Installing SBC 5000 System Hardware in SBC 4.0 Documentation Set – SBC 5000 Series*" 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 amd management ports and to install the SBC application software. Please follow the detailed instructions in "*Installing SBC 5000 Series Software in SBC 4.0 Documentation Set – SBC 5000 Series*" for configuring, installing, and upgrading the SBC 5x10 appplication, 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 5000 Series application software using the Platform Manager. For stand-alone installation and configuration guide, see section *"Installing SBC 5000 Series Application (ERE Configuration) in SBC 4.0 Documentation Set – SBC 5000 Series"*.

After successful installation, configure the module per the configuration instructions in the "*Configuring SBC 5000 Series in SBC 4.0 Documentation Set – SBC 5000 Series*" 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 "*Enabling SBC 5000 Series for FIPS 140-2 Compliance in SBC 4.0 Documentation Set – SBC 5000 Series*" 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 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 Crypto-Officer 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 modules 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 modules 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 *"Operations and Troubleshooting in SBC 4.0 Documentation Set – SBC 5000 Series"* 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 specificed in Table 8 above and the CO password is at least 8 characters in length.

For details regarding the management of the modules, please refer to the *"Operations and Troubleshooting in SBC 4.0 Documentation Set – SBC 5000 Series"*.

3.2.2 Zeroization

There are many CSPs within the modules' 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 modules 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 modules.

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

CLI: *request system admin <systemName> zeroizePersistenKeys*

EMA: *Navigator -> System ->Admin -> <systemName>-> zeroizePersistenKeys*

3.2.3 Status Monitoring

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

Detailed steps and procedure required to determine whether the module is operating in FIPS-Approved mode or not can be found in the *"Enabling SBC 5000 Series for FIPS 140-2 Compliance in SBC 4.0 Documentation Set – SBC 5000 Series"*, which is made available through a secure customer portal after purchase.

3.2.4 Additional Usage Policies

As noted above, the module includes an integrated BMC to facilitate initial setup and configuration. Additionally, the BMC monitors and controls the modules' power, cooling, and alarms, and presents system information to internal/external management agents via standard Intelligent Platform Management Interface (IPMI) 2.0 compliant data records. Operator access to the BMC is provided over two external ports: an RS-232 serial port and a 1Gbps Ethernet port.

The CO must use the BMC in order to accomplish the module's initial setup and configuration as described in section 3.1.1 above. Additionally, the BMC sends status signals to module LEDs for the monitoring of various environmental sensors on the module. Beyond this, the BMC 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.

As noted above in Table 2, the module's implementation of EC Diffie-Hellman supports non-compliant curves. In order to maintain FIPS compliancy, use of these curves is expressly disallowed while the module is operating in its Approved mode. These curves shall not be used for any purpose once the module has been installed and configured as described in the guidance above.

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 Non-Approved Mode

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

4 Acronyms

Table 9 below defines the acronyms used in this document.

Table 9 – 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
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
DC	Direct Current
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DMZ	Demilitiarized 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
EMA	Embedded Management Application
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference

Acronym	Definition
ENUM	E.164 NUmber Mapping
FIPS	Federal Information Processing Standard
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
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
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SDRAM	Synchronous Dynamic Random Access Memory

Acronym	Definition
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
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.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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