Avaya G250 and G250-BRI Branch Office Media Gateways w/FIPS Non-Proprietary Security Policy

Avaya Inc.

Revision Date: 14 December 2005

Version 1.2

TABLE OF CONTENTS

G250/G250-BRI Module Overview

The Avaya G250 and G250-BRI Branch Office Media Gateways w/FIPS (HW P/N 700356231, 700356223 Version 1.0, FW Version 24.16.0) are complete branch office business communications systems that integrate a TDM/VoIP telephony gateway, an advanced IP WAN router, and a PoE LAN switch into a compact (2U) chassis. Ideally suited for enterprise with distributed branch office locations of 2-10 extensions, the G250 and G250-BRI Gateways replace the complexity and cost of managing disparate key and voice systems with a survivable networked solution that is easy to deploy and can be administered from a central location

The G250 and G250-BRI share common hardware and firmware compatibility, other than that G250-BRI contains additional ISDN-B circuitry with 2 ISDN-BRI trunks plus 1 Analog trunk versus 4 Analog trunks in G250. The rules in this policy generally apply to all the above devices. Exceptions are explicitly rendered by device name, otherwise general cryptographic module notation is used.

The Avaya G250 and G250-BRI Branch Office Media Gateway w/FIPS are multi-chip stand-alone cryptographic modules encased in a commercial grade metal case. The cryptographic module provides status output via LEDs and logs available through its management interface. The cryptographic module provides network interfaces for data input and output. The cryptographic module provides a separate port for control input.

G250 cryptographic boundary includes all of the components within the physical enclosure of the chassis without any expansion modules plugged in. The figure (Figure 1) illustrates G250 cryptographic module:

Figure 1 – G250 Cryptographic module

G250-BRI module cryptographic boundary includes all of the components within the physical enclosure of the chassis without any expansion modules plugged in. The figure below (Figure 2) illustrates G250-BRI cryptographic module:

Figure 2 – G250-BRI Cryptographic module

1. Security Level

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

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

Table 1 - Module Security Level Specification

2. Modes of Operation

*2.1. **Approved mode of operation***

In FIPS mode, the cryptographic module supports the following algorithms:

a. RSA digital signature verification during firmware upgrades, and license file authentication. Support for RSA defined in PKCS#1 standard. RSA implementation as defined by ANSI X9.31 is not supported.

b. Triple-DES CBC (three key) for IKE encryption and IPSec, and serial number exchange

c. AES-CBC (128, 192, 256 bit) for IPSec and IKE encryption

d. SHA-1 for hashing download image digest, license file digest

e. HMAC SHA-1 for message authentication codes for IKE and IPSEC

f. DES CBC for encryption of IPSec, and IKE (only supported for communication with legacy systems) (transitional phase only – valid until May 19, 2007)

g. Diffie-Hellman key-agreement protocol (groups 2, 5, 14) used to derive IKE and IPSEC session keys.

The cryptographic module relies on the implemented deterministic random number generator (DRNG) that is compliant with X9.31 for generation of all cryptographic keys. The non-deterministic random seed generator is used for the periodic re-seeding of the PRNG.

The cryptographic module may be configured for FIPS mode via execution of the specified configuration procedure (Section 2.3).

The user can determine if the cryptographic module is running in FIPS vs. non-FIPS mode via execution of the **show running-config** command through the command-line-interface (CLI), and verification that the configuration meets the requirements specified in (Section 2.3), and

- Use the show system command and verify that "HW ready for FIP: Yes."
- Verify that both firmware banks contain firmware images that have been FIPS Approved. - Use the dir command. The output should show the FIPS Approved versions of the FW (which can be found at the following URL *http://www.csrc.nist.gov/cryptval/140-1/140val.all.htm*).

2.2. Non-FIPS mode of operation

The non-FIPS Approved algorithms implemented by the module are:

a. Diffie-Hellman (key agreement; key establishment methodology provides between 80–bits and 112-bits of encryption strength)

b. MD5

c. H.248 Link Encryption (use of PTLS and non-compliant AES in non-FIPS mode only, encryption algorithm)

d. Avaya Media Encryption (AEA for encryption/decryption)

e. SSH v2 (use of MD5, DH group 786-2048, non-compliant TDES, non-compliant DES in non-FIPS mode only, commercially available key establishment protocol)

f. HMAC-SHA-1 (used in non-compliant manner in SNMPv3 in non-FIPS mode only)

2.3. Entering FIPS Mode

To enter FIPS mode, the Crypto-Officer must follow the procedure outlined in the Table 2 below.

#	**Step Description**
1.	Log in to the device as default root/root user acting in Crypto-Officer role, through the local console port.
2.	Define PMI (Primary Management Interface) interface and execute device reset to activate PMI.
3.	Verify that the HW version of the module is of a FIPS Approved version.
4.	Verify that both firmware image banks contain firmware images, which have been FIPS Approved.
5.	Verify successful completion of power-up self-tests
6.	If more recent FIPS Approved Gateway image is available download the image using existing procedures for image download.
7.	If not installed download the Avaya License file with VPN feature activated
8.	Physically disconnect all network interfaces

#	**Step Description**
9.	Disable Signaling Encryption (H.248).
10.	Disable Avaya Media Encryption (SRTP, AEA, RTP/AES).
11.	Disable modem interfaces (USB, Console), Disable Modem Dial Backup
12.	Disable the recovery password mechanism
13.	Disable SSH service.
14.	Disable Chatter Test Plug application.
15.	Disable Survivability Application. Only holds true for G250. G250-BRI doesn't support Survivability.
16.	Configure other module configuration related parameters – VoIP, media, L2 switching, E1/T1.
17.	Determine which interfaces will be used for clear-text data, and which for encrypted data.
18.	Configure additional interfaces including the IP addresses of the interfaces.
19.	Change the password of the default Crypto-Officer. Define additional operators for Crypto-Officer, User, and Read-Only User roles as required. Remove all redundant users. For existing users define new CLI and SNMPv3 secrets.
20.	Configure Radius servers (primary/secondary), OSPF router peers, and PPPoE peer. Redundant OSPF peers need to be removed. New secret need to be assigned to Radius and PPPoE.
21.	Activate enhanced-security mode.
22.	Define an Access Control list that block packets with IP destination address of any of the module interfaces for the following protocols: TELNET, FTP, TFTP, SNMP. Activate the ACL on the inbound direction of all clear-text interfaces.
23.	Configure packet forwarding: static routes, dynamic routes learned via RIP and/or OSPF, and policy based routing lists.
24.	Configure IKE: Diffie-Hellman (group 2, group 5 or group 14), HMAC-SHA-1, AES, TDES (or DES for interconnection with legacy systems) and optional PFS parameters.
25.	Configure VPN peers (pre-shared keys). Redundant VPN peers need to be removed. For existing peers a new preshared keys need to be assigned.
26.	Configure IPSec transform-sets: HMAC-SHA-1, AES, TDES (or DES for interconnection with legacy systems).
27.	Define IPSec Crypto list(s) that provide encryption rules for traffic that needs protection. Make sure that packets with IP source address of any of the module interfaces for the following protocols: TELNET, FTP, TFTP, SNMP, are always ESP protected with TDES or AES encryption – null encryption is explicitly is NOT allowed for such flows.
28.	Activate the crypto-list(s) on all cipher-text interfaces. For flows that need to be encrypted even if directed to clear-text interfaces, apply crypto-lists to all interfaces.
29.	Save running config to startup config.

#	Step Description
30.	*FIPS-140-2 achieved*
31.	Re-connect network interfaces.

Table 2 – FIPS Approved mode configuration

3. Ports and Interfaces

3.1. G250 Ports and Interfaces

Figure 3 – G250 faceplate

The G250 cryptographic module provides the physical ports and logical interfaces defined in Table 3 below.

#	Interface	Qty	Logical interface definition	Comments
1.	ETH LAN POE	8	Data input, data output, status output, control input, power outout	Supports local area network connectivity.
2.	ETH WAN	1	Data input, data output, status output, control input	Supports wide area network connectivity.
3.	CCA	1	Power output.	Contact Closure Adjunct. Powers two contact-closure relays.
4.	Analog Line	2	Analog Phones.	Line 2 ceases to be a data input/output from the module and is directly connected to Analog

#	Interface	Qty	Logical interface definition	Comments
			Data input/output, power output	Trunk, providing a power interface, when an emergency state occurs: a) Power failure b) Failure to communicate with a call controller c) Firmware error state
5.	Analog Trunk	4	Analog Phone Trunks. Data input/output, power input	The Trunk ceases to be a data input/output from the module and is directly connected to Analog Line 2, providing a power interface, when an emergency state occurs: a) Power failure b) Failure to communicate with a call controller c) Firmware error state
6.	Console	1	Control inputs, Status output	Supports cryptographic module administration.
7.	USB	1	Control inputs, Status output, Power output	Supports cryptographic module administration for modem dial in connection. Disabled in FIPS Approved mode.
8.	Media Module Connectors	2	Data input, data output, status output, control input	Provide the ability to communicate using, Serial/TDM Data, Ethernet, PCI, CPU Device Bus, facilitates Power.
9.	AC Power Input	1	Power Input	Provides power to the module from an external source.
10.	Ground Connector	1	Ground	Provides power to the module from an external source.
11.	Reset Button	1	Control Input	Resets the device
12.	ASB Button	1	Control Input	When pressed with the reset button, cause the device to boot from an alternate firmware image bank
13.	System LEDs	4	Status Output	Indicates Power, Modem connection through Console interface, CPU activity, and Alarm state.
14.	LEDs on ETH WAN	2	Status Output	Link state and activity indication on the associated data interface
15.	LEDs on ETH LAN	2	Status Output	Link state and activity indication on the associated data interface

Table 3 – G250 Ports and Interfaces

3.2. G250-BRI Ports and Interfaces

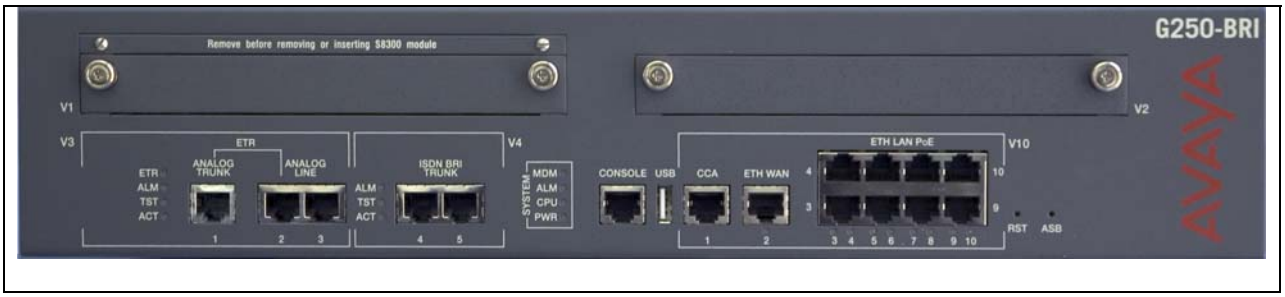

Figure 4 – G250-BRI faceplate

The G250_BRI cryptographic module provides the physical ports and logical interfaces defined in Table 4 below.

#	Interface	Qty	Logical interface definition	Comments
1.	ETH LAN POE	8	Data input, data output, status output, control input, power output	Supports local area network connectivity.
2.	ETH WAN	1	Data input, data output, status output, control input	Supports wide area network connectivity.
3.	CCA	1	Power output.	Contact Closure Adjunct. Powers two contact-closure relays.
4.	Analog Line	2	Analog Phones (Line1/Line2) Data input/output, power output	Line 2 ceases to be a data input/output from the module and is directly connected to Analog Trunk, providing a power interface, when an emergency state occurs: a) Power failure b) Failure to communicate with a call controller c) Firmware error state
5.	Analog Trunk	1	Analog Phone Trunks. Data input/output, power input	The Trunk ceases to be a data input/output from the module and is directly connected to Analog Line 2, providing a power interface, when an emergency state occurs: a) Power failure b) Failure to communicate with a call controller c) Firmware error state

#	Interface	Qty	Logical interface definition	Comments
6.	BRI Ports	2	BRI Phone Trunks. Data input/output	2 BRI Trunks (4 ISDN-B Channels) supporting ISDN based CO access.
7.	Console	1	Control inputs, Status output	Supports cryptographic module administration.
8.	USB	1	Control inputs, Status output, Power output	Supports cryptographic module administration for modem dial in connection. Disabled in FIPS Approved mode.
9.	Media Module Connectors	2	Data input, data output, status output, control input	Provide the ability to communicate using, Serial/TDM Data, Ethernet, PCI, CPU Device Bus, facilitates Power.
10.	AC Power Input	1	Power Input	Provides power to the module from an external source.
11.	Ground Connector	1	Ground	Provides power to the module from an external source.
12.	Reset Button	1	Control Input	Resets the device
13.	ASB Button	1	Control Input	When pressed with the reset button, cause the device to boot from an alternate firmware image bank
14.	System LEDs	4	Status Output	Indicates Power, Modem connection through Console interface, CPU activity, and Alarm state.
15.	LEDs on ETH WAN	2	Status Output	Link state and activity indication on the associated data interface
16.	LEDs on ETH LAN	2	Status Output	Link state and activity indication on the associated data interface

Table 4 – G250-BRI Ports and Interfaces

4. Identification and Authentication Policy

4.1. Assumption of roles

The definition of all supported roles is shown Table 5 below.

Role	Type of Authentication	Authentication Data	Description
Cryptographic -Officer (Admin User)	Identity-based operator authentication.	Username and Password. The module stores user identity information in an internal or an external Radius Server database.	The owner of the cryptographic module with full access to the services of the module.
User (Read/Write	Identity-based operator	Username and Password. The module stores user identity information in an internal or an external Radius Server	An assistant to the Admin User that has read/write access to a subset of

User)	authentication	database.	configuration and status indications.
Read Only User	Identity-based operator authentication	Username and Password. The module stores user identity information in an internal or an external Radius Server database.	An assistant to the Admin User that has read only access to a subset of module configuration and status indications.
Radius Client	Role-based operator authentication	Shared Radius secret. Gateway authenticates Radius server response by examining the MD5 hash of the shared secret, the request Authenticator, and other response values in a response message.	An entity authenticates to the module for the purpose of permitting/denying access to services.
OSPF Router Peer	Role-based operator authentication	Router peer Secret Authentication of OSPF protocol executed by examining the authentication field in OSPF packet carrying MD5 hash of the packet and the secret.	An entity authenticates to the module for the purpose of permitting/denying access to services.
PPPoE client	Role-based operator authentication	Chap/Pap Secrets Simple password authentication is used for PAP-based authentication. Gateway use MD5 function to hash the challenge and the secret value in the response message to PPPoE Server.	An entity that facilitates connection to the broadband access network using PPP over Ethernet protocol. PPPoE client can be attached only to WAN Ethernet port.
IKE Peer	Role-based operator authentication	IKE pre-shared keys.	An entity that facilitates IPSec VPNs.
Serial Number Peer	Role based authentication	TDES encrypted challenge.	Gateway exchanges its serial number with a Server to enable feature activation.

Table 5 - Roles and Required Identification and Authentication

4.2. Strengths of Authentication Mechanisms

All passwords used for role or identity authentication are accepting 94 ASCII codes. The authentication strength is shown in Table 6 below.

Role	Minimum password length	Probability of successfully authenticating	Probability of successfully authenticating in one minute
OSPF, PPPoE, Radius	6 characters	1/ 689,869,781,056	1 / 209,052
Crypto Officer, User, Read-Only User	8 characters	1 / 6,095,689,385,410,816	1 / 1,847,178,602

Serial Number Peer	32 bit challenge	1 / 4,294,967,296	1 / 357,913
IKE peer	13 characters	1/ 44,736,509,592,539,817,388,662,784	1/13,556,518,058,345,399,207

Table 6 – Authentication strength

5. Access Control Policy

5.1. Services

- *Enable FIPS mode:* configure the module for the Approved mode of operation.
- *Firmware Update:* load firmware images digitally signed by RSA-SHA1 (1024 bit) algorithm.
- *CSPs management:* edit IKE pre-shared keys, OSPF secrets, PPPoE secrets.
- *Users Management:* add and delete users Admin, Read/Write Users, Read Only Users. Radius Servers.
- *Module configuration:* configure networking capabilities including bypass capability.
- *Reset:* force the module to power cycle via a remote command.
- *Read all status indications:* obtain all statuses securely via IPSEC, console port and LEDs on the front panel of a Gateway. This service also reports about the status of the bypass capability. Bypass status is reported by CLI commands **show ip active lists crypto**, **show ip crypto list #**, **show crypto ipsec transform-set** #, available from the console and remote telnet.
- *Read subset of status indications:* obtain subset of statuses securely via IPSEC, console port and LEDs on the front panel of a Gateway. Bypass status is reported by CLI commands **show ip active lists crypto**, **show ip crypto list #, show crypto ipsec transform-set #** available from the console and remote telnet.
- *Module configuration backup:* backup non-CSP related configuration data via IPSEC.
- *Restore configuration:* restore configuration data.
- *Zeroization:* actively destroy all plaintext CSPs and keys.
- *IKE negotiation:* use DH, DES, TDES, AES, HMAC-SHA1, PRNG X9.31.
- *IPSec traffic processing:* use AES, DES, TDES, and HMAC-SHA1.
- *Serial number exchange service:* use encryption to prevent fraud of Avaya license activation.

- *OSPF routing*: authenticate and exchange routing control data with a peer OSPF router.
- *PPPoE service*: authenticate PPP connection over an Ethernet link.
- *Radius authentication:* authenticate communication between the module and a primary/or secondary Radius server.

Unauthenticated Services:

- *Show status*: provide the status of the cryptographic module – the status is shown using the LEDs on the front panel. Constantly lit CPU led indicates normal operation. Flashing CPU led indicates operation in error state.
- *Self-tests*: execute the suite of self-tests required by FIPS 140-2 during power-up not requiring operator intervention.
- *Zeroize*: destroy all plaintext secret parameters and cryptographic keys.

5.2. Roles and Services

Service	Crypto-Officer	User	Read Only User	Radius Client	IKE Peer	OSPF Router peer	PPPoE client	Serial Number Peer
Enable FIPS mode	X							
Firmware Update	X							
CSPs Management	X	X						
User Management	X							
Module configuration	X	X						
Reset	X	X						
Read all status indications	X							
Read subset of status indications	X	X	X					
Module configuration backup	X	X						
Module configuration Restore	X							
Zeroization	X							
IKE negotiation	X	X	X		X			
IPSec traffic processing	X	X	X		X			
Serial Number Exchange								X
OSPF routing						X		
PPPoE connection							X	
Radius authentication				X				

Table 7 – Services to Roles mapping

5.3. Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Key	**Description/Usage**
IKE Pre-shared Keys	IKE Pre-Shared key is used to establish the IKE SKEYID_d during pre-shared key authentication, as part of the commercially available IKE key establishment process that meet the requirements specified in FIPS PUB 140-2 Annex D.
HASH_I, HASH_R	Used for generation of SKEYID, SKEYID_d, SKEYID_a, SKEYID_e. Generated for VPN IKE Phase 1 key establishment.
IKE Pre-shared Session Key (SKEYID)	Generated for VPN IKE Phase 1 by hashing pre-shared keys with responder/receiver nonce.
IKE Ephemeral DH shared secret (g^ab)	Generated for VPN IKE Phase 1 key establishment.
IKE Ephemeral DH private key (a)	The private exponent used in DH exchange. Generated for VPN IKE Phase 1 key establishment.
IKE Session Phase 1 Secret (SKEYID_d)	Phase 1 key used to derive keying material for IPSec Sas.
IKE Session Phase 1 HMAC Key (SKEYID_a)	Key used for integrity and authentication of the ISAKMP SA.
IKE Session Phase 1 Encrypted Key (SKEYID_e)	Shared key used for extraction of encryption keys protecting the ISAKMP SA.
IKE Session Phase 1 TDES key	Key used for TDES data encryption of ISAKMP SA.
IKE Session Phase 1 DES key	Key used for DES data encryption of ISAKMP SA.
IKE Session Phase 1 AES key	Key used for AES data encryption of ISAKMP SA.
Noncei, Noncer	Phase 2 initiator and responder nonce.
IPSEC SA Phase-2 TDES key	Phase 2, basic quick mode
IPSEC SA Phase-2 DES key	Phase 2, basic quick mode
IPSEC SA Phase-2 AES key	Phase 2, basic quick mode
IPSEC SA Phase-2 HMAC key	Phase 2, basic quick mode
IKE Ephemeral Phase-2 DH private key	Phase 2 Diffie Hellman private keys used in PFS for key renewal.
IKE Ephemeral Phase-2 DH shared secret	Phase 2 Diffie Hellman shared secret used in PFS for key renewal.
User password	Used for password authentication of CLI users.
Root password	Used for authentication of default CLI user during first setup.

Key	Description/Usage
Radius Secret	Used for hashing password with MD5. One secret common to both primary and Secondary Radius server.
OSPF Secret	Used for authentication OSPF messages with the Peer OSPF routers. Secret exchanged hashed using MD5. One secret defined per peer router identity.
PPPoE CHAP/PAP Secret	Used for authentication to PPPoE server.
SNMPv3 user authentication password	SNMPv3 operator MD5 authentication password used for authenticating the User and Read-Only User roles.
Fixed Serial Number secret	The TDES key used for the serial number exchange protocol.
Ephemeral Serial Number secret	The TDES key used for the serial number exchange protocol.
X9.31 PRNG State	Internal state for X9.31 PRNG

Table 8 – CSPs and private keys

The following are the public keys contained in the module:

Key	Description/Usage
IKE Ephemeral DH Phase –1 public keys	Generated for VPN IKE Phase 1 key establishment.
IKE Ephemeral DH Phase –2 public keys	Generated for VPN IKE Phase 2 PFS key renewal.
Image download certificate (Avaya root CA RSA public key)	Used for authentication of software download. The Avaya Root certificate is hard-code in Gateway image and used directely for authentication of the chain of trust of the Avaya Signing Authority that is downloaded together with the software.
License download public key	Used for authentication of license file validity. The license signing authority public key is hard-code in Gateway image and used directely for authentication of the digital signature embedded in the license file.

Table 9 – Public keys

5.4. Definition of CSPs Modes of Access

Table 10 below defines the relationship between access to CSPs and the services. The modes of access shown in the table include:

- Read: the data item is read from memory.
- Write: the data item is written into memory.
- Zeroize: the data item is actively overwritten.

Key	Enable FIPS mode	Firmware Update	CSPs management	User Management	Module configuration	Reset	Read all status indications	Module backup	Restore	Zeroization	IKE negotiation	IPSec traffic processing	Read subset of status indications	OSPF routing	PPPoE Service	Radius Authentication	Serial Number Exchange
PRNG keys	*RWZ*					*ZW*				*Z*	*R*						
IKE Pre-shared Keys	*RWZ*		*W*		*Z*					*Z*	*R*						
Pre-shared Session Key (SKEYID)						*Z*				*Z*	*RW*						
Ephemeral DH private key						*Z*				*Z*	*RW*						
Ephemeral DH shared secret						*Z*				*Z*	*RW*						
HASH_I, HASH_R						*Z*				*Z*	*RW*						
IKE session Phase 1 Secret (SKEYID_d)						*Z*				*Z*	*RW*						
IKE Phase 1 HMAC Key (SKEYID_a)						*Z*				*Z*	*RW*						
IKE Session Phase 1 SKEYID_e						*Z*				*Z*	*RW*						
IKE Session Phase 1 TDES						*Z*				*Z*	*RW*						
IKE Session Phase 1 DES						*Z*				*Z*	*RW*						
IKE Session Phase 1 AES						*Z*				*Z*	*RW*						
IKE Phase 1 TDES key (SKEYID_e)						*Z*				*Z*	*RW*						
Nonce						*Z*				*Z*	*W*	*R*					
IPSEC SA Phase-2 TDES key						*Z*				*Z*	*W*	*R*					
IPSEC SA Phased-2 AES key	*WZ*					*Z*				*Z*	*W*	*R*					
IPSEC SA Phased-2 HMAC keys						*Z*				*Z*	*W*	*R*					
IPSEC SA Phased-2 keys per protocol						*Z*				*Z*	*RW*						

Key	Enable FIPS mode	Firmware Update	CSPs management	User Management	Module configuration	Reset	Read all status indications	Module backup	Restore	Zeroization	IKE negotiation	IPSec traffic processing	Read subset of status indications	OSPF routing	PPPoE Service	Radius Authentication	Serial Number Exchange
Ephemeral DH Phase-2 private key						*Z*				*Z*	*RW*						
Ephemeral DH Phase 2 shared secret						*Z*				*Z*	*RW*						
User password	*WZ*	*R*	*R*	*WZ*	*R*	*R*	*R*	*R*	*R*	*Z*			*R*				
Root password	*RW*	*RW*	*R*	*W*	*R*	*R*	*R*	*R*	*R*	*W**			*R*				
OSPF Secret	*WZ*		*WZ*		*Z*					*Z*				*R*			
Radius Secret	*WZ*		*WZ*							*Z*						*R*	
PPPoE Chap/PAP Secret	*WZ*		*W*		*Z*					*Z*					*R*		
SNMPv3 authentication password	*WZ*	*R*	*R*	*WZ*	*R*	*R*	*R*	*R*	*R*	*Z*							
Fixed Serial Number secret		*W*								*Z*							*R*
Ephemeral Serial Number secret						*Z*				*Z*							*RW*
IKE Ephemeral DH public keys						*Z*				*Z*	*RW*						
IKE Ephemeral DH Phase 2 public keys						*Z*				*Z*	*RW*						
Avaya root CA RSA public key		*RW*															
License RSA public key	*R*	*RW*															

Table 10– CSP Access Rights within Roles & Services

(*) – The root password is set back to a factory default value during zeroization.

6. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device does not support the loading and execution of un-trusted code. Avaya digitally signs firmware images of the crypto module using RSA. Through this signature, the crypto module verifies the authenticity of any update to its firmware image.

7. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. When exiting FIPS-140-2 mode, the Crypto-Officer shall zeroize the CSP.
2. The cryptographic module shall perform the Power up Self-Tests:
   - Cryptographic algorithm tests:
     - TDES Known Answer Test (DES KAT fulfilled in this test per IG9.2)
     - AES Known Answer Test
     - SHA-1 Known Answer Test
     - HMAC-SHA-1 Known Answer Test
     - DRNG Known Answer Test
     - RSA Known Answer Test
   - Gateway Software Integrity Test (32 bit CRC verification) and Booter Integrity Test (32 bit CRC verification).
   - Critical Functions Tests:
     - Non-Volatile Random Memory (NVRAM) Integrity test
     - EEPROM Integrity Test
3. The cryptographic module shall perform the Conditional Self-Tests:
   - Continuous Random Number Generator (RNG) test – performed on all RNGs supporting crypto activities in FIPS Approved mode. Done for PRNG x9.31 and Random Seed Generator.
   - Bypass Test
   - Firmware load test (RSA Signature Verification)
4. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
5. The module shall support concurrent operators and shall maintain separation of roles and services.
6. The users of the system can plug-in and use any Avaya Media Module that does not support cryptographic functionality without restriction.
7. Media modules with cryptographic functionality must be tested and validated separately against the requirements FIPS 140-2.

8. Physical Security Policy

8.1. Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade enclosure.

8.2. Operator Required Actions

There are no operator-required actions to maintain physical security.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Production-grade components and production-grade enclosure	N/A	N/A

Table 8 – Inspection/Testing of Physical Security Mechanisms

9. Mitigation of Other Attacks Policy

The FIPS 140-2 Area 11 requirements are not applicable because the cryptographic module has not been designed to mitigate specific attacks outside of the scope of FIPS 140-2.

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Table 9 – Mitigation of Other Attacks

10. References

- For more information on the FIPS 140-2 standard and validation program please see the NIST website at *http://csrc.nist.gov/cryptval/*
- For more information about Avaya ask your Avaya representative or see *http://www.avaya.com/*
- For more information about Avaya G250 Media Gateway ask your Avaya representative or see *http://www.avaya.com/gcm/master-usa/en-us/products/offers/g250_media_gateway.htm*

11. Definitions and Acronyms

AEA – Avaya Encryption Algorithm

AES – Advanced Encryption Standard

BRI – Basic Rate ISDN

CBC – Cipher Block Chaining

CCA – Contact Closure Adjunct

CLI – Command Line Interface

CNA – Converged Network Analyzer

DES – Data Encryption Standard

DH – Diffie-Hellman

DSS – Digital Signature Standard

FTP – File Transfer Protocol

HMAC – Hash Message Authentication Code

IKE – Internet Key Exchange

IP – Internet Protocol

ISDN - Integrated Services Digital Network

LAN – Local Area Network

KAT – Known Answer Test

OSPF – Open Shortest Path First

PFS – Perfect Forward Secrecy

PMI – Primary Management Interface

PPPoE – Point-To-Point over Ethernet

PTLS – Avaya Proprietary Transport Layer Security

RSA – Rivest Shamir Adelman Algorithm

SNMP – Simple Network Management Protocol

TFTP – Trivial File Transfer Protocol

USB – Universal Serial Bus

WAN – Wide Area Network