BS-500
Security Policy

Document *Version 1.6*

AudioCodes

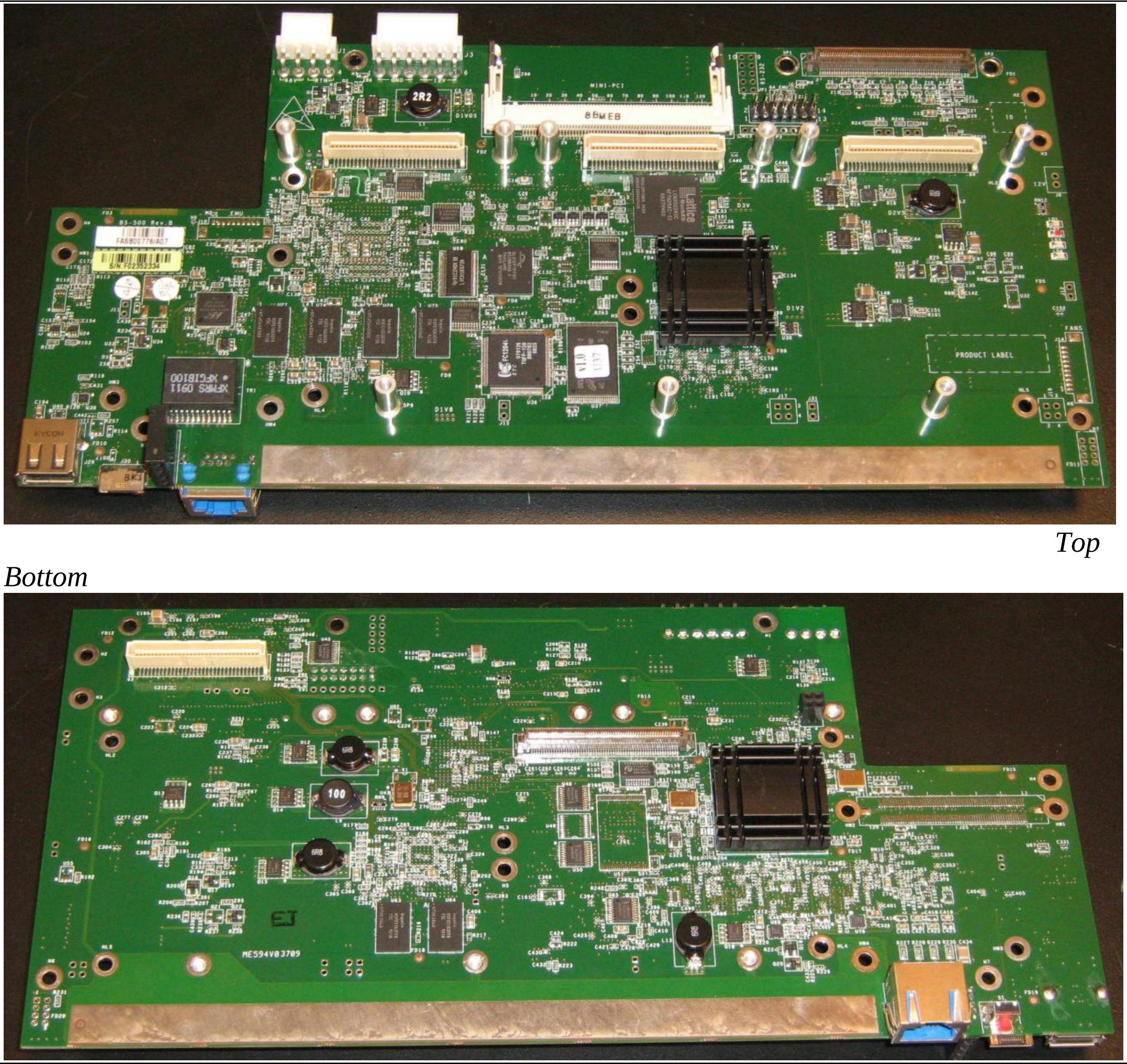
August 24, 2010

TABLE OF CONTENTS

1. Module Overview

The BS-500 is a multi-chip embedded cryptographic module whose primary purpose is to provide VoIP services as the main component of the MediaPack 500 VoIP gateway. The cryptographic boundary is defined as the perimeter of the PCB. The diagram below illustrates the cryptographic boundary.

Figure 1 – Image of the Cryptographic Module



Top

Bottom

The following table lists the module version numbers:

Product	**Hardware part number**	**Firmware version**
BS-500	FASB0885	5.80AM.023

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The following table lists the relevant configuration parameters and the values permitted for FIPS mode. To check if the device is operating in FIPS mode, verify the setting of all the parameters below using one of the available device management interfaces, e.g. SSH.

Parameter	*Permitted values*	*Notes*
TLS_FIPS140_Mode	1	Enables self-tests and Approved function implementation
TLSVersion	1	Disables SSL 2.0 and SSL 3.0
HTTPSRequireClientCertificate	1	Enables mutual TLS authentication in HTTPS
MutualAuthenticationMode	1	Mutual TLS authentication in SIP
SIPSRequireClientCertificate	1	Mutual TLS authentication in SIP
VerifyServerCertificate	1	Mutual TLS authentication in SIP
AUPDVerifyCertificates	1	Enables peer certificate verification for the Automatic Update Facility
HTTPSCipherString	'AES:3DES:!ADH'	Selects AES and Triple-DES ciphersuites for TLS and disables anonymous DH
TelnetServerEnable	0	Disables Telnet
HTTPSOnly	1	Disables plain-text HTTP
EnableSIPS	1	Enables SIP/TLS tunneling
SIPTransportType	2	Selects TLS as SIP transport
SSHRequirePublicKey	1	Force usage of RSA keys in SSH
SSHAdminKey	Non-blank key	RSA administrator key for SSH
DenyAuthenticationTimer	20 or higher	Limits failed authentication attempts to three per minute
EnableTPNCPSecurity	1	Disables TPNCP control
IniFileURL and CmpFileURL	https://... or ftps://…	Selects transport for the Automatic Update Facility
ActivityListToLog	afl, ard, spc, swu, dr, fb, naa (all except "pvc")	Selects which events are reported to Syslog. Parameter Value Change (PVC) logging is prohibited.
DisableRS232	1	Disables the serial console port
WebAuthMode	0	Selects HTTP basic authentication

In FIPS mode, the cryptographic module will support the following Approved algorithms:

- RSA with 1024 or 2048 bit keys for digital signature generation and verification
    - Algorithm certificate number: **556**
- AES with 128, 192, or 256 bit keys
    - Algorithm certificate numbers: **1114, 1169**
- Triple-DES with 128 or 192 bit keys
    - Algorithm certificate numbers: **811, 847**
- HMAC
    - Algorithm certificate numbers: **669**
- SHS
    - Algorithm certificate numbers: **1037**
- RNG - FIPS 186-2
    - Algorithm certificate number: **646**

The module also supports the following non-Approved algorithms:

- RSA key establishment, with 80-bit key strength
- Diffie Hellman Group 2, with 80-bit key strength
- HMAC-MD5 within RADIUS and TLS
- DES
- RC4
- MD5

  An NDRNG is used to provide seed data to the FIPS 186-2 RNG, the NDRNG is based on the output of 128 free-running oscillators. Clock jitter between oscillators is the source of uncertainty which drives the NDRNG.

The following security rules must be followed to maintain the Approved mode of operation. Detailed instructions are provided in the Operator Guidance document:

- TLS must always be used instead of SSL 2.0, 3.0
- Mutual authentication is required for TLS
- MD5, HMAC MD5 are not to be used unless mandated by an Acceptable Key Establishment Protocol
- Telnet must be disabled

- HTTPS must always be used instead of HTTP
- A TLS session must be enabled for SIP
- SNMPv3 keys must be entered in hexadecimal (password derivation must not be used)
- Keys must only be imported through a dedicated physical link or a secure tunnel
- Passwords shall be configured to be at least four characters
- The RADIUS secret shall be configured to be at least four characters
- The module shall be configured to restrict the number of failed authentication attempts to three per minute
- The serial port shall be disabled

Note: The module supports SSHv2 for crypto officer access, and does not support SSHv1.

3.1. Initial Device Set-up

The following instructions are a step-by-step guide to setting up a device in FIPS 140 Approved mode. The device is assumed to be in factory-default condition, and the environment secure.

a. Connect the device to a management PC using an Ethernet cross-over cable, establishing a private network .

b. Power up the device by connecting the electric cabling. BS-500 modules should be properly seated in a MediaPack 500 chassis. Consult the product's installation manual for related details.

c. Obtain the device’s IP address using a network monitor; the device will issue a GARP as part of the start-up process. Record this IP address for later use, and modify your PC’s IP configuration to match the device’s subnet (e.g. if the device has IP address 192.168.0.2, set your IP address to 192.168.0.5).

d. Wait for the device LEDs to turn green, indicating firmware start-up has completed.

e. Using a web browser, navigate to *http://xx.xx.xx.xx* where *xx.xx.xx.xx* denotes the device’s IP address recorded above. The default username and password are **Admin** (case-sensitive). Verify that the web interface functions correctly.

f. If your network provides PKI services, obtain the appropriate data from your security administrator and skip to the next bullet; otherwise follow the instructions below to establish a minimal PKI configuration (intended to serve as an example only; installation of the OpenSSL toolkit for Windows is assumed).

   Create a text file called **ca.cnf** and copy the following text into it:

```
[ req ]
default_bits           = 1024
distinguished_name     = req_distinguished_name
prompt                 = no
output_password        = password
[ req_distinguished_name ]
C                      = US
ST                     = New York
L                      = Poughkeepsie
O                      = Corporate
CN                     = Local CA
emailAddress           = test@corp.com
[ ca ]
default_ca  = CA_default            # The default ca section
[ CA_default ]
dir         = ./testCA        # Where everything is kept
certs       = $dir/certs            # Where the issued certs are kept
new_certs_dir     = $dir/newcerts         # default place for new certs.
database    = $dir/index.txt  # database index file.
certificate = $dir/cacert.pem       # The CA certificate
serial            = $dir/serial           # The current serial number
private_key = $dir/private/cakey.pem# The private key
RANDFILE    = $dir/private/.rand    # private random number file
default_md  = sha1                  # which md to use.
policy            = policy_anything
[ policy_anything ]
countryName       = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName  = optional
organizationalUnitName  = optional
commonName        = supplied
emailAddress            = optional
```

Issue these commands at your PC's prompt:

```
mkdir testCA
mkdir testCA\private
mkdir testCA\certs
mkdir testCA\newcerts
mkdir testCA\crl

openssl req -config ca.cnf -x509 -newkey rsa:1024 -keyout
testCA\private\cakey.pem -out testCA\cacert.pem -batch

copy /y testCA\cacert.pem root.pem
echo 01 > testCA\serial

copy /y nul testCA\index.txt

openssl req -config ca.cnf -new -keyout dev_pkey.pem -out server.csr -
nodes -batch

openssl ca -config ca.cnf -in server.csr -subj /CN=acDevice -days 3650 -
notext -passin pass:password -out dev_cert.pem -batch

openssl req -config ca.cnf -new -keyout pc_pkey.pem -out server.csr -
nodes -batch

openssl ca -config ca.cnf -in server.csr -subj /CN=acManager -days 3650
-notext -passin pass:password -out pc_cert.pem -batch

del server.csr

openssl pkcs12 -export -inkey pc_pkey.pem -in pc_cert.pem -out
pc_key.pfx -passout pass:1234
```

g. On the device's web interface, locate the navigation tree on the left pane and click "Full". Click "Security Settings" and select the "Certificates" page.

h. Upload the file **dev_cert.pem** as the device's server certificate.
Upload the file **root.pem** as the trusted root certificate.
Upload the file **dev_pkey.pem** as the device's private key.
Save the configuration to flash using the "Burn" button.

i. Import the generated certificates into your browser (e.g. in Firefox, click Tools - Advanced - Encryption - View Certificates); add **root.pem** as a trusted authority, and import **pc_key.pfx** as a personal certificate (in the example above, the import password is 1234).

<u>Notes:</u>

1. Make sure that SSL 2.0/3.0 usage is disabled in your browser.
2. Make sure that your browser selects your personal certificate automatically, when the server requests it.

j. Delete the files **dev_pkey.pem**, **pc_pkey.pem** and **pc_key.pfx** from your PC.

k. Add the module's IP and host name to your PC's **hosts** file, commonly `C:\WINDOWS\system32\drivers\etc\hosts`, e.g.:

```
127.0.0.1       localhost
192.168.0.2     acDevice
```

l. Using an SSH key-generation utility such as *PuTTYGen*, create an RSA 1024-bit key for SSH authentication (see the product reference manual for further instructions). Record the generated public key.

m. Create a text file called **device.ini** with the desired configuration, e.g.:

```
; Sample configuration
TLS_FIPS140_Mode = 1
TLSVersion = 1
HTTPSRequireClientCertificate = 1
MutualAuthenticationMode = 1
SIPSRequireClientCertificate = 1
VerifyServerCertificate = 1
AUPDVerifyCertificates = 1
HTTPSCipherString = 'AES:3DES:!ADH'
HTTPSOnly = 1
EnableSIPS = 1
SIPTransportType = 2
SSHServerEnable = 1
SSHRequirePublicKey = 1
SSHAdminKey = 'AAAAB3NzaC1yc2EAAAABJQAAAIEAorGT9I1XQC......'
DenyAuthenticationTimer = 20
EnableTPNCPSecurity = 1
ActivityListToLog = ''
DisableRS232 = 1
WebAuthMode = 0

NTPServerIp = 192.168.0.5
NTPServerUTCOffset = 10800
```

Notes:

1. The value of **SSHAdminKey** is the RSA key generated in the previous step.
2. The value of **NTPServerIp** is the IP address of your PC. Note that the module cannot function without proper NTP configuration; if you use Microsoft Windows, NTP services would be provided automatically.
3. The value of **NTPServerUTCOffset** is the time zone, in seconds; in this example, 10800 denotes a time zone of GMT+3.

n. Upload the file **device.ini** to the device, using the "Device actions" menu. Make sure to restart the device after loading the configuration. Verify that the new configuration is functional.
Note: Navigate your browser to https://acDevice in order to access the device through the configured host name.

o. If desired, upgrade to the latest FIPS 140 validated firmware image, using the Software Upgrade wizard. The wizard will reject any image not digitally signed by AudioCodes.

p. Using SSH, connect to the device's command-line interface.
Type the following command to verify FIPS status:

```
/SEC/FST
```

The device should display FIPS mode status ("ON") and a self-test output code of 0 ("passed").

q. Configuration is now complete. If desired, reconfigure the device to its production IP address (and production NTP server address) before powering off.

3.2. Non-Approved Mode of Operation

The previous section discussed initial set-up of the module, bringing it into Approved mode of operation. To return the device to Non-Approved mode of operation, the operator shall perform the zeroization procedure as described below.

The operator shall not change any of the configuration parameters discussed above, to a non-Approved value, while in Approved mode of operation.

3.3. Zeroization

To zeroize all security parameters, connect to the device using SSH and issue the command:

```
/SEC/ZEROIZE
```

The device will respond with the message "Zeroization complete" and reboot with default configuration.

4. Ports and Interfaces

The BS-500 provides the following physical ports and logical interfaces:

- Ethernet interface: Data In/Out, Control In, Status Out
- Telephony extension interfaces (Qty. 3): Data In/Out, Control In, Status Out, Power Out
- LAN extension interface: Data In/Out, Control In, Status Out, Power Out
- Reset Button: Control In
- Serial: Disabled
- Power: Power In
- LEDs (Qty. 8): Status Output, as follows:
  - Power LED
  - Ethernet activity LED
  - Boot failure LED
  - PCI activity LED
  - Packet transmit activity LED (orange)
  - Packet receive activity LED (red)
  - Device ready LED (green)
  - General failure LED (yellow)
- PCI port: N/A (reserved for future use)
- USB port: N/A (reserved for future use)
- Secondary CPU interface: N/A (reserved for future use)

5. Identification and Authentication Policy

Assumption of roles

The BS-500 support several distinct operator roles as defined in the table below. No feedback during authentication will weaken the strength of the authentication mechanism. The module does not retain the authenticated state across power cycles.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Role-based operator authentication	Digital Signature

(a.k.a. SIP agent)		Verification
Element Management System	Role-based operator authentication	Knowledge of a shared secret
Monitor	Identity-based operator authentication	Digital Signature Verification **plus** Username and Password
Administrator	Identity-based operator authentication	Digital Signature Verification **plus** Username and Password
Crypto Officer *(a.k.a. Security Administrator)*	Identity-based operator authentication	Digital Signature Verification **and/or** Username and Password
RADIUS Server	Role-based operator authentication	Knowledge of a shared secret

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The password is a minimum of four characters (maximum of 19 characters) selected from the set of 94-printable and human readable characters. The probability that a random attempt will succeed is 1/94^4, which is less than 1/1,000,000. The module will only allow three failed authentication attempts per minute, which ensures that the probability of multiple random authentication attempts being successful is less than 1/100,000.
Digital Signature Verification	The minimum signature size supported by the module is 1024 bits, which has an effective strength of 80 bits. The probability that a random attempt will succeed is 1/2^80, which is less than 1/1,000,000. The module is limited to 40 signature verifications per second, therefore the probability of multiple random authentication attempts being successful is about 1/(2^68), which is much lower than 1/100,000.
Knowledge of a Shared Secret	The smallest RADIUS shared secret that is supported is four characters chosen from the set of 94-printable and human readable characters. The probability that a random attempt will succeed is 1/94^4, which is less than 1/1,000,000. The module will only allow 60 failed RADIUS authentication attempts per minute, as there is a one second timeout after each failed attempt, which ensures that the probability of multiple random authentication attempts being successful is less than 1/100,000. SNMPv3 uses two shared secrets: a 16-byte encryption key (used for 128-bit AES) and a 20-byte authentication key (used for HMAC-SHA1). Both keys are entered in hexadecimal notation, by the operator. The probability that a random authentication attempt will succeed is therefore 1/(2^128), which is less than 1/1,000,000. The module is limited to 40 SNMP operations per second, therefore the probability of multiple random authentication attempts being successful is about 1/(2^116), which is much lower than 1/100,000.

Notes:

- The roles of **Monitor**, **Administrator**, and **Crypto Officer** are assumed when connecting to the module using mutually-authenticated TLS (hence digital signature verification is required); username and password are required after the digital signature verification, in order to distinguish between the three roles.
- The **Crypto Officer** role may be assumed when connecting to the module using SSHv2 and an RSA key (i.e. digital signature verification alone).
- Default authentication values exist when the module is new or in factory reset condition.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User *(SIP agent)*	• Establish VoIP Session • Terminate VoIP Session
Element Management System	• Security Settings • Restart • Lock/Unlock • Show Status • Configure Settings • FW Upgrade • Load Private Key • Self-Tests
Monitor	• Show Status
Administrator	• Restart • Lock/Unlock • Show Status • Configure Settings • FW Upgrade

	• Self-Tests
Crypto Officer *(Security Administrator)*	• Security Settings • Restart • Lock/Unlock • Show Status • Configure Settings • FW Upgrade • Load Private Key • Zeroize • Self-Tests
RADIUS Server	• Facilitate Authentication

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2 and is invoked by power cycling the module.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Device Private Key
- DH Private Key
- TLS Session Key
- TLS Integrity Key
- SSHv2 Encryption Key
- SSHv2 Integrity Key
- RADIUS Secret
- DRNG State
- SRTP Master Key
- SRTP Master Salt
- SRTP Encryption Key
- SRTP Integrity Key
- SRTP Salting Key
- SRTCP Encryption Key
- SRTCP Integrity Key
- SRTCP Salting Key
- Passwords
- SNMPv3 Authentication Key
- SNMPv3 Privacy Key

Definition of Public Keys:

The following are the public keys contained in the module:

- FW Verification Key
- Device Public Key
- DH Public Key
- DH Peer Public Key
- Peer Certificate
- Root Certificate
- SSHv2 administrator public key

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read (R)
- Write (W)
- Zeroize (Z)
- None (N)

Table 5 – CSP Access Rights within Services

Service/CSPs	**Device Private Key**	**DH Private Key**	**TLS Session Encryption Key**	**TLS Session Integrity Key**	**SSH Session Encryption Key**	**SSH Session Integrity Key**	**RADIUS Shared Secret**	**DRNG State**	**Passwords**	**SRTP Master Key**	**SRTP Master Salt**	**SRTP Encryption Key**	**SRTP Integrity Key**	**SRTP Salting Key**	**SRTCP Encryption Key**	**SRTCP Integrity Key**	**SRTCP Salting Key**	**SNMPv3 Authentication Key**	**SNMPv3 Encryption Key**
Establish VoIP Session	R	R W	R W	R W	N	N	N	R W	N	R W	R W	R W	R W	R W	R W	R W	R W	N	N
Terminate VoIP Session	R	R W	R W	R W	N	N	N	R W	N	R W	R W	R W	R W	R W	R W	R W	R W	N	N
Security Settings	R	R W	R W	R W	R W	R W	W	R W	W	N	N	N	N	N	N	N	N	R W	R W
Restart	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Lock/Unlock	R	RW	RW	RW	RW	RW	N	RW	N	N	N	N	N	N	N	N	N	R	R
Show Status	R	RW	RW	RW	RW	RW	N	RW	N	N	N	N	N	N	N	N	N	R	R
Configure Settings	R	RW	RW	RW	RW	RW	N	RW	N	N	N	N	N	N	N	N	N	RW	RW
FW Upgrade	R	RW	RW	RW	RW	RW	N	RW	N	N	N	N	N	N	N	N	N	R	R
Load Private Key	W	RW	RW	RW	RW	RW	N	RW	N	N	N	N	N	N	N	N	N	RW	RW
Facilitate Auth.	N	N	N	N	N	N	R	RW	R	N	N	N	N	N	N	N	N	R	R
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Self-Tests	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module supports a limited operational environment that only allows the loading of trusted firmware images signed by AudioCodes.

8. Self Tests

The cryptographic module shall perform the following tests:

A. Power up Self-Tests:

1. Cryptographic algorithm tests:

   a. Triple-DES Known Answer Test

   b. AES Known Answer Test

   c. RSA Sign/Verify Known Answer Test

   d. HMAC SHA-1 Known Answer Test

   e. FIPS 186-2 DRNG Known Answer Test

   f. SHA-1 Known Answer Test

Upon successful completion of the power-up self tests, the module displays the following message via syslog: "***FIPS140 self-test: All tests passed successfully***".

2. Firmware Integrity Test (32-bit Checksum)

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on the NDRNG and FIPS 186-2 DRNG

2. RSA Pairwise Consistency Test

3. Firmware Load Test (RSA signature validation)

At any time, the operator shall be capable of commanding the module to perform the power-up self-test by power cycling the module.

9. Physical Security Policy

Physical Security Mechanisms

The multi-chip embedded cryptographic module includes production-grade components compliant with Level 1 physical security requirements.

10. EMI/EMC

The AudioCodes MediaPack 500 gateway, a product which includes the BS-500 module, has been tested for conformance with FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A.

11. Mitigation of Other Attacks Policy

The module has not been designed to mitigate specific attacks beyond the scope of FIPS 140-2 requirements.