



Motorola GGM 8000 Gateway FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.14

Revision Date: 7/16/2014

Contents

1. MODULE OVERVIEW.....	3
2. SECURITY LEVEL	5
3. MODES OF OPERATION	6
4. PORTS AND INTERFACES.....	9
5. IDENTIFICATION AND AUTHENTICATION POLICY	11
6. ACCESS CONTROL POLICY	13
7. OPERATIONAL ENVIRONMENT	18
8. SECURITY RULES	19
9. CRYPTO-OFFICER GUIDANCE.....	20
10. PHYSICAL SECURITY POLICY.....	21
11. MITIGATION OF OTHER ATTACKS POLICY	22
12. DEFINITIONS AND ACRONYMS.....	23
GGM 8000 GATEWAY TAMPER EVIDENCE LABEL INSTALLATION INSTRUCTIONS.....	24

1. Module Overview

The Motorola GGM 8000 Gateway is a modular purpose-built gateway that can easily be configured to support a variety of public safety network applications. The Motorola GGM 8000 Gateway is a multi-chip standalone cryptographic module encased in a commercial grade metal case made of cold rolled steel. The Motorola GGM 8000 Gateway cryptographic boundary is the gateway’s enclosure which includes all components, and one of the power supply options (AC or DC) identified in Table 1b. Figure 1 illustrates the cryptographic boundary of the Motorola GGM 8000 Gateway. In the photo, there is a slot that can hold an optional expansion module for increased device connectivity. The optional expansion module is not included within the Motorola GGM 8000 Gateway cryptographic boundary. The FIPS validated firmware versions are XS-16.6.0.69, GS-16.6.0.69 and KS-16.6.0.69. (The firmware versions have identical FIPS 140-2 security relevant functionality. They differ only in non-security relevant features.)

Note: A FIPS label kit can be ordered by using part number CLN8787A, Rev. B.

Configuration	GGM 8000 Base Unit		FW Version
	HW P/N	Version	
1	CLN1841E	Rev A	XS-16.6.0.69, GS-16.6.0.69, or KS-16.6.0.69

Table 1a – Motorola GGM 8000 Gateway Version Numbers

Configuration	GGM 8000 AC Power Supply		GGM 8000 DC Power Supply	
	HW P/N	Revision	HW P/N	Revision
1	CLN1850A	G	CLN1849A	H

Table 1b – Motorola GGM 8000 Gateway Power Supply Options

Previous Validation Versions – FIPS 140-2 Cert. #1546

Configuration	GGM 8000 Base Unit		GGM 8000 Encryption Module		FW Version
	HW P/N	Version	P/N	Version	
1	CLN1841A	Rev B	CLN8492D	Rev B	XS-16.0.1.44

Table 2a – Motorola GGM 8000 Gateway Version Numbers

Configuration	GGM 8000 AC Power Supply		GGM 8000 DC Power Supply	
	HW P/N	Revision	HW P/N	Revision
1	CLN1850A	C	CLN1849A	C

Table 2b – Motorola GGM 8000 Gateway Power Supply Options





Figure 1 – Motorola GGM 8000 Gateway Cryptographic Module Boundary

2. Security Level

The Motorola GGM 8000 Gateway cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

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

Table 3 – Module Security Level Specification

3. Modes of Operation

Approved mode of operation

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

Hardware Implementations

- Triple-DES– CBC mode (168 bit) for IPsec and FRF.17 encryption (Cert. #757)
- AES - CBC mode (128, 192, 256 bit) for IPsec and FRF.17 encryption (Cert. #962)
- HMAC-SHA-1 for IPsec and FRF.17 authentication (Cert. #1487)
- SHA-1 for message hash (Cert. #933)

Firmware Implementations

- Triple-DES – CBC mode (168 bit) for IKE and SSHv2 encryption (Cert. #1493)
- AES – CBC (128, 192, 256-bit), ECB (128-bit), and CFB128 (128-bit) modes for IKE, SSHv2 and SNMPv3 encryption (Cert. #2395)
- HMAC-SHA-1 for IKE, SSHv2 and SNMPv3 authentication (Cert. #1486)
- SHA-1 and SHA-256 for message hash (Cert. #2057)
- RSA PKCS#1 v1.5 – for signature verification (1024- and 2048-bit) (Cert. #1239)
- SP800-90 Hash_Based Deterministic Random Bit Generator (DRBG) (Cert. #399)
- KDF for SSH (CVL Cert. #99)
- KDF for SNMPv3 (CVL Cert. #122)
- KDF for IKEv1/IKEv2 (CVL Cert. #315)

The Motorola GGM 8000 Gateway supports the commercially available IKE and Diffie-Hellman protocols for key establishment, IPsec (ESP) and FRF.17 protocols to provide data confidentiality using FIPS Approved encryption and authentication algorithms, and SSHv2 for secure remote access.

Key strength provided by the key establishment protocols is limited by the parameters of the specific protocol and by the minimum entropy of 128 bits provided by the hardware non-deterministic RNG (NDRNG).

Allowed Algorithms

- Diffie-Hellman Group 14 (2048-bit) (allowed for key agreement per FIPS 140-2 Annex D) (key agreement; key establishment methodology provides 112 bits of encryption strength)
- Hardware non-deterministic RNG (NDRNG): Provides seed for Approved DRBG

Non-FIPS approved algorithms

The cryptographic module provides non-FIPS Approved algorithms which are only available in the Non-Approved mode as follows:

- DES for encryption/decryption
- DSA 1024-bit – for public/private key pair generation and digital signatures (non-compliant)
- Non approved SW RNG: Provides random numbers for networking functions (non-compliant)
- Diffie-Hellman Group 1 (768 bit)
- MD5: for hashing (Provides interoperability within supported protocols)
- HMAC-MD5

The module supports the following algorithms which are Disallowed as of January 1, 2014 per the NIST SP 800-131A algorithm transitions:

- FIPS 186-2 RSA PKCS#1 v1.5 signature generation (1024-bit using SHA-1) (Cert. #1239)
- Diffie-Hellman Group 2 (1024-bit) and Group 5 (1536-bit) (key agreement; key establishment methodology provides <112 bits of encryption strength; non-compliant)

Algorithms providing less than 112 bits of security strength (Disallowed per NIST SP 800-131A) are not allowed in the FIPS Approved mode of operation for use by Federal agencies.

Entering FIPS Mode

To enter FIPS mode, the Crypto-Officer must follow the procedure outlined in Table 4 below. For details on individual gateway commands, use the online help facility or review the *Enterprise OS Software User Guide* and the *Enterprise OS Software Reference Guide*.

Step	Description
1.	Configure the parameters for the IKE negotiations using the IKEProfile command. For FIPS mode, only the following values are allowed: Diffie-Hellman Group (Group 14 required for 112-bit key strength), Encryption Algorithm (AES or Triple-DES), Hash Algorithm (SHA), and Authentication Method (PreSharedKey).
2.	Electronically establish via the local console port the pre-shared key (PSK) to be used for the IKE protocol using: ADD -CRYPTO FipsPreSharedKey <peer_ID> <pre-shared_key> <pre-shared_key>
3.	If IPsec is used, configure IPsec transform lists using the ADD -CRYPTO TransformList command. For FIPS mode, only the following values are allowed: Encryption Transform (ESP-TDES, or ESP-AES) and Authentication Transform (ESP-SHA).
4.	If FRF.17 is used, configure FRF.17 transform lists using the ADD -CRYPTO TransformList command. For FIPS mode, only the following values are allowed: Encryption Transform (FRF-TDES, or FRF-AES) and Authentication Transform (FRF-SHA).
5.	For each port for which encryption is required, bind a dynamic policy to the ports using: ADD [!<portlist>] -CRYPTO DynamicPOLicy <policy_name> <priority> <mode> <selcrlist_name> <xfrmllist_name> [<pfs>] [<lifetime>] [<preconnect>] To be in FIPS mode, the selector list and transform list names must be defined as in previous steps.
6.	For each port for which encryption is required, enable encryption on that port using: SETDefault [!<portlist>] -CRYPTO CONTrol = Enabled
7.	DSA keys must not be used in FIPS mode.
8.	FIPS-140-2 mode achieved.

Table 4 – FIPS Approved mode configuration

To obtain the FIPS Mode Indicator, use the following command:

SHOW -CRYPTO CONFIguration

This command shows a detailed summary of the cryptographic configuration. By reviewing the results of this command, as discussed in the following steps, the Crypto-Officer verifies that the gateway is in FIPS mode.

Step 1: Look at the IKEProfile section of the cryptographic configuration summary output to verify that FIPS-Approved algorithms have been selected for IKE negotiations (AES or Triple-DES for encryption, and SHA as the hash algorithm), Diffie-Hellman Group 14 has been selected and that pre-shared key has been selected as the authentication method. Summary output should look similar to the following:

CRYPTO IKEProfile:

Priority	Authentication Method	Encrypt Alg	Hash Alg	DH Group	Lifetime
1	PreSharedKey	AES/256	SHA	Group14	1 dy
2	PreSharedKey	AES/256	SHA	Group14	1 dy

Step 2: For each port for which encryption is required, verify that the dynamic policy points to a transform list that uses FIPS-Approved algorithms (AES or Triple-DES for encryption, and SHA as the hash algorithm), as shown in the following example:

CRYPTO DynamicPOLicy: dp1

Priority 1
PortList: !V1
DpolCont: Enabled
Mode: Tunnel
Lifetime: GlobalLifeTime (8 hr)
PFS: GlobalPFS (NoPFS)
SelectorList: s1
TransformList: t1
Preconnect: Yes, Peer IP: 10.1.233.165

CRYPTO TransformList: t1 In use by 1 policy

1 ESP-AES/256 ESP-SHA

In this example, the dynamic policy named dp1 points to a transform list t1. The transform list t1 uses FIPS-Approved algorithms AES/256 and SHA.

Step 3: For each port for which encryption is required, look at the summary output to verify that encryption has been enabled on the required ports, as shown in the following example:

CRYPTO CONFIguration:

Port !V1 CONTrol = Enabled
Port !V102 CONTrol = Enabled

Upon successful completion of these three steps, the Crypto-Officer has been shown the FIPS Mode Indicator and verified that the gateway is in FIPS mode.

4. Ports and Interfaces

Table 5 below provides a listing of the physical ports and logical interfaces for the Motorola GGM 8000 Gateway.

The Motorola GGM 8000 Gateway base unit provides four 10/100 Mbps Ethernet interfaces, two T1/E1 interfaces and a console port. The Motorola GGM 8000 Gateway incorporates an optional expansion module that accommodates a variety of interfaces for both analog and WAN connectivity. The expansion module is not part of the cryptographic boundary.

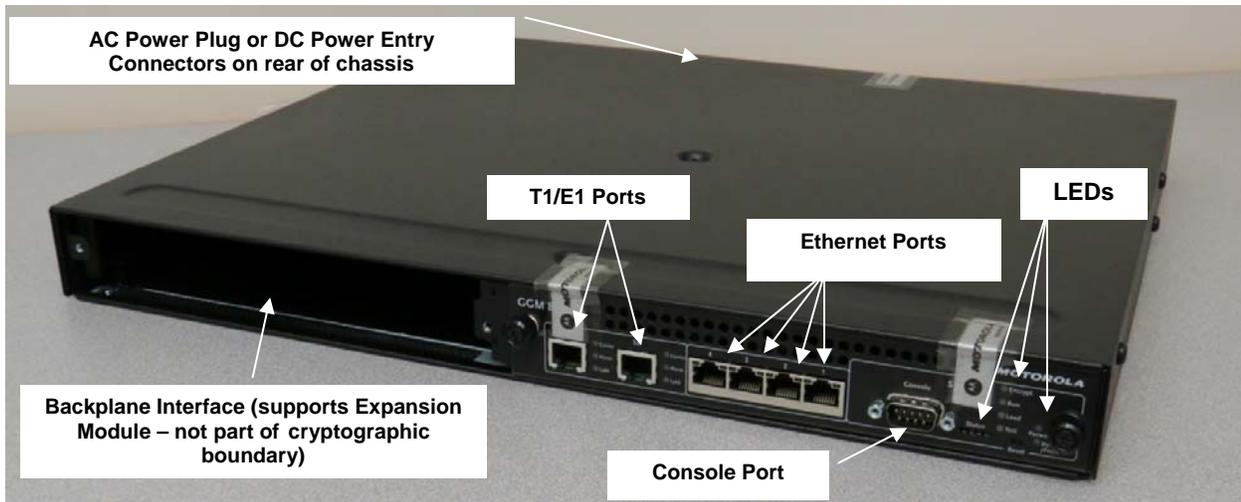


Figure 2 – GGM 8000 Ports

Physical Port	Qty	Logical interface definition	Interface Card	Comments
Ethernet	4	Data input, data output, status output, control input	Part of the Motorola GGM 8000 Gateway base system	LAN ports that provide connection to Ethernet LANs using either 10BASE-T, 100BASE-TX, or 1 Gigabit Ethernet
T1/E1	2	Data input, data output, status output, control input, power output	Part of the GGM 8000 Gateway base system	T1/E1 interfaces that support T1/E1 CSU/DSU
Console	1	Status output, control input	Part of the GGM 8000 Gateway base system	RS-232 interface
Backplane interface Supports expansion module containing optional interface cards (expansion module not part of cryptographic boundary)		Data input, data output, status output, control input, power output	Optional FlexWAN module supported in one of the I/O slots on the expansion module	High-speed multifunction serial interfaces that provide connection to industry-standard V.35, Data Communications Equipment (DCE) or Data Terminal Equipment (DTE) serial devices
			Optional module supported in the analog slot on the expansion module as part of the analog/V.24 interface kit	Provides 4 four-wire with E&M relay interfaces to analog conventional base stations
			Optional modules supported in the two I/O slots on the expansion module as part of the analog/V.24 interface kit	Provide V.24 serial ports that communicate at 9600 bps.
AC power plug -OR- DC power entry connectors	1 -OR- 2	AC power input -OR- DC Power input	AC power subsystem module -OR- DC power subsystem module	External AC power input port -OR- External DC power input ports
LEDs	7	Status Output	N.A	Provide Module status for traffic and module power.

Table 5 – Motorola GGM 8000 Gateway physical ports and logical interfaces

5. Identification and Authentication Policy

Assumption of roles

The Motorola GGM 8000 Gateway supports the following distinct operator roles:

1. Crypto-Officer (Super User) Roles #1-4 require operator authentication via username and password when accessing the gateway via any interface. (See Table 7.) Upon correct authentication, the role is selected based on the username of the operator. At the end of a session, the operator must log-out.
2. Admin
3. Network Manager
4. User
5. MotoAdmin Roles #5-7 are specific to SNMPv3 operations. Each SNMPv3 user has its own pair of encryption and authentication passphrases. (See Table 7.)
6. MotoMaster
7. MotoInformA/B

The module stores operator identity information internally for all roles.

When a gateway power cycles, sessions are terminated. An operator must reauthenticate to access the gateway.

Multiple concurrent operators. Each operator has an independent session with the gateway, either through SSH or via the console. Once authenticated to a role, each operator can access only those services for that role. In this way, separation is maintained between the role and services allowed for each operator.

The definition of all supported roles is shown in Table 6 below.

Role	Type of Authentication	Authentication Data	Description
Crypto-Officer (Super User)	Role-based operator authentication.	Username and Password.	The owner of the cryptographic module with full access to services of the module.
Network Manager	Role-based operator authentication.	Username and Password.	An operator of the module with almost full access to services of the module.
Admin	Role-based operator authentication.	Username and Password.	An assistant to the Crypto-Officer that has read only access to a subset of module configuration and status indications.
User	Role-based operator authentication.	Username and Password.	A user of the module that has read only access to a subset of module configuration and status indications.
MotoAdmin (SNMPv3)	Role-based operator authentication.	Passphrase.	An SNMPv3 user who can issue any command from the SNMP V3 User Manager menu.
MotoMaster (SNMPv3)	Role-based operator authentication.	Passphrase.	An SNMPv3 user who can change its own passphrases from the SNMP V3 User Manager menu.
MotoInformA/B (SNMPv3)	Role-based operator authentication.	Passphrase.	An SNMPv3 user who receives and transmits reliable messages over SNMPv3.

Table 6 – Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Username and Password	<p>Passwords are alphanumeric strings consisting of 7 to 15 characters chosen from the 94 standard keyboard characters.</p> <p>The probability that a random attempt will succeed or a false acceptance will occur is $1/94^7$ which is less than $1/1,000,000$. After three consecutive unsuccessful login attempts, an operator is locked out for two minutes, ensuring that that the probability is less than one in 100,000 per minute, that random multiple attempts will succeed or a false acceptance will occur.</p>
Passphrase	<p>Each SNMPv3 user has its own pair of encryption and authentication passphrases. The SNMPv3 user authentication or encryption passphrase must be 8-64 characters long and may contain uppercase and lowercase alphabetic characters (A-Z) and (a-z); numeric characters (0-9); and any of the following special characters (! " % & ' () * + , - . / : ; < = > ?).</p> <p>The probability that a random attempt will succeed or a false acceptance will occur is $1/80^8$ which is less than $1/1,000,000$. The timing of the SNMPv3 authentication protocol as implemented limits the probability of randomly guessing an SNMPv3 passphrase in 60 seconds to less than 1 in 100,000.</p>

Table 7 – Strengths of Authentication Mechanisms

6. Access Control Policy

Authenticated Services

- Firmware Update: Load firmware images digitally signed by RSA (1024 bit) algorithm.
- Key Entry: Enter Pre-Shared Keys (PSK).
- User Management: Add/Delete and manage operator passwords.
- Reboot: Force the module to power cycle via a command.
- Zeroization: Actively destroy all plaintext CSPs and keys.
- Crypto Configuration: Configure IPsec and FRF.17 services.
- *IKE: Key establishment utilizing the IKE protocol.
- *IPsec Tunnel Establishment: IPsec protocol.
- FRF.17 Tunnel Establishment: Frame Relay Privacy Protocol.
- Alternating Bypass: Provide some services *with* cryptographic processing and some services *without* cryptographic processing.
- *SSHv2: For remote access to the gateway.
- Network Configuration: Configure networking capabilities.
- SNMPv3: Network management, including traps and configuration.
- Enable Ports: Apply a security policy to a port.
- File System: Access file system.
- Authenticated Show Status: Provide status to an authenticated operator.
- Access Control: Provide access control for Crypto-Officer, Network Manager, Admin, and User.

* Services impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used.

Unauthenticated Services:

- Unauthenticated Show Status: Provide the status of the cryptographic module – the status is shown using the LEDs on the front panel.
- Power-up Self-tests: Execute the suite of self-tests required by FIPS 140-2 during power-up.

All Services available in FIPS Approved mode are also available in FIPS Non-Approved mode. The Approved mode is defined by the correct configuration.

Roles and Services

Service	Crypto-Officer (Super User)	Network Manager	User	Admin	MotoAdmin (SNMPv3)	MotoMaster (SNMPv3)	MotoInformA/B (SNMPv3)
Firmware Update	X	X					
Key Entry	X	X					
User Management	X	X					
IKE	X	X					
IPsec Tunnel Establishment	X	X					
FRF.17 Tunnel Establishment	X	X					
SSHv2	X	X					
Reboot	X	X					
Zeroization	X	X					
Crypto Configuration	X	X					
Network Configuration	X	X					
SNMPv3	X	X			X	X	X
Alternating Bypass	X	X					
Enable Ports	X	X					
File System	X	X					
Authenticated Show Status	X	X	X	X			
Access Control	X	X	X	X			

Table 8 – Authenticated Services to Roles Mapping

Definition of Critical Security Parameters (CSPs)

The following CSPs are contained within the module:

Key	Description/Usage
KEK	This is the master key that encrypts persistent CSPs stored within the module. KEK-protected keys include PSK and passwords. Encryption of keys uses AES128ECB
IKE Preshared Keys	Used to authenticate peer to peer during IKE session
SKEYID	HMAC-SHA-1, used in IKE to provide for authentication of peer router. Generated for IKE Phase 1 by hashing preshared keys with responder/receiver nonce
SKEYID_d	Phase 1 key used to derive keying material for IKE SAs
SKEYID_a	Key used for integrity and authentication of the phase 1 exchange
SKEYID_e	Key used for Triple-DES or AES data encryption of phase 1 exchange
*Ephemeral DH Phase-1 private key (a)	Generated for IKE Phase 1 key establishment
*Ephemeral DH Phase-2 private key (a)	Phase 2 Diffie-Hellman private keys used in PFS for key renewal
*IPsec Session Keys	128/192/256-bit AES-CBC and 168-bit Triple-DES keys are used to encrypt and authenticate IPsec ESP packets
FRF.17 Session Keys	168-bit Triple-DES-CBC and 128/192/256-bit AES-CBC keys are used to encrypt and authenticate FRF.17 Mode 2
*SSH-RSA Private Key	Key used to authenticate oneself to peer
SSH Session Keys	168-bit Triple-DES-CBC and 128/192/256-bit AES-CBC keys are used to encrypt and authenticate SSH packets
*SSH DH Private Key	Generated for SSH key establishment
SNMPv3 Passphrases	Passphrases used in generation of SNMPv3 session keys
SNMPv3 Session Keys	128-bit keys to encrypt (AES-CFB) and authenticate (SHA1) SNMPv3 packets
RADIUS Secret	<i>Used for authentication of packets sent/received to RADIUS Server, up to 32 characters.</i>
Hash-DRBG Seed	Initial seed for FIPS-Approved DRBG
Hash-DRBG Internal State	Internal state/context for FIPS-Approved DRBG. The critical security parameters are the values V and C.
Passwords <ul style="list-style-type: none"> • Crypto-Officer (Super User) • Network Manager • Admin • User 	7 (to 15) character password used to authenticate to the module

Table 9 – Critical Security Parameters (CSPs)

* CSPs impacted by the SP 800-131A algorithm transitions. It is the responsibility of the module operator to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used.

Definition of Public Keys:

The following public keys are contained within the module:

Key	Description/Usage
RSA Firmware Load Key	Distributed to module, for firmware authentication
SSH-RSA Key	Distributed to peer, used for SSH authentication
SSH Known Host Keys	Distributed to module, used to authenticate peer
IKE DH public key (g^a)	Generated for IKE Phase 1 key establishment
IKE DH phase-2 public (g^a) key	Phase 2 Diffie-Hellman public keys used in PFS for key renewal (if configured)
SSH DH Key	Generated for SSH key establishment

Table 10 – Public Keys

Definition of CSPs Modes of Access

Table 11 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- = No access to the CSP by the service.
- G = Generate: The Module generates the CSP.
- R = Read: The Module exports the CSP.
- E = Execute: The Module executes using the CSP.
- W = Write: The Module writes the CSP.
- Z = Zeroize: The Module zeroizes the CSP.

CSP	Firmware Update	Key entry	User Management	IKE	IPsec tunnel establishment	FRF.17 tunnel establishment	SSHv2	Reboot	Zeroization	Crypto Configuration	Network Configuration	SNMPv3	Alternating Bypass	Enable Ports	File System	Authenticated Show Status	Access Control
KEK	-	-	E	-	-	-	-	E	Z	GE	-	-	-	-	-	-	-
IKE Pre-shared Key	-	W	-	E	-	-	-	-	Z	RW	-	-	-	-	EW	E	-
SKEYID	-	-	-	EG	-	-	-	Z	Z	-	-	-	-	-	-	-	-
SKEYID_d	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SKEYID_a	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SKEYID_e	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
Ephemeral DH Phase-1 private key (a)	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-

CSP	Firmware Update	Key entry	User Management	IKE	IPsec tunnel establishment	FRF.17 tunnel establishment	SSHv2	Reboot	Zeroization	Crypto Configuration	Network Configuration	SNMPv3	Alternating Bypass	Enable Ports	File System	Authenticated Show Status	Access Control
Ephemeral DH Phase-2 private key (a)	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
IPsec Session Keys	-	-	-	EG	E	-	-	-	Z	-	-	-	-	-	-	-	-
FRF.17 Session Keys	-	-	-	EG	-	E	-	-	Z	-	-	-	-	-	-	-	-
SSH-RSA Private Key	-	-	-	-	-	-	EG	-	Z	EG	-	-	-	-	-	-	-
SSH Session Keys	-	-	-	-	-	-	EG	-	Z	-	-	-	-	-	-	-	-
SSH DH Private Key	-	-	-	-	-	-	EG	-	Z	-	-	-	-	-	-	-	-
Passwords	-	-	EW	-	-	-	-	-	Z	-	-	-	-	-	-	-	E
RADIUS Secret	-	-	-	-	-	-	-	-	Z	-	-	-	-	-	-	-	EW
SNMPv3 Passphrase	-	-	EW	-	-	-	-	-	Z	-	-	E	-	-	-	-	-
SNMPv3 Session Keys	-	-	-	-	-	-	-	-	-	-	-	EGZ	-	-	-	-	-
DRBG Seed	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
DRBG Internal State	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-

Table 11 – Services to CSP Access mapping

7. Operational Environment

The Motorola GGM 8000 Gateway does not contain a modifiable operational environment.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the Motorola GGM 8000 Gateway to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The Motorola GGM 8000 Gateway provides seven distinct operator roles: Crypto-Officer (Super User), Admin, Network Manager, User, MotoAdmin (SNMPv3), MotoMaster (SNMPv3), and MotoInformA/B (SNMPv3). The Crypto-Officer role uses the Super User account.
2. The Motorola GGM 8000 Gateway encrypts message traffic using the AES or Triple-DES algorithm.
3. The Motorola GGM 8000 Gateway performs the following tests:
 - A. Power up Self-tests:
 1. Cryptographic algorithm tests:
 - Hardware Implementations:
 - a. AES-CBC Encrypt and Decrypt Known Answer Test
 - b. Triple-DES-CBC Encrypt and Decrypt Known Answer Tests
 - c. HMAC-SHA-1 Known Answer Test (Includes SHA-1 KAT)
 - Firmware Implementations:
 - a. AES-ECB128, CBC128,192,256 Encrypt and Decrypt Known Answer Tests
 - b. Triple-DES-CBC Encrypt and Decrypt Known Answer Tests
 - c. HMAC-SHA-1 Known Answer Test
 - d. SHA-1, SHA-256 Known Answer Tests
 - e. DRBG Known Answer Test
 - f. RSA Sign and Verify Known Answer Test
 - Critical functions test
 - a. DSA Sign and Verify Known Answer Test
 2. Firmware Integrity Test (16 bit CRC)
 - B. Conditional Self-tests:
 - a. Continuous Random Number Generator (RNG) test on FIPS-Approved DRBG and Hardware NDRNG.
 - b. Firmware load test – RSA signature verification of externally loaded code.
 - c. Alternating bypass tests – when configuring Selector Lists.
 - d. Pair-wise consistency test for public and private key establishment (RSA).
4. If a self-test fails, the module will enter a soft error state and output an error indicator specifying the test that failed and the reason for the failure. No commands can be entered when in this error state. The module must be rebooted to leave this error state.
5. At any time the Motorola GGM 8000 Gateway is in an idle state, the operator can command the gateway to perform the power up self-test by power-cycling or rebooting the gateway.
6. Data output is inhibited during key generation, self-tests, zeroization, and error states.
7. To enter the alternating bypass state, the two required independent internal actions that are required are first, to configure the module for alternating bypass, and second, to verify the integrity of the configuration by running the alternating bypass test.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. Crypto-Officer Guidance

The module is distributed to authorized operators wrapped in plastic with instructions on how to securely install the module. On initial installation, perform the following steps:

1. Power on the module and verify successful completion of power up self-tests from console port or inspection of log file. The following message will appear on the console interface: “power-on self-tests passed”.
2. Authenticate to the module using the default operator acting as the Crypto-Officer with the default password and username.
3. Verify that the Hardware and Firmware P/Ns and version numbers of the module are the FIPS Approved versions.
4. Change the Crypto-Officer and User passwords using the **SysPassWord** command.
5. Initialize the Key Encryption Key (KEK) with the **KEKGenerate** command. Account passwords and certain keys are persistent across reboots and are encrypted with the Key Encryption Key (KEK). This key can be reinitialized at any time.
6. Configure the module as described in Section 3, Table 4.

The module supports a minimum password length of 7 characters and a maximum length of 15 characters. The Crypto-Officer controls the minimum password length through the **PwMinLength** parameter: **SETDefault -SYS PwMinLength = <length>**, where **<length>** specifies the minimum length.

The Zeroization Service should also be invoked to zeroize all CSPs prior to removing a gateway from service for repair.

10. Physical Security Policy

Physical Security Mechanisms

The Motorola GGM 8000 Gateway is composed of industry standard production-grade components. To meet FIPS 140-2 Level 2 requirements, the Motorola GGM 8000 Gateway must have tamper-evident seals applied as described in this section. It is the responsibility of the Crypto-Officer to maintain the tamper seals. The seals should be inspected for evidence of tamper every three (3) months. If evidence of tamper has been identified, the module should be considered compromised and Customer Service should be contacted for further instructions. The tamper evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. Please see Appendix A for specific instructions on installation of the tamper labels.

Note: A FIPS label kit can be ordered by using part number CLN8787A, Rev. B.

11. Mitigation of Other Attacks Policy

The Motorola GGM 8000 Gateway has not been designed to mitigate against other attacks outside the scope of FIPS 140-2.

12. Definitions and Acronyms

AES – Advanced Encryption Standard

CBC – Cipher Block Chaining

CLI – Command Line Interface

CSP – Critical Security Parameter

DRBG – Deterministic Random Bit Generator

DH – Diffie-Hellman

FRF – Frame Relay Forum

FRF.17 – Frame Relay Privacy Implementation Agreement

FRPP – Frame Relay Privacy Protocol

HMAC – Hash Message Authentication Code

IKE – Internet Key Exchange

IP – Internet Protocol

IPsec – Internet Protocol Security

KAT – Known Answer Test

KDF – Key Derivation Function

KEK – Key Encrypting Key

MNR – Motorola Network Router

OSPF – Open Shortest Path First

PFS – Perfect Forward Secrecy

RNG – Random Number Generator

SHA – Secure Hash Algorithm

SSH – Secure Shell

SNMP – Simple Network Management Protocol

Tanapa – The part number that is built and stocked for customer orders.

GGM 8000 GATEWAY TAMPER EVIDENCE LABEL INSTALLATION INSTRUCTIONS

Follow these steps to install tamper evidence labels on the GGM 8000 gateway:



The surface to which the labels will be attached must be at a temperature of at least +10°C (+50°F), and the surface must be clean and dry. Clean any grease, dirt, oil, or adhesive residue from the areas to which the labels are to be attached before applying the tamper evidence labels. If you are replacing tamper evidence labels (after a repair, for example), remove the old labels and any adhesive residue with isopropyl alcohol (99% concentration) prior to applying the new labels.

1. Wipe the surface clean with isopropyl alcohol (99% concentration) to remove surface contaminants. Please note that using a solution with an isopropyl alcohol concentration less than 99% is not acceptable.
2. **Do not allow excess alcohol to air dry.** Use a clean paper towel or cotton cloth to completely remove any excess alcohol, thereby removing any residual contaminants.
3. Apply tamper evidence labels 1, 2, and 3 (optional) to secure the GGM 8000 base module and blank filler panel on the front of the chassis.

Do not push labels 1, 2, and 3 all the way up under the top cover overhang or tuck the labels into the gap between the front panel and the top cover overhang. As shown in Detail A in [Figure 1](#), the labels should come out at approximately a 45 degree angle from where they are affixed to the front panel to where they wrap around and over the top cover.

- a. Remove the Kraft liner from the back of label 1 and attach the label as illustrated in [Figure 1](#) (GGM 8000 base unit (base module and blank filler panel)) :
Center the silver portion of the label between the rightmost cooling hole and the Encrypt, Run, Load, and Test LEDs, with the Motorola logo on the label lined up with the top of the Load LED. Starting from the short edge of the label that is positioned on the front panel, affix the label by applying pressure while pushing the label up the front panel and onto the top cover.

- b.** Remove the Kraft liner from the back of label 2 and attach the label as illustrated in [Figure 1](#) (GGM 8000 base unit (base module and blank filler panel)). Position the Motorola logo edge of the label directly above the top edge of connector “5B” with the left edge of the clear portion of the label aligned with the edge of the thumbscrew. Starting from the short edge of the label that is positioned on the front panel, affix the label by applying pressure while pushing the label up the front panel and onto the top cover.



NOTE

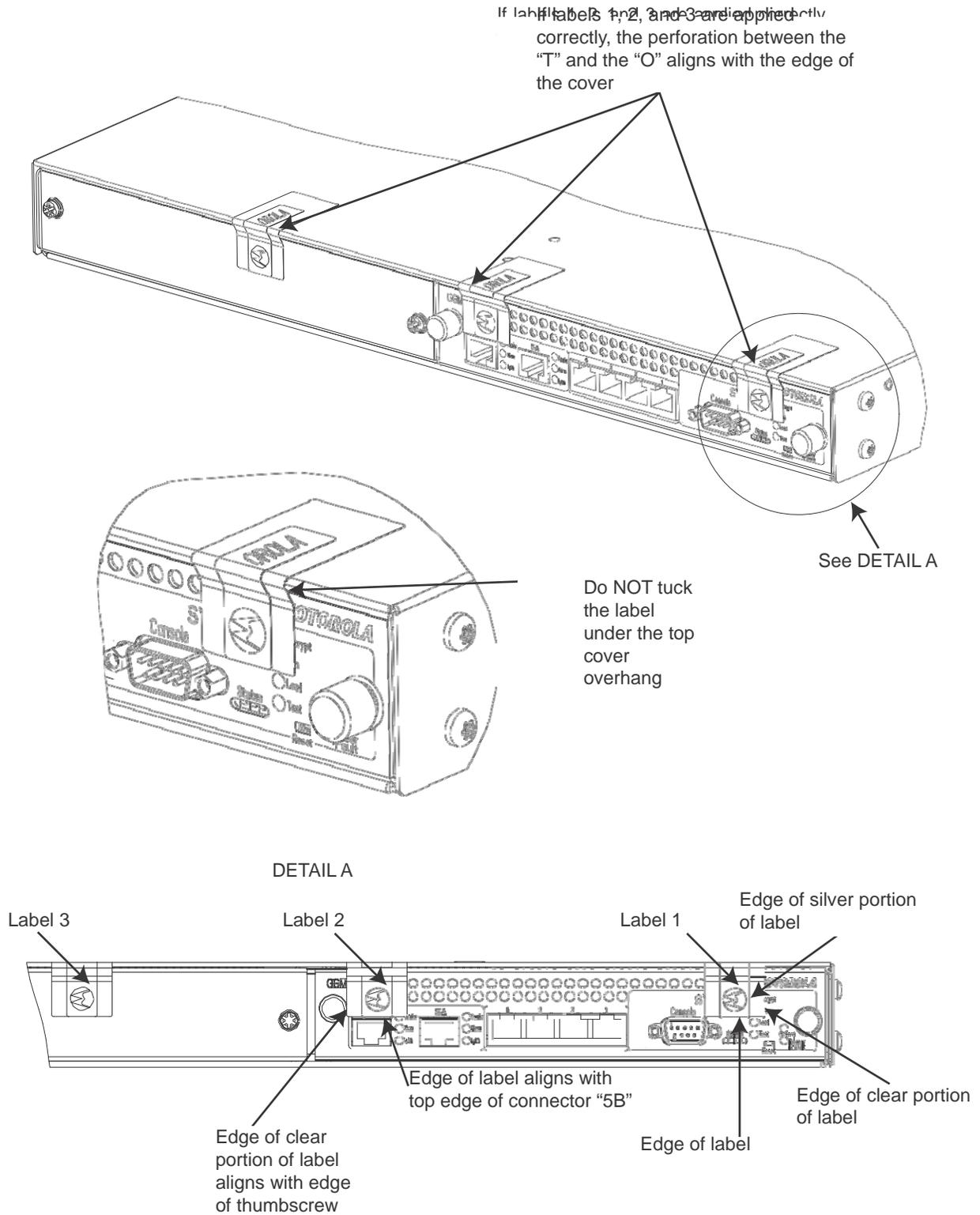
Label 3 is optional and is not required for a FIPS-approved configuration. The additional tamper evidence label provides additional tamper evidence beyond the module cryptographic boundary.

- c.** Remove the Kraft liner from the back of label 3 and attach the label as illustrated in [Figure 1](#).

Position the label approximately in the middle of the blank panel with the perforation between the “T” and the “O” aligned with the edge of the top cover. Starting from the short edge of the label that is positioned on the front panel, affix the label by applying pressure while pushing the label up the front panel and onto the top cover.

- d.** Rub the labels on the front and top of the chassis for 2 seconds to ensure that the labels have adhered.

FIGURE 1 APPLYING TAMPER EVIDENCE LABELS 1, 2, AND 3 TO SECURE THE GGM 8000 BASE UNIT (BASE MODULE AND BLANK FILLER PANEL IN EXPANSION MODULE SLOT



4. Apply tamper evidence **label 4** to secure the GGM 8000 power supply module on the rear of the chassis.



NOTE

These instructions apply to a GGM 8000 equipped with either an AC or a DC power supply module.

- a. Remove the Kraft liner from the back of the label and position the label as illustrated in Figure 2.



Figure 2 illustrates the label placement for the AC power supply module. The label placement for the DC power supply module is the same.

Position the Motorola logo edge of the label directly above the mounting screw, with the right edge of the silver portion of the label aligned with the right edge of the power supply module. Starting from the short edge of the label that is positioned on the rear panel, affix the label by applying pressure while pushing the label up the rear panel and onto the top cover.

- b. Rub the label on the top and rear of the chassis for 2 seconds to ensure that the label has adhered.

5. Secure the unit in a restricted area.
6. Allow the applied labels to cure for at least 4 hours; do not touch the labels during this time.

If you need to re-apply the tamper evidence labels to the GGM 8000, repeat steps 1-6.

FIGURE 2 APPLYING TAMPER EVIDENCE LABEL 4 TO SECURE THE GGM 8000 POWER SUPPLY MODULE (AC OR DC)

