Avaya G450/G430 FIPS 140-2 Cryptographic Module

Non-Proprietary Security Policy

Document Version: 1.6

Date: April 25, 2023

Avaya, Inc.

12121 Grant St.
Thornton, CO
80241
www.avaya.com

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

AVAYA

Table of Contents

List of Tables

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

List of Figures

1 Introduction

The Avaya G450/G430 FIPS 140-2 Cryptographic Module is defined as a hardware module with a multi-chip standalone embodiment. The module is designated as a Limited Operational Environment under the FIPS 140-2 definitions. The following key hardware components host are found within the module:

- Media Gateway Processor and memory (Flash, EEPROM, RAM)
- DSP Media Processor and memory (RAM)
- Entropy Noise Source hosted on a PLD device
- Ethernet switch

For the remainder of this document, we will often refer to the Cryptographic Module as simply the "Module" or "module."

The primary function of the G450/G430 module is to operate as a VoIP media gateway in a telecommunications network, transcoding audio between circuit-switched (land line) telephones and trunks, and Voice-over-IP (VoIP) transmitted over IP networks.

The G450/G430 operates as a networked adjunct of Avaya's software product called Avaya Aura Communications Manager (Communication Manager). Communication Manager is configured with the specifics of telephones and trunks attached to the G450/G430, and through the ITU H.248 protocol, commands the media gateway to relay voice and voice-band data streams to off-gateway VoIP peers.

All networking and security configuration of the G450/G430 is performed through an authenticated CLI local to the media gateway.

The G450/G430 module provides FIPS 140-2 validated cryptography for use in:

- Encryption of H.248 control links over TLS connections to Avaya Aura Communication Manager
- Remote administration via SSHv2 and SNMPv3
- SRTP VoIP media encryption

Table 1 – Cryptographic Module Tested Configurations

Model	Hardware P/N	Firmware
G450	A. 700506955 B. 700506955 with 700501368	41.34.5
G430	A. 700512173 B. 700512173 with 700503274	41.34.5

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

The module is designed to meet FIPS 140-2 Level 1 overall as shown in Table 2.

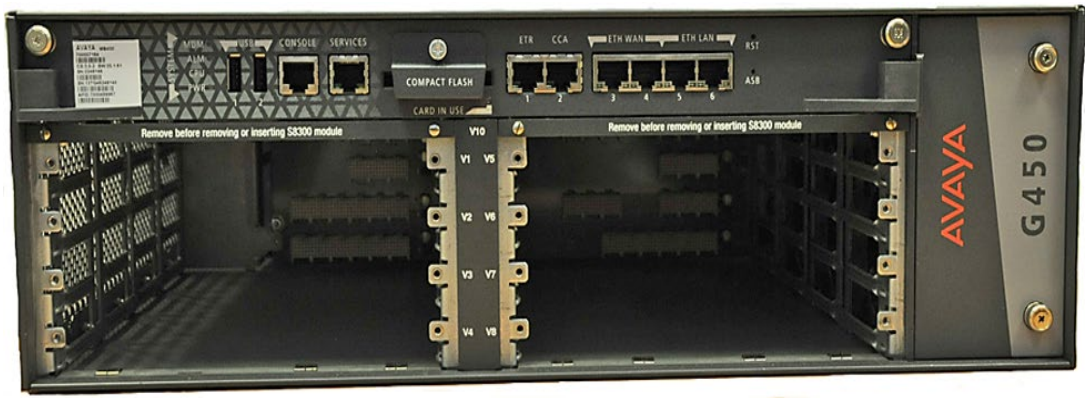
Table 2 – Security Level of Security Requirements

Area	Description	Level
1	Module Specification	1
2	Ports and Interfaces	1
3	Roles and Services	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Key Management	1
8	EMI/EMC	1
9	Self-test	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
	Overall	1

1.1 Introduction to the G450 Cryptographic Module

The physical forms of the G450 module in all configurations are depicted in Figure 1. The physical cryptographic boundary for the module is defined as the outer edge of the chassis excluding the hot-pluggable "Media Module" circuit packs which may populate slots V1-V8 to provide telephony interfaces supporting legacy PSTN equipment (such as analog stations and ISDN trunks). The G450 chassis may be optionally equipped with two internal power supplies. The rear view of Figure 1 shows a single power supply installed in the upper bay. The Module's ports and interfaces are listed in Table 3.

Figure 1 – G450 Front and Rear Faces



(Front)

(Rear)

Table 3 – G450 Ports and Interfaces

Port	QTY	Description	Logical Interface Type
Status LEDs	15	Status indicator lighting - MDM - ALM - CPU - PWR - Ethernet LEDs – 2 per port - Compact Flash in use	Status out
USB	2	USB ports	Data in, Data out
Console	1	Console serial port	Control in, Status out, Data in, Data out
Services	1	10/100M Local Ethernet port	Control in, Data in, Data out, Status out
Compact Flash	1	Compact flash	Data in, Data out
ETR	1	Emergency Transfer Relay	Status out
CCA	1	Contact closure	Status out
Ethernet WAN	2	10/100/1000M WAN Communications	Control in, Data in, Data out, Status out
Ethernet LAN	2	10/100/1000M LAN Communications	Control in, Data in, Data out, Status out
G450 Back Plane Media Module Connectors	8	TDM Voice/Data Communications, LAN Communications,10/100/1000M Ethernet LAN Communications.	Control in, Data in, Data out, Status out
RST	1	Reset (recessed)	Control in
ASB	1	Alternate Software Bank (recessed)	Control in
AC	1	AC Power	Power
GRD	1	Ground Connector	Power

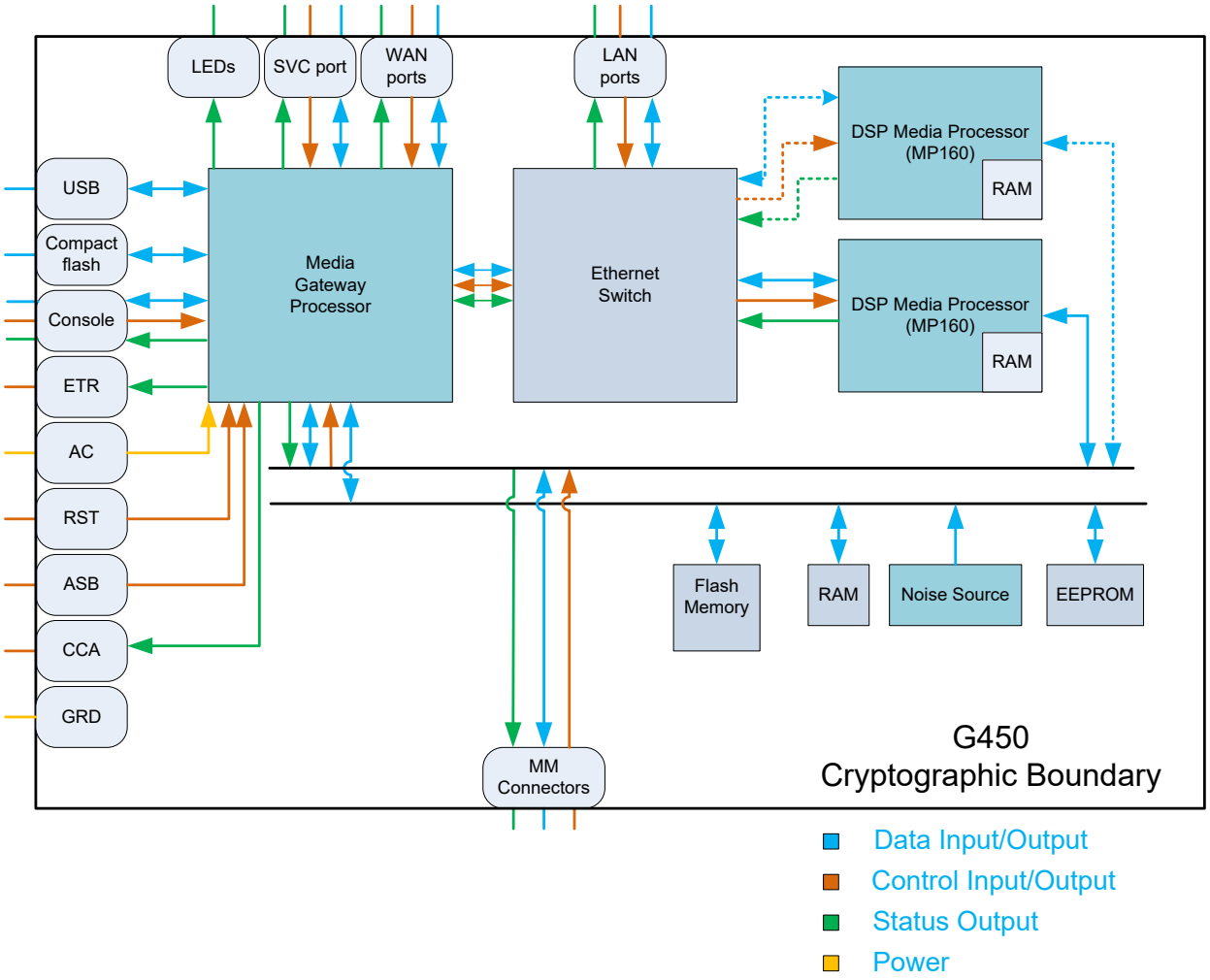
© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Figure 2 depicts the Module functional block diagram.

The Avaya G450 media gateway functions as an ITU-T H.248 media gateway subtending a Media Gateway Controller (Avaya's Communication Manager).

Figure 2 - G450 Cryptographic Module Block Diagram



1.2 Introduction to the G430 Cryptographic Module

The physical form of the G430 module is depicted in Figure 3. The physical cryptographic boundary for the module is defined as the outer edge of the chassis excluding the hot-pluggable "Media Module" circuit packs which may populate slots V1-V3 to provide telephony interfaces supporting legacy PSTN equipment (such as analog stations and ISDN trunks).

Figure 3 shows the G430 gateway module. This module has three media module card slots (V1, V2, V3). The module's ports and interfaces are listed in Table 4.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Figure 3 - G430 Front and Rear Faces

(Front)

(Rear)

Table 4 – G430 Ports and Interfaces

Port	QTY	Description	Logical Interface Type
Status LEDs	13	Status indicator lighting - MDM - ALM - CPU - PWR - Ethernet LEDs – 2 per port - Compact Flash in use	Status out
USB	2	USB ports	Data in, Data out
Services	1	10/100M Local Ethernet port	Control in, Data in, Data out, Status out
Compact Flash	1	Compact flash	Data in, Data out
ETR	1	Emergency Transfer Relay	Status out
CCA/ Serial Console	1	Contact closure and Serial Console	Control in, Status out, Data in, Data out
Ethernet WAN	1	10/100M WAN Communications	Control in, Data in, Data out, Status out
Ethernet LAN	2	10/100M LAN Communications	Control in, Data in, Data out, Status out
G430 Back Plane Media Module Connector	3	TDM Voice/Data Communications, 1G LAN Communications, 10/100/1000M Ethernet LAN Communications.	Control in, Data in, Data out, Status out
Expansion Out	2	Connectors for two Avaya EM200 expansion cabinets offering more Media Module slots	Control In, Data In, Data out, Status out
RST	1	Reset (recessed)	Control in
ASB	1	Alternate Software Bank (recessed)	Control in
AC	1	AC Power	Power
GRD	1	Ground Connector	Power

© 2023 Avaya, Inc. All rights reserved.

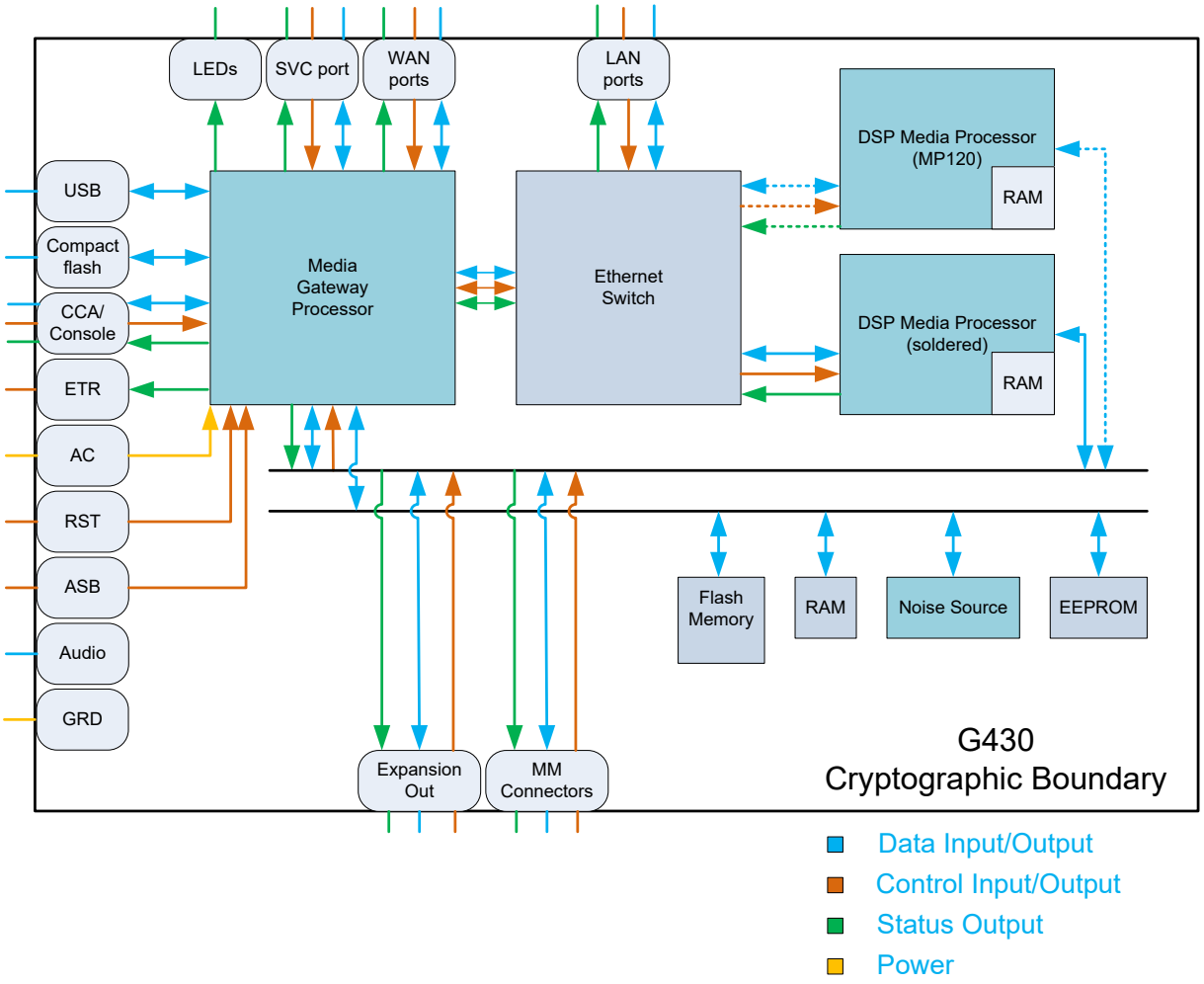
Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Audio	1	Music on Hold connector	This is non-operative with no supporting software driver

Figure 4 depicts the Module functional block diagram.

The Avaya G430 media gateway functions as an ITU-T H.248 media gateway subtending a Media Gateway Controller (Avaya's Communication Manager).

Figure 4 - G430 Cryptographic Module Block Diagram



1.3 Functional Components of the G450/G430 Cryptographic Module

The G450/G430 cryptographic module is comprised of three main components, which are all housed on the Supervisor board:

1) The Media Gateway Processor (MGP)
    a. The MGP uses several other internal components:
        i. EEPROM for semi-permanent data
        ii. Flash Memory for semi-permanent data

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

iii. Random Access Memory (RAM)
iv. Ethernet Switch

2) The DSP Media Processor
   a. The G450 must be equipped with at least one DSP processor plug-in circuit card with the marketing name “MP160” supporting 160 voice channels. A second MP160 is optional.
   b. The G430 comes equipped with a default DSP processor mounted on the Supervisor board. An optional DSP processor plug-in card with the marketing name “MP120” may be added, in which case the default DSP is automatically disabled.
   c. All DSP cards mount in sockets on the Supervisor board located within the module’s enclosure.
3) The Noise Source
   a. The Module’s Noise Source supplies noise to the Entropy Source used for seeding the DBRG. The noise source is an internal component soldered to the main circuit board located within the module’s enclosure.

1.4 Power Cycle Reset

The state of authentication and other dynamic session application information is not preserved over a power cycle (on-to-off-to-on) transaction.

1.5 Error States

The module defines three Error States which may be entered due to hard or soft operational failures. Entry into these Error States is externally indicated via Console messages and status LED flash patterns. The exit from an Error State may be automatic or require operator input.

These states are:

- Error State 1 – This state processes hard errors due to failures of the Module’s Power-up Self-Tests. Exit via operator selection of reboot or zeroization with reboot.
- Error State 2 – This state processes soft errors related to conditional self-test failures. Exit is through automatic reboot.
- Error State 3 – This state processes hard errors linked to critical function failures. Exit is automatic with immediate zeroization.

The module has a serial console cable which may be connected to a monitor for display of Error States. Alternatively, the LED lamps on the faceplate may be monitored for display of Error States.

Upon entering an Error State, the System CPU and ALM LED lamps will indicate the type of failure by providing a unique pattern of flashing and/or steadily lit lamps.

For viewing the LED lamps, the flash/blink rate is defined as follows:

- 0.25 seconds “on”
- 0.25 seconds “off”
- 1.25 seconds “off” for quiet time to complete the period, upon which the cycle will repeat.

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

- ***ERROR STATE1:***

a) This state is entered due to a failure of the boot-time Power-up Self Tests of cryptographic algorithms. Since these tests are based on static known answers, a failure in any test would probably recur with each reboot of the module and could eventually require a technician to diagnose the problem. For that reason, this state requires the operator to direct the module to either reset, or zeroize and reset. The latter action would be desirable if the module was to be scheduled for servicing.

b) On entry into Error State1, the Module will disable all data outputs and wait for operator input. This state is indicated by faceplate LED and Console messages (if the Console exists and is active):

❖ Display to the Console:

A recovery set of information will be displayed as follows:

G450 ERROR_STATE1 Recovery Screen

DSP0 Core3 SHA1 Test Failed

ERROR_STATE1 Recovery Services:

Enter <1> Exit ERROR_STATE1 and Retest

Enter <2> Critical Security Parameter Zeroization

Enter 1 or 2 to select a recovery service:

❖ Display on LEDs:

- MDM: continuous ON 15 seconds, OFF 15 seconds
- ALM: continuous ON-OFF flash
- CPU: continuous cycles of two ON-OFF flashes separated by 2.25s OFF
- PWR: solid ON if all power supplies are healthy, flashing otherwise

c) Exit from Error State1 requires operator input directing the gateway to either reset, or to zeroize and reset. This input can be provided by a menu choice at the active Console, or by depressing the recessed RST button during the MDM cycle:

- If RST is pressed while MDM is on, the action will be to zeroize and reset.
- If RST is pressed while MDM is off, the action will be to reset.

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

- ***ERROR STATE2:***
  a) This state is entered in response to a transient error observed by a conditional test in the module's Entropy Source or Deterministic Random Bit Generator (DRBG). The chances of such errors occurring are believed to be infinitesimally small and are unconditionally dealt with by an immediate disablement of all data outputs and reset of the gateway. This state is automatically exited upon reboot.

  b) Upon reboot the Module will pause during the Power-up Self-Test sequence to indicate it has passed through Error State 2. This indication consists of a message on the active Console and a LED flash-pattern.
     - ❖ Display to the Console:

       A recovery set of information will be displayed as follows:

Error state 2 is implemented as a spontaneous reboot. As the module reboots and performs its POST, it will indicate the reason for the reboot. For example:

```
Device is booting from bank:B
Target Name: vxTarget

Adding 80920 symbols for standalone.

FIPS POST TEST - STARTED
NVRAM POST Integrity Test OK
E2PROM POST Integrity Test OK
        FIPS Mode Conditional Test Failure Has Occurred
        Entropy Source - Adaptive Proportion Test Failed

FIPS Object Module POST Started
        Integrity Test OK
        DRBG AES-256-CTR DF Test OK
        DRBG AES-256-CTR Test OK
```

- ❖ Display on LEDs:
  - MDM: solid on
  - ALM: continuous on-off flash
  - CPU: continuous cycles of three on-off flashes
  - PWR: on if all power supplies are healthy, flashing otherwise

- ***ERROR STATE3:***
  a) This state is entered in response to an error with the test of "Critical Functions." These tests include EEPROM checksum test and NVRAM testing.
  - ❖ Display to the Console:

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

A recovery set of information will be displayed as follows:

Error State3 entry may occur at boot time when EEPROM and NVRAM sanity are tested during the POST phase:

```
E2PROM POST Integrity Test FAILED!
ENTER ERROR_STATE3
The G450 will now zeroize and delete all existing configuration data.
Once completed, the G450 will reset and attempt to provide service in
non-FIPS mode. FIPS mode may be enabled later if required.
```

❖ Display on LEDs:
- MDM: solid on
- ALM: continuous on-off flashes
- CPU: continuous cycles of four on-off flashes
- PWR: on if all power supplies are healthy, flashing otherwise

1.6 LED Patterns During Zeroization

- When zeroization may be performed by providing the following unique pattern
  - CPU LED: 2 blinks
  - ALM LED: flashing

- The Module will alternate in 15 seconds intervals as to when zeroization can and can't be perform for a period of 2 hours.
  - The MDM LED will indicate whether zeroization can be performed:
    - When zeroization can be performed:
      - MDM LED: on (for 15 seconds).
    - When zeroization cannot be performed:
      - MDM LED: off (for 15 seconds).
  - If the reset button is pressed when the MDM LED is on, both a reset and zeroization will be performed.
  - If the reset button is pressed when the MDM LED is off, only a reset will occur.
  - After 2 hours, the user will no longer be given the option to zeroize and only a reset may be performed. At this point in time, the MDM LED remains off.

1.7 Power-up Testing:

a) When the Module is performing Power-up Self-Test, the LED states will be as follows
   - CPU LED: flashing
   - ALM LED: on

b) If FIPS power-up testing completes successfully, the System CPU and ALM LEDS will resume to their normal operational state:
   - CPU LED: on
   - ALM LED: off

c) If Power-up Self-Test does not complete successfully, the Module will reset and enter the Error State 1 or Error State 3 depending on the nature of the failure.

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

1.8 Mode of Operation

The Module supports both Approved and non-Approved modes. The Module is configured to be in Approved mode using the CLI interface accessible through the serial console and SSH remote access.

To enter Approved Mode, the Crypto-Officer must follow the procedure outlined in Table 5 .

Table 5 – Procedure for Entering Approved Mode

#	Step Description
1.	Cryptographic Officer logs in to the device's serial console or SSH, using an administrative userid.
2.	Cryptographic Officer verifies that both firmware image banks contain FIPS-validated firmware images. The command is "show image version".
3.	Cryptographic Officer runs the following command "set fips-mode enable". Select "yes" once prompted.
4.	The system will automatically reset. Verify the power-up self-tests have passed, by viewing the console's interface display output or alternatively monitor the LEDs for status.
5.	Cryptographic Officer runs the following command "show fips-mode" to verify that it is enabled.

1.9 Determination of Approved Mode

The Module offers a CLI command 'show fips-mode' that allows an operator to invoke this command to verify that the product is operating in an Approved mode. The module will output the following:

```
FIPS Mode:  Enabled
```

1.10 Invocation of non-Approved Services

In Tables 18 and 19, these services are all available to the roles of Cryptographic Officer and to the User-R/W and User-R.

Tables 18 and 19 provides a summary of features resident in the Module which are inhibited when it's operating in Approved mode. These services are all available to the roles of Cryptographic Officer and to the User-R/W and User-R.

To invoke the non-approved mode, the command "set fips-mode disable" must be entered if the module has already been set to the FIPS mode of operation.

1.11 Approved and Allowed Algorithms

The Module implements the "Approved" cryptographic functions and the "Non-Approved but Allowed" cryptographic functions listed in the tables below. Note that Table 6 breaks up the algorithms into those supported by the DSP and those supported by the MGP. Also note that algorithms that are tested but not used by the module are not listed in these tables.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Table 6 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Reference	Mode	Functions	Parameter Size	Cert Number
DSP					
AES	FIPS 197, SP 800-38A	ECB, CTR	encrypt and decrypt	Key Size = 128, 256	A2079
CVL (SRTP KDF)	SP 800-135		SRTP KDF	Key Size = 128, 256	Vendor Affirmed
HMAC	FIPS 198-1		keyed hash	Output Length = 160 Key Size = 128	A2081
SHS	FIPS 180-4		hash	SHA-1	A2080
MGP					
AES	FIPS 197, SP 800-38A, SP 800-38D	ECB, CBC, OFB, CFB 1, CFB 8, CFB128, CTR	encrypt and decrypt	Key Size = 128, 192, 256	A2082
AES	FIPS 197, SP 800-38D	GCM[1]	Encrypt and decrypt with message authentication	Key Size = 128, 192, 256	A2085
CKG	SP 800-133r2	Section 4[2]	KeyGen	Key Size = 128	Vendor affirmed
CVL (SNMP KDF)	SP 800-135		SNMPv3 KDF		A2077
CVL (SSH KDF)	SP 800-135		SSHv2 KDF	Hash Length = SHA-1, SHA-256, SHA-512 Key size = 128, 192, 256	A2076
CVL (TLS KDF)	SP 800-135	TLS v1.0/1.1, v1.2	TLS KDF	Hash Length v1.2 = SHA-256, SHA-384	A2075
DRBG	SP 800-90A	CTR_DRBG w/AES-256 (DF enabled)	random bit generation	Entropy Input = 256 Nonce Input = 128	A2083
ECDSA	FIPS 186-4		KeyGen, KeyVer, SigGen, SigVer	Curve Length = P-256, P-384, P-521, Hash Length = SHA- 1, SHA-224, SHA-256, SHA-384, SHA-512 Note: SHA-1 can be used for signature verification only	A2084
ENT (P)	SP 800-90B		entropy source		N/A
HMAC	FIPS 198-1		keyed hash	Output Length = 160, 224, 256, 384, 512 Key size = Minimum 112 bits	A2086

[1] For TLS, the GCM implementation is compliant to IG A.5 scenario 1. It is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment. During operational testing, the module was tested against an independent version of TLS and found to behave correctly.

[2] The method follows Section 4, example 1. U is obtained from the approved DRBG within the module's boundary. Post-processing and XOR operations are not used, such that the bit string *B* = *U*.

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

KAS	SP 800-56Ar3	KAS-SSC with either TLS or SSH	Key agreement	Curve Length = P-256, P-384, P-521 Key Strength: 128-256 bits Modulus = 2048, 3072, 4096, 6144, 8192 Key Strength: 112-200 bits	KAS-SSC: A2078 CVL: A2076, A2075
KAS-SSC	SP 800-56Ar3	Ephemeral Unified DHephem	Key agreement	Curve Length = P-256, P-384, P-521 Key Strength: 128-256 bits Modulus = 2048, 3072, 4096, 6144, 8192 Key Strength: 112-200 bits	A2078
KTS	SP 800-38D	GCM	Key transport	Key Strength: 128 - 256	A2085
KTS	SP800-38A FIPS 198-1	AES-CBC + HMAC	Key transport	Key Strength: 128 - 256	AES: A2082 HMAC: A2086
RSA	FIPS 186-4 FIPS 186-2[iii]	PKCS1 v1.5 PSS	KeyGen, SigGen, SigVer	Modulus=2048, 3072 Note: 1024, 1536, and 4096 can be used for signature verification only Hash Length = SHA-224, SHA-256, SHA-384, SHA-512 Note: SHA-1 can be used for signature verification only	A2087
SHS	FIPS 180-4		hash	SHA- 1, SHA-224, SHA-256, SHA-384, SHA-512	A2088
Triple-DES	SP 800-67r2	ECB, CBC	decrypt[3]	Key Size = 168 Encryption Strength = 112	A2074

Table 7 – Non-Approved but Allowed Cryptographic Functions

Algorithm[iv]	Reference
AES PBKDF Triple-DES	[IG 1.23] Obfuscation of certificate and private key data using PKCS #12 (No Security Claimed). Uses the following: • Non-compliant KTS (AES or Triple-DES encryption without message authentication) • PBKDF to create keys for non-storage use (Non-Compliant).

[3] This algorithm is used only in decrypt-mode and does not implement nor is subject to the rekey requirements of IG A.13.

[iii] 186-2 is used for legacy signature verification only.

iv Note: The Keys and CSPs in these algorithms are not shared with Approved or Allowed algorithms per IG 1.23.

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

1.12 Protocols Allowed in Approved mode

The module supports the following protocols in Approved mode. These protocols have neither been reviewed nor tested by the NIST CAVP and CMVP. Operations involving elliptic curves are restricted to NIST curves (P-256, P-384, P-521).

Table 8 – Protocols Allowed in Approved Mode

Protocol	Key Exchange
SNMPv3	AES-128 in CFB mode; Authentication protocols truncate the HMAC output. When SHA1 hash is used, it uses HMAC-SHA-96 (per RFC3414).
SRTP	AES-128 and AES-256 with HMAC-SHA1-32 and HMAC-SHA1-80 authentication
SSHv2 server	(diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256), (aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc), (hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512), (ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521)
SSHv2 client	(diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256), (aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc), (hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512), (ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521)
TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS 1.2	TLS_ECDHE_ECDSA_AES_256_CBC_SHA384
TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC
TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS 1.2	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS 1.2	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS 1.2	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS 1.2	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384
TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS 1.2	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS 1.2	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS 1.2	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS 1.2	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256

Table 9 – Protocols Allowed in Non-Approved Mode

Protocol	Description
AEA	Avaya Encryption Algorithm used for legacy media encryption.

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

AES (Proprietary)	Legacy use of AES for media encryption without SRTP KDF.
IKEv1	Oakley groups 1 and 2. This is used in conjunction with the features of IPsec.
PTLS	Legacy H.248 channel encryption

1.13 Critical Security Parameters and Public Keys

All CSPs and public keys used by the Module are described in this section.

- All CSPs - except those that begin with SRTP – are used exclusively by MGP.
- SRTP-MEK and SRTP-MSALT are used by both
- All other SRTP-* parameters are used only by the DSP.

Please refer to the Legend that follows Table 11 for a complete list of the codes used in these tables.

Table 10 – Critical Security Parameters

Critical Security Parameters: G = Generated; S = Stored; I = Input; O = Output; Z = Zeroized						
Name	Description and usage	G	S	I	O	Z
AUTH-User-R	User Authentication Key. An 8 character or greater length password is used to authenticate read- only users to the module.	G1	S1, S2	I1	-	Z1, Z6
AUTH-User-RW	User Authentication Key. An 8 character or greater length password is used to authenticate read/write users to the module.	G1	S1, S2	I1	-	Z1, Z6
AUTH-CO	Crypto Officer Authentication Key. An 8 character or greater length password is used to authenticate COs to the module.	G1	S1, S2	I1	-	Z1, Z6
DRBG_Seed	Seed material used to seed or reseed the DRBG from the HW NDRNG	G2	S1	-	-	Z1, Z2
DRBG_State	The CTR_DRBG internal state	G3	S1	-	-	Z1, Z2
Master-EK	AES-128 key for backup/restore (direct output of DRBG)	G13	S1	-	-	Z1
SSH-DH-Priv	Diffie-Hellman private key for SSH	G13	S1	-	-	Z1, Z2
SSH-Host-Priv	SSH Private host key: RSA 2048/3072, ECDSA P-256/384/521	G4, G5	S1, S2	-	-	Z1, Z2
SSH-SENC	SSH Session Encryption Key; AES CBC/CTR 128/256 keys	G7	S1	-	-	Z2, Z3
SSH-SMAC	SSH HMAC key using SHA-1 or SHA-2	G7	S1	-	-	Z2, Z3
TLS-DH-Priv	TLS Diffie-Hellman private key for DH key establishment	G13	S1	-	-	Z2, Z5
TLS-Host-Priv	Device Private Key: RSA/ECDSA private key used for TLS client authentication	G12	S3	I3	-	Z1, Z6
TLS-MS	TLS master secret	G8	S1	-	-	Z2, Z5
TLS-PMS	TLS pre-master secret (DH and RSA key establishment)	G6, G13	S1	-	O2	Z2, Z5
TLS-SENC	TLS Session Data encryption key	G9	S1		-	Z2, Z5
TLS-SMAC	TLS HMAC authentication key using SHA-1 or SHA-2	G9	S1	-	-	Z2, Z5
SRTP-MEK	SRTP Master Key: AES128 and AES256	G12	S1	I2	-	Z2, Z4
SRTP-MSALT	SRTP Master Salt: 112 bits for AES128, AES256	G12	S1	I2	-	Z2, Z4

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

SRTP-SENC	SRTP Session Encryption Key: 128 bits for AES-128 and 256 bits for AES-256	G10	S1	-	-	Z2, Z4
SRTP-SMAC	SRTP Session Authentication Key using SHA-1 (160 bit)	G10	S1	-	-	Z2, Z4
SRTP-SSALT	SRTP Session Salting Key: 112 bits for AES-128, AES-256	G10	S1	-	-	Z2, Z4
SRTCP-SENC	SRTCP Session Encryption Key: 128 bits for AES-128 and 256 bits for AES-256	G10	S1	-	-	Z2, Z4
SRTCP-SMAC	SRTCP Session Authentication Key using SHA-1 (160 bit)	G10	S1	-	-	Z2, Z4
SRTCP-SSALT	SRTCP Session Salting Key: 112 bits	G10	S1	-	-	Z2, Z4
SNMP-PP	SNMPv3 pass phrase: (8-char minimum) privacy and authentication passwords	G1	S1, S2	I1	-	Z2, Z6
SNMP-SENC	SNMPv3 Data Encryption Key: AES CFB 128 bit key	G11	S1	-	-	Z2
SNMP-SMAC	SNMPv3 Authentication HMAC-SHA-1 key	G11	S1	-	-	Z2

Table 11 – Public Keys

Public keys: G = Generated; S = Stored; I = Input; O = output					
Name	Description and usage	G	S	I	O
CodeSign-Pub	Embedded trusted X.509v3 certificate for validation of signed firmware	G14	S2	-	-
EASG-Prod-Pub	EASG public key for technician access	G14	S2	-	-
SSH-DH-Pub	SSH Diffie-Hellman public key	G13	S2	-	O3
SSH-Host-Pub	SSH Public Host Key. RSA 2048/3072, ECDSA P-256/384/512	G4, G5	S1, S2	-	O3
TLS-DH-Pub	TLS Diffie-Hellman public key	G13	S2	-	O3
TLS-Host-Pub	Device Public Key: RSA/ECDSA public key associated with the module's X.509v3 end entity certificate	G12	S1, S2	I3	O1, O3
TLS-Trusted-Pub	Trusted X.509v3 root certificates: RSA/ECDSA public key used for TLS server authentication:	G12	S1, S2	I3	O1

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Legend for Codes Used in CSP Table 10 and Public Key Table 11

	Codes Used in CSP and Public Key Tables
Code	**Meaning**
G1	Generated by the user
G2	Entropy source compliant with SP 800-90B
G3	Derived from the seed per SP 800-90Ar1
G4	FIPS 186-4 compliant RSA key generation, using the internal CAVP validated DRBG
G5	FPS 186-4 compliant ECDSA key generation, using the internal CAVP validated DRBG.
G6	Diffie-Hellman shared secret generation
G7	Derived using SP 800-135 compliant SSHv2 KDF.
G8	Derived using SP 800-135 compliant TLS KDF (using Pre-master secret)
G9	Derived using SP 800-135 compliant TLS KDF (using master secret)
G10	Derived using SP 800-135 compliant SRTP KDF
G11	Derived using SP 800-135 compliant SNMP KDF
G12	Generated outside the module
G13	Generated from SP 800-90A DRBG output
G14	Generated prior to module construction, permanently embedded within module
S1	Stored in RAM.
S2	Stored in flash in plaintext.
S3	Stored in flash in obfuscated form.
I1	Input in plaintext
I2	Input in plain text through TLS channel • This includes cipher/mode and authentication algorithm “AES-CBC + HMAC, AES-GCM”.
I3	Input as PKCS#12-obfuscated plaintext through direct USB or encrypted SCP
O1	Output in plaintext public key
O2	Output encrypted as part of the protocol
O3	Output in plaintext as part of protocol
Z1	Zeroized by zeroizing error state or “zeroize” command
Z2	RAM copy zeroized by a system reboot
Z3	Destroyed by SSH session termination.
Z4	Destroyed by RTP session termination.
Z5	Destroyed by TLS session termination.
Z6	Destroyed via CLI erasure

1.14 Non-Approved and Allowed Algorithms in non-Approved Mode

The Module may be operated in non-Approved mode. In this mode, the Module may use non-validated cryptographic algorithms. Table 12 provides a list of “Non-Approved and Non-Compliant Cryptographic functions.

Table 12 – Non-Approved and Non-Compliant Cryptographic Functions

Algorithm	Functions
AES – MGP (non-compliant)	encrypt and decrypt
DES-MGP (non-Approved)	encrypt and decrypt
DRBG	random generation
ECDSA-MGP (non-compliant)	KeyGen, SigGen, SigVer
HMAC – MGP (non-compliant)	keyed hash
KAS-MGP (non-compliant)	Finite-field/ECC Diffie-Hellman
MD5-MGP (non-Approved)	hash
RSA-MGP (non-compliant)	KeyGen, SigGen, SigVer
SHA – MGP (non-compliant)	hash
Triple-DES-MGP (non-compliant)	decrypt

2 Roles, Authentication and Services

2.1 Roles and Authentication of Operators to Roles

The module supports the following types of usage roles.

- Security & Administration
  - Cryptographic Officer
- General Administration
  - User-R/W
  - User-R
- Troubleshooting
  - User-MTCE
- SNMP User
- Machine-Machine Management of Gateway
  - Avaya Aura Communication Manager Server (CM)

The module enforces the separation of roles using either identity-based or role-based operator authentication.

Table 13 – Roles and Authentication

Role Name	Role Description	Auth Type	Len (min)	PoFA	PoFA Per min
	SECURITY				
CO	Cryptographic Officer - administrative operators authenticated by username and password via direct console access or using SSH. This is currently named "Admin" in the gateway CLI command set. See Section 7 for a list of Security Rules.	Identity	8	$1/(94^8)$	$20/(94^8)$
User-MTCE	Maintenance technician. Logins for this role via SSH or direct console use a challenge-response authentication employing public key methods.	Identity	>300	$1/1.59 \times 10^{604}$	$20/1.59 \times 10^{604}$
	GENERAL ADMINISTRATION (User CLI Processing)				
User-RW	An assistant to the Admin User that has read/write access to a subset of configuration and status indications. The User-RW is authenticated by username and password via direct console access or using SSH.	Identity	8	$1/(94^8)$	$20/(94^8)$
User-R	An assistant to the Admin User that has read only access to a subset of module configuration and status indications. The User-R is authenticated by username and password via direct console access or using SSH.	Identity	8	$1/(94^8)$	$20/(94^8)$
	SNMP MANAGEMENT				
SNMP User	SNMPv3 network management user. This user can be configured to have different levels of access such as read only or read and write.	Identity	8	$1/(94^8)$	$(9x10^7)/(94^8)$
	MACHINE-to-MACHINE MANAGEMENT				
Avaya Aura Communication Manager Server	Communication Manager TLS server authenticates to the gateway using an RSA certificate.	Role	RSA 2048	1.59×10^{610}	$1/7.04 \times 10^{604}$

2.2 Probability of False Acceptance

FIPS 140-2 requires that the probability of false acceptance of a random authentication attempt be less than one in 1,000,000. FIPS 140-2 requires the probability of false acceptance within a one-minute period to be less than one in 100,000. These requirements are met as follows:

- Authentication of usernames, passwords and SNMPv3 shared secrets. The module enforces 8-character passwords (at minimum) chosen from the 94 human readable ASCII characters (95

excluding the space (0x20) character. The probability that a random attempt will succeed, or a false acceptance will occur is $1/94^8$, which is less than 1/1,000,000.

- The Password Authentication module enforces a maximum of ten password attempts before the module locks the user out between 30 and 3600 seconds. Therefore, there are twenty attempts possible in a one-minute period. The chances of a random attempt succeeding, or a false acceptance is $20/94^8$ which is less than 1/100,000.
- For SNMPv3 shared secrets, the processing speed of the Module will limit the number of allowed SNMPv3 requests to a much lower number. But even at the theoretical maximum transmission rate of 1,488,065 packets per second for the 1Gbit ethernet interface, there is no problem to satisfy the FIPS 140-2 requirement, since the probability of failure in 1 minute is $(60 \times 1.5 \times 10^6) / 94^8 = 9 \times 10^7 / 94^8 = 1 / 67 \times 10^6$ that is less than 1/100,000.

- For all TLS connections, the module acts as a TLS client equipped with the trusted root certificate that lies at the head of the server's certificate chain of trust.

  The module continuously attempts TLS connections to Communication Manager until successful. CPU availability and network bandwidth ultimately limit the number of possible failed TLS authentications per minute (server providing an unverifiable certificate). Assuming the module's 1 Gbit interface, and that a failed attempt requires the exchange of 8 packets, attempted TLS connections per minute can be no greater than 1,488,065/8x60 = 11,160,480/minute, or 1.12×10^7.

  A successful TLS handshake requires the server to send the module its end-entity certificate, which must be verified by a chain of trust leading to a trusted root certificate held by the module. In a brute force attack attempting to guess the trusted root's private key, the server could attempt to sign the chain with all possible keys in hopes of matching the public key held by the module's trusted root.

  In such an attack (e.g., 2048-bit RSA) it could try all keys which are the products of two 1024-bit primes, p & q. By the prime number theorem, we know the number of 1024-bit primes is approximately $\pi(2^{1024})-\pi(2^{1023}) \approx ((2^{1024})/(\ln 2^{1024})) - ((2^{1023})/(\ln 2^{1023})) \approx 1.26 \times 10^{305}$, so there are at least 1.59×10^{610} 2048-bit RSA keys. The chances of one of these keys matching in one minute is then $(1.12 \times 10^7)/(1.59 \times 10^{610}) = 1/7.04 \times 10^{604}$.

- Maintenance logins are authenticated using a challenge-response mechanism based on public-key methods. On maintenance login, the module prompts with a numeric challenge which must then be externally encrypted with a 2048-bit RSA key to form the response. The response is entered into the module, where a successful decryption will produce the original challenge. The probability of false acceptance is equivalent to the probability of breaking a 2048-bit RSA private key. Similar to the argument above, an iterative attack over 20 logins per minute has a success probability of $20/1.59 \times 10^{610}$.

2.3 Services for Approved Mode

The services implemented by the Module are listed in the tables below. Please refer to Table 14, Table 15, Table 16, and Table 17. Each service description also identifies the cryptographic user roles which utilize that service.

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Table 14 – Authenticated Services –Approved Mode

Service	Description	CO	User-MTCE	User-RW	User-R	CM Server	SNMP User
Configure Security	Security relevant configuration such as setting of FIPS mode, network security management, certificate management, and user management	x	x				
Password Set	Users and CO can change their password	x	x	x			
Configure	Non-security relevant configuration	x	x	x		x	x
Status	Show status	x	x	x	x	x	x
Zeroization	Destroy all CSPs	x	x				
SSH Server	Initiate SSH connection for SSH monitoring and control (CLI)	x	x	x	x		
SSH Client	Supports a client who wishes to deploy SCP for a secure file transfer.	x	x	x			
SNMPv3 Server	Provide SNMP service	x					x
TLS Connect	Initiate TLS connection for h248 control link to CM or for sending Syslog events to a remote Syslog server.	x	x			x	
Console Access	Console monitoring and control (CLI)	x	x	x	x		
Remote/Local Reset	Error state entry since reset could occur in more than just POSTs.	x	x	x		x	x
Audio Channel	An audio channel is created on the gateway upon request from the CM.					x	
Voice Communication Control	H.248 signaling to and from CM					x	
Firmware Load	Provide download of firmware images.	x	x				x
Backup & Restore	Provide backup and restore operation.	x	x	x			

Table 15 – Unauthenticated Services –Approved Mode

Service	Description
Local reset	Hardware reset or power cycle which includes running the POSTs
Status of LED lamps	Front panel's MDM, ALM, CPU, and PWR operate per Section 1.5.
Zeroization	Zeroization is performed when the Module has exited Error State1. This is also performed when the Module has entered Error State3.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Table 16 defines the relationship between access to CSPs and the different module services.
The modes of access shown in the table are defined as:

LEGEND:

- **G** = Generate: The module generates the CSP
- **R** = Read or Output: The CSP is read from the module
  - By "Output" this designates that information from this CSP function is sent out across the boundary of this module to another function.
- **E** = Execute: The module executes using the CSP
- **W** = Write or Input: The CSP is written to the module
  - By "Input" this designates that information is sent from another function inward across the boundary of this module to this CSP function.
- **Z** = Zeroize: The module zeroizes the CSP

Table 16 – CSP Access Rights within Services –Approved Mode

CSPs	Services															
	Configure security	Configure	Password Set	Status	Zeroization	SSH Server	SSH Client	SNMPv3 Server	TLS Connect	Console access	Remote/Local Reset	Audio Channel	Voice Communication Control	Firmware Load	Local Reset	Backup & Restore
Auth-User R	--	--	W	--	Z	WE	--	--	--	WE	--	--	--	--	--	RW
Auth-User RW	--	--	W	--	Z	WE	--	--	--	WE	--	--	--	--	--	RW
Auth-CO	--	--	W	--	Z	WE	--	--	--	WE	--	--	--	--	--	RW
DRBG Seed	G	--	--	--	Z	--	--	--	--	--	Z	--	--	--	Z	--
DRBG State	GE	--	--	--	Z	GE	--	--	GE	--	Z	--	GE	--	Z	--
Master-EK	G	--	--	--	Z	--	--	--	--	--	--	--	--	--	--	R
SSH-DH-Priv	--	--	--	--	Z	GE	GEZ	--	--	--	Z	--	--	--	Z	--
SSH-Host-Priv	GZ	--	--	--	Z	E	-	--	--	--	--	--	--	--	--	--
SSH-SENC	--	--	--	--	Z	GEZ	GEZ	--	--	--	Z	--	--	--	Z	--
SSH-SMAC	--	--	--	--	Z	GEZ	GEZ	--	--	--	Z	--	--	--	Z	--
TLS-DH-Priv	--	--	--	--	Z	--	--	--	GEZ	--	--	--	--	--	Z	--
TLS-Host-Priv	WZ	--	--	--	Z	--	--	--	WE	--	--	--	--	--	--	--
TLS-MS	--	--	--	--	Z	--	--	--	GEZ	--	Z	--	--	--	Z	--
TLS-PMS	--	--	--	--	Z	--	--	--	GEZ	--	Z	--	--	--	Z	--
TLS-SENC	--	--	--	--	Z	--	--	--	GEZ	--	Z	--	--	--	Z	--
TLS-SMAC	--	--	--	--	Z	--	--	--	GEZ	--	Z	--	--	--	Z	--

SRTP-MEK	--	--	--	--	Z	--	--	--	--	--	Z	WEZ	WEZ	--	Z	--
SRTP-MSALT	--	--	--	--	Z	--	--	--	--	--	Z	WEZ	WEZ	--	Z	--
SRTP-SENC	--	--	--	--	Z	--	--	--	--	--	Z	GEZ	--	--	Z	--
SRTP-SMAC	--	--	--	--	Z	--	--	--	--	--	Z	GEZ	--	--	Z	--
SRTP-SSALT	--	--	--	--	Z	--	--	--	--	--	Z	GEZ	--	--	Z	--
SRTCP-SENC	--	--	--	--	Z	--	--	--	--	--	Z	GEZ	--	--	Z	--
SRTCP-SMAC	--	--	--	--	Z	--	--	--	--	--	Z	GEZ	--	--	Z	--
SRTCP-SSALT	--	--	--	--	Z	--	--	--	--	--	Z	GEZ	--	--	Z	--
SNMP-PP	W	--	--	--	Z	--	--	E	--	--	Z	--	--	--	--	RW
SNMP-SENC	--	--	--	--	Z	--	--	GE	--	--	Z	--	--	--	Z	--
SNMP-SMAC	--	--	--	--	Z	--	--	GE	--	--	Z	--	--	--	Z	--

Table 17 – Public Key Access Rights within Services –Approved Mode

CSPs	Services															
	Configure security	Configure	Password Set	Status	Zeroization	SSH Server	SSH Client	SNMPv3 Server	TLS Connect	Console access	Remote/Local Reset	Audio Channel	Voice Communication Control	Firmware Load	Local Reset	Backup & Restore
CodeSign-Pub	--	--	--	--	--	--	--	--	--	--	--	--	--	RE	--	--
EASG-Prod-Pub	--	--	--	--	--	--	--	--	--	--	--	--	--	RE	--	--
SSH-DH-Pub	--	--	--	--	Z	RGE	RGE Z	--	--	--	Z	--	--	--	Z	--
SSH-Host-Pub	G Z	--	--	--	Z	RE	EZ	--	E	--	--	--	--	--	--	--
TLS-DH-Pub	--	--	--	--	Z	GEZ	--	--	RE	--	Z	--	--	--	Z	--
TLS-Host-Pub	RW Z	--	--	--	Z	--	--	--	RE	R	--	--	--	--	--	--
TLS-Trusted-Pub	RW Z	--	--	--	Z	--	--	--	RE	R	--	--	--	--	--	RW

2.4 Services for non-Approved Mode

The Module may be operated in non-Approved mode. In this mode, the Module may use non-validated cryptographic algorithms. A summary of the services in non-Approved mode is presented in Table 18 and Table 19.

Table 18 – Authenticated Services for non-Approved Mode

Service	Description	CO	User-MTCE	User-RW	User-R	CM Server	SNMP User
Configure security	Security relevant configuration such as setting of FIPS mode, network security management, certificate, and user management	x	x				
Password Set	Users and Administrator(s) can change their password	x	x	x			
Configure	Non-security relevant configuration	x	x	x		x	x
Status	Show status	x	x	x	x	x	x
Zeroization	Destroy all CSPs	x	x				
SSH Server	Initiate SSH connection for SSH monitoring and control (CLI)	x	x	x	x		
SSH Client	Support a client who wishes to deploy SCP for a secure file transfer	x	x	x			
SNMPv3 Server	Provide SNMP service						x
TLS connect	Initiate TLS connection for h248 control link to CM or for sending Syslog events to a remote Syslog server.	x				x	
Console access	Console monitoring and control (CLI)	x	x	x	x		
Remote/Local Reset	Firmware initiated reset which includes running the POSTs.	x	x	x		x	x
Audio Channel	An audio channel is created on the gateway upon request from the CM.					x	
Voice Communication Control	H.248 signaling to and from CM					x	
Firmware Load	Provide download of firmware images.	x	x				x
Backup & Restore	Provide backup and restore operation.	x	x	x			

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

In Table 19, these services are all available to the roles of Cryptographic Officer and to the User-R/W and User-R.

Table 19 – Other Communication Services for Non-Approved Mode

Service	Description
Local reset	Hardware reset or power cycle which includes running the POSTs
Standard Local Survivability (SLS)	This supports a local call processing functionality when all ability to register to a Communication Manager is lost. In this mode, the gateway's SLS module will support call requests, dial plan processing and call routing; among local endpoints (analog, DCP, H.323 station sets) and to/from the local PSTN trunks (analog, BRI, PRI, and R1-signaling). *This is inhibited in Approved mode.*
ADS SLA Monitor	The Avaya Diagnostic Services Monitor should not be deployed. *This is inhibited in Approved mode.*
FTP	The File Transfer Protocol should not be invoked. Rather the SCP feature should be deployed as a more secure alternative method for file transfer. *The server side cannot be enabled in the Module.* *The client side is used in a restrictive manner by some functions such as download.*
TFTP	The Trivial File Transfer Protocol should not be invoked. Rather the SCP feature should be deployed as a more secure alternative method for file transfer.
Telnet	The Telnet remote access protocol should not be invoked. Rather the SSH protocol should be deployed as a more secure alternative method for remote access. *This is inhibited in Approved mode.*
RIP	The Routing Information Protocol is a data feature available in the Gateway. *This is inhibited in Approved mode.*
OSPF	The Open Shortest Path First Protocol is a data feature available in the Gateway. *This is inhibited in Approved mode.*
SNMPv1 and v2	This services function may be described as available for the SNMP user, along with the General Administrative user while in non-Approved mode. *This is inhibited in Approved mode.*
VPN (IPsec)	VPN services are deployed for remote access. This protocol employs IPsec to tunnel information securely across IP-based networks. *This is inhibited in Approved mode.*
RADIUS	Remote Authentication Dial-In User Service. This allows end users to authenticate and login into the Module through a centrally managed server. *This is inhibited in Approved mode.*

CHAP	Challenge Handshake Authentication Protocol. This verifies the caller's identity by using a three-way handshake upon initial link establishment. *This is inhibited in Approved mode.*
PAP	Password Authentication protocol. This protocol uses a two-way handshake method of establishing a caller's identity. This is used during the initial establishment of the PPP data link. *This is inhibited in Approved mode.*
PPP	Point-to-Point protocol. This is an encapsulation protocol for transport over the WAN. It supports modem dial access from a personal computer. *This is inhibited in Approved mode.*
PTLS	Proprietary-TLS protocol. The user of this service is really the machine-to-machine interaction with the Communication Manager (host-based telecommunication server). *This is inhibited in Approved mode.*
Vintage License Exchange	Older versions of Communication Manager required the module to transmit unique product information such as 'serial number' and 'firmware vintage'. *This is inhibited in Approved mode.*

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

3 Self-Tests

On power up or reset, the Module performs self-tests described in Table 20 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters Error State1.

Table 20 – Power-On Self-Test

Test Target	Description
DSP	
AES-ECB	Encrypt/decrypt, ECB mode, 128- and 256-bit key lengths
HMAC	One KAT to cover HMAC-SHA1
SHS	One KAT to cover SHA1
MGP	
AES	Encrypt/decrypt, ECB mode, 128-bit key length
AES-GCM	Encrypt/decrypt, 256-bit key length
DRBG_CTR	KAT for AES-256-CTR with derivation function
ECDSA	Sign/verify using P-256, P-384 and P-521
Firmware Integrity	HMAC-SHA256
HMAC	One KAT per SHA1, SHA224, SHA256, SHA384, SHA512.
KAS SSC	KATs for finite field (MODP-2048) and elliptic curve (P-256, P-384, P-521) Diffie-Hellman
SSH KDF	KAT for SSH key derivation function for 128/256-bit keys
TLS KDF	KAT for TLS key derivation function for TLS 1.0/1.1/1.2
RSA	Sign/verify using PKCS#1 2048- & 3072-bit keys, SHA-256
SHS	One KAT per SHA1, SHA256, SHA512
Triple-DES	Encrypt/decrypt, ECB mode, 3-Key

Table 21 – Conditional Self-Tests

Test Target	Description
Entropy Source	Continuous test performed when a random value is requested from the NDRNG. • PLD Stuck test • Adaptive Proportion test • Repetition Count test See NIST SP 800-90B
DRBG	Continuous test performed when a random value is requested from the DRBG. (including Health tests per SP 800-90A Section 11.3)
ECDSA / RSA	Pairwise consistency test on each generation of a key pair.
Firmware Load	RSA 2048 with SHA-256 signature verification performed when firmware is authenticated before installation.
AES, SHA-1, HMAC-SHA-1	Continuous cross compare of crypto-algorithm results between DSP and MGP

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Table 22 – Critical Function Tests

These are all included in the set of Power-On Self tests.

Test Target	Description
NVRAM Self-test	Execute CRC checks over NVRAM blocks.
EEPROM Self-test	Conduct checksum over the EEPROM.

4 Physical Security

The module design is classified as a "Hardware Module with Multichip Standalone Embodiment." Physical security is provided by a production-grade enclosure.

5 Operational Environment

The module supports a limited operational environment. The module includes a firmware load service to support necessary updates. Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on the Security Policy. Any firmware not identified in this Security Policy does not constitute the module defined by this Security Policy or covered by this validation.

6 Mitigation of Other Attacks Policy

The module is not designed to mitigate against attacks which are outside of the scope of FIPS 140-2.

7 Security Rules and Guidance

The module design corresponds to the security rules below.

1. The module clears previous authentications on power cycle.
2. Power up self-tests do not require any operator action.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
4. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
5. When entering/exiting the maintenance role, the operator shall invoke the zeroization service ("zeroize").
6. The module does not support manual key entry.
7. The module does not output intermediate key values.
8. The module does not output plaintext CSPs.
9. The Cryptographic Officer shall change the default password before initial configuration is completed. The Cryptographic Officer shall define the roles of the other user accounts.
10. The module shall not be used with compact flash when operating in Approved mode.

© 2023 Avaya, Inc. All rights reserved.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

8 References and Definitions

The following standards are referred to in this Security Policy.

Table 23 – References

Abbreviation	Full Specification Name
FIPS 140-2	*Security Requirements for Cryptographic Modules, NIST, December 2002*
SP 800-52 Rev. 2	*Guidelines for the Selection, Configuration, and use of Transport Layer Security (TLS) Implementations, NIST, August 2019*
SP 800-90A Rev. 1	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST, June 2015*
SP 800-90B	*Recommendation for the Entropy Sources Used for Random Bit Generation, NIST, January 2018*
SP 800-135 Rev. 1	*Recommendation for Existing Application-Specific Key Derivation Functions, NIST, December 2011*
RFC 5288	*AES Galois Counter Mode (GCM) Cipher Suites for TLS, IETF, August 2008*

Table 24 – Acronyms and Definitions

Acronym	Definition
AEA	Avaya Encryption Algorithm – proprietary algorithm for media encryption
AES	Advanced Encryption Standard
Approved Mode	FIPS Approved Mode of operation. In the G450 customer documentation, this is referred to as “FIPS Mode.”
ASB	Recessed Alternate Software Bank button on front face of G450/G430
CA	Certificate Authority. This is an authority (private or public) which bears responsibility to sign Identity certificates issued to a given product.
CAVP	Cryptographic Algorithm Validation Program
CCA	Contact Closure Adjunct. When this port is connected to an Avaya Partner Contact Closure Adjunct box, the gateway can be commanded to open or close a relay on the box. No cryptographically-relevant operations are involved.
CLI	Command Line Interface
CM	Communication Manager, a.k.a. Avaya Aura Communication Manager. This Avaya product directs the VoIP and circuit-switched telecom resources of the G450 and G430 to form audio connections between communicating parties. Communication Manager is not involved with the configuration or security management of the G450 and G430. In ITU H.248 parlance, Communication Manager acts as an H.248 “Media Gateway Controller,” with the G450 or G430 performing as a “Media Gateway.”
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer. This is the security operator who represents the customer for purpose of management of all security configuration.
CSP	Critical Security Parameter

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Acronym	Definition
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
EEPROM	Electronically Erasable Programmable Read Only Memory
EMC	Electromagnetic Compatibility
ETR	Emergency Transfer Relay. Emergency Transfer is a media gateway feature that connects pre-determined telephones and external service provider trunks in case of a power outage. The ETR port is for optional connection to an Avaya 808A ETR Panel that aids in the support of such connections. No cryptographic-relevant functions are involved.
FIPS	Federal Information Processing Standard
H.248	ITU Gateway Control Protocol (a.k.a. Megaco)
HMAC	Hash-Based Message Authentication Code
IKEv1	Internet Key Exchange version 1
IP	Internet Protocol
ISDN	Integrated Services Digital Network
KAT	Known Answer Test
Media Module	A small pluggable circuit pack which is inserted into a Media Module slot in either the Avaya G450 or G430 media gateway. Avaya Media Modules support a variety of legacy (land line) telephone and trunk interfaces. Media Modules have no cryptographic-relevant functions.
MG	Media Gateway. In the G450 documentation, this is also referred to as MGW. It is also referred to as “BGW” for Branch gateway. The preference is Media Gateway. It is part of a branch office solution, but not all gateways have to be located in a branch office.
MGP	Media Gateway Processor
NDRNG	Hardware Non-Deterministic RNG Noise Source for the Entropy Source. This Entropy Source is used to seed the FIPS approved DRBG
NIST	National Institute of Standards & Technology
Non-Approved Mode	This is a non-FIPS Approved Mode of operation. In customer documentation, this is referred to as “non-FIPS Mode.”
NVRAM	Non-Volatile Random-Access Memory (a.k.a. flash memory)
PLD	Programmable Logic Device
PSTN	Public Switched Telephone Network
PTLS	Pseudo TLS – proprietary encryption algorithm for H.248 used prior to TLS
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
RST	Recessed reset button on front face of G450/G430
RTP	Real-Time transport Protocol, defined in IETF RFC 3550
SHA-1	Secure Hash Algorithm 1
SNMP	Simple Network Management Protocol
SRTP	Secure RTP, defined in IETF RFC 3711 and RFC 6188
SSH	Secure Shell

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).

Acronym	Definition
Supervisor	The primary circuit board in the media gateway is described as a “Supervisor” board. Alternatively, it is also referred as the “Mainboard” or the “Motherboard” in some Avaya documentation.
TDM	Time Division Multiplexing
TLS	Transport Layer Security
Triple-DES	Triple - Data Encryption Standard. This sometimes is named “3DES” and “TDES.” The original source description evolved from the NIST TDEA (Triple Data Encryption Algorithm) documentation.
VoIP	Voice over IP. This is a media stream that has been sampled with a codec and transmitted across an IP based network in RTP payload packets.

Avaya, Inc. Public Material – May be reproduced only in its original entirety (without revision).