Motorola Network Router (MNR) S6000

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Version: 3.0

Date: 6/21/2016

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Motorola Network Router (MNR) S6000, hereafter denoted the Module. The Module is a network router supporting secure integrated voice and data applications as well as high-speed site-to-site WAN connections. In addition to the normal routing functions, the MNR S6000 supports data encryption and authentication over Ethernet and Frame Relay links using the IPSec and FRF.17 protocols. The Module meets FIPS 140-2 overall Level 1 requirements.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version
1	MNR S6000 Base Unit	CLN1780L Rev F	GS-16.8.1.06
2	S6000 Encryption Unit	CLN8261D Rev NA	N/A

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated network appliances. The Module is a multi-chip standalone embodiment; the cryptographic boundary is the module's enclosure which includes all components.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

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

The Module implementation is compliant with:

- FIPS 140-2
- FIPS 197
- SP 800-38A
- SP 800-90A

- FIPS 198-1
- SP 800-135
- FIPS 186-4
- FIPS 180-4
- SP 800-20

1.1 Hardware and Physical Cryptographic Boundary

The physical cryptographic boundary of the Module is depicted in Figure 1. In the photo, blank plates cover slots that can hold optional network interface cards that are external to the boundary of the module.

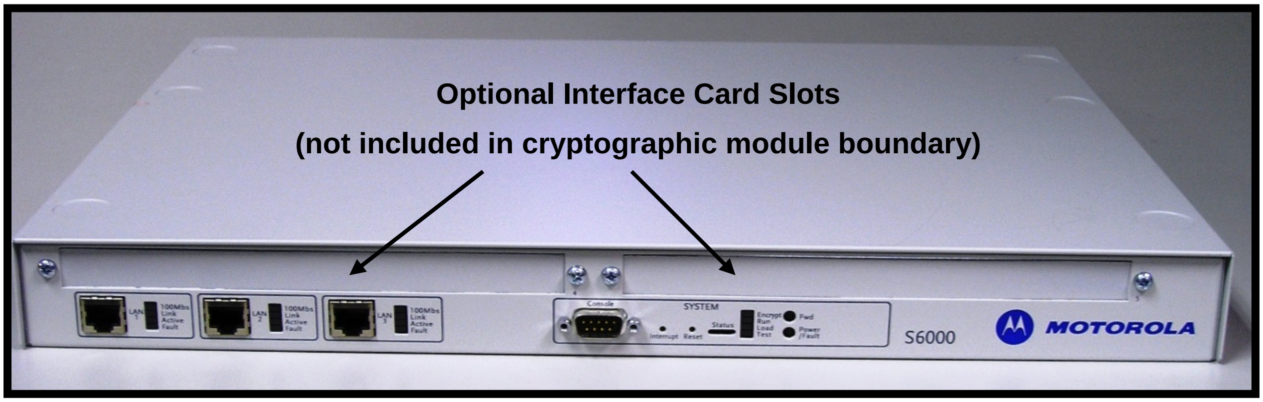

Figure 1 – Motorola Network Router (MNR) S6000

Table 3 – Ports and Interfaces

Physical Port	Qty	Logical interface definition	Interface Card	Description
Ethernet	3	Data input, data output, status output, control input	Part of the S6000 Base system	LAN port that provides connection to Ethernet LANs using either 10BASE-T or 100BASE-TX Ethernet
Console	1	Status output, control input	Part of the S6000 Base system	RS-232 interface
Power Plug	1	Power input	N/A	Power
LEDs	7	Status output	N/A	Provides LED status output on network traffic, power, and errors

1.2 Modes of Operation

The module supports both an Approved and non-Approved mode of operation. 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.	Check if FIPS mode is enabled using the **show –SYS FIPS** command. If **FIPS = ON**, go to next step. If **FIPS = OFF**, issue **SETD -SYS FIPS=ON** command.
2.	Configure the parameters for the IKE negotiations using the **IKEProfile** command. For FIPS mode, only the

Step	Description
	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).
3.	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>** For FIPS mode, minimum key length is 14 bytes.
4.	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).
5.	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).
6.	For each port for which encryption is required, bind a dynamic policy to the ports using: **ADD [!<portlist>] –CRYPTO DynamicPOLicy <policy_name> <priority>** **<mode> <selctrlist_name> <xfrmlist_name> [<pfs>] [<lifetime>] [<preconnect>]** To be in FIPS mode, the selector list and transform list names must be defined as in previous steps.
7.	If PIM authentication is enabled, configure Manual Key set using the **ADD –CRYPTO ManKeySet** command. For FIPS mode, minimum authentication key length is 14 bytes.
8.	If SNMPv3 is enabled, configure authentication and encryption passphrases for all SNMP users with AuthPriv privileges. For FIPS mode, minimum authentication passphrase length is 14 bytes.
9.	If SSHv2 is enabled, generate RSA 2048 bit keys using **GenSshKey RSA 2048**.
10.	For each port for which encryption is required, enable encryption on that port using: **SETDefault [!<portlist>] –CRYPTO CONTrol = Enabled**
11.	DSA keys must not be used in FIPS mode.
12.	Use the **Show –SYS SwSignatureAlgorithm** command to verify that firmware signing algorithm is set to SHA2withRSA2048. If not use the **SetD –SYS SwSignAlgorithm = SHA2withRSA2048** command to change signing algorithm.
13.	FIPS-140-2 mode achieved.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the table(s) below.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES (Hardware Implementation)	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, CTR Key sizes: 128, 192, 256 bits (ECB, CBC only)	173
AES (Firmware Implementation)	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, CFB128 Key sizes: 128, 192 (CBC only), 256 bits (CBC only)	3547
DRBG	[SP 800-90A] Functions: Hash DRBG Security Strengths: 256 bits	903
HMAC (Hardware Implementation)	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1 Key Size: 160 bits	39
HMAC (Firmware Implementation)	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-256 Key Size: minimum 112 bits	2265, 2266
KDF, Existing Application-Specific (CVL)	[SP 800-135] Functions: SSH KDF, SNMP KDF, IKE v1 KDF, IKEv2 KDF	603, 604, 605
RSA	[FIPS 186-4, PKCS #1 v2.1 (PKCS1.5)] Functions: Key Generation, Signature Generation, Signature Verification Key sizes: 1024 (RSA Verify only), 2048 bits	1827
SHA (Hardware Implementation)	[FIPS 180-4] Functions: Message Digest SHA size: SHA-1	258
SHA (Firmware Implementation)	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1, SHA-256	2926

Algorithm	Description	Cert #
Triple-DES (TDEA) (Hardware Implementation)	[SP 800-20] Functions: Encryption, Decryption Modes: TCBC Key sizes: 3-key	275
Triple-DES (TDES) (Firmware Implementation)	[SP 800-20] Functions: Encryption, Decryption Modes: TCBC Key sizes: 3-key	1986

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Non-SP 800-56A Compliant DH	[IG D.8] Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
NDRNG	[Annex C] Hardware Non-Deterministic RNG; minimum of 32 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG.

Table 6 – Protocols Allowed in FIPS Mode

Protocol	Description
IKE v1	[IG D.8 and SP 800-135] Cipher Suites: Oakley Group 1,2, 5 and 14 DH key agreement with PreSharedKey authentication, AES or Triple-DES CBC encryption, SHA-1 hashing, and HMAC PRF
IKE v2	[IG D.8 and SP 800-135] Cipher Suites: Oakley Group 1,2,5 and 14 DH key agreement with PreSharedKey authentication, AES or Triple-DES CBC encryption, HMAC-SHA-1 integrity and PRF
SNMPv3	[IG D.8 and SP 800-135] Allowed only with the *SP 800-135* SNMP KDF and AES encryption/decryption
SSH v2	[IG D.8 and SP 800-135] Cipher Suites: RSA 2048 DH group 14 SHA-1 key transport, AES CBC encryption, HMAC-SHA-1 MAC

Note: these protocols have not been reviewed or tested by CMVP or CAVP

Non-Approved Cryptographic Functions for use in non-Approved mode only:

- DES
- Triple-DES (2-Key)
- FIPS 186-4 RSA Signature Generation: 4096 bit keys with SHA-2

- MD5
- HMAC-MD5
- HMAC-SHA-1-96
- DSA 1024-bit – for public/private key pair generation and digital signatures (non-compliant)
- RSA 1024 – for key transport within SSH v2
- Non approved SW RNG: Provides random numbers for networking functions (non-compliant)
- Diffie-Hellman Group 1, 2 and 5

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 7 – Critical Security Parameters (CSPs)

CSP	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
SKEYSEED	Seed value is generated from initiator and responder nonce values and DH – pre-shared key. Used in IKEv2 IKE_SA
SK_d	Key used to derive keying material for the CHILD_SAs established with IKEv2 IKE_SAs
SK_ai	Key used by initiator as a key to the integrity protection algorithm for authenticating the component messages in IKEv2 IKE_SA
SK_ar	Key used by responder as a key to the integrity protection algorithm for authenticating the component messages in IKEv2 IKE_SA
SK_ei	Key used by initiator for encrypting and decrypting all subsequent exchanges in IKEv2 IKE_SA
SK_er	Key used by responder for encrypting and decrypting all subsequent exchanges in IKEv2 IKE_SA
SK_pi	Key used by initiator when generating an AUTH payload in IKEv2 IKE_SA
SK_pr	Key used by responder when generating an AUTH payload in IKEv2 IKE_SA

CSP	Description / Usage
*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	128-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 used to encrypt and authenticate SNMPv3 packets
RADIUS Secret	Used for authentication of packets sent/received to RADIUS Server, up to 32 characters.
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 • Crypto-Officer (Super User) • Network Manager • Admin • User	7 (to 15) character password used to authenticate to the module

2.2 Public Keys

Table 8 – Public Keys

Key	Description / Usage
RSA Firmware Load Key	RSA 2048 bit key used for firmware authentication
SSH-RSA Key	(RSA 2048-bit) Distributed to peer, used for SSH authentication
SSH Known Host Keys	(RSA 1024 and 2048-bit) Distributed to module, used to authenticate peer
IKE DH public key (g^a)	(2048-bit) Generated for IKE Phase 1 key establishment
IKE DH phase-2 public (g^a) key	(2048-bit) Phase 2 Diffie-Hellman public keys used in PFS for key renewal (if configured)
SSH DH Key	(2048-bit) Generated for SSH key establishment

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports eight distinct operator roles, Cryptographic Officer (Super User), Admin, Network Manager, User, Maintenance, MotoAdmin, MotoMaster, and MotoInformA/B. The cryptographic module enforces the separation of roles using Role-based authentication.

Table 10 lists all operator roles supported by the module. The Module supports concurrent operators. Each operator has an independent session with the gateway, either though 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 role-based authentication capabilities will be described here, although the role based-authentication is not required to comply with Level 1 requirements.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
Crypto-Officer (Super User)	The owner of the cryptographic module with full access to services of the module.	Role-based operator authentication.	Username and Password
Network Manager (NM)	An operator of the module with almost full access to services of the module.	Role-based operator authentication.	Username and Password
Admin	An assistant to the Crypto-Officer that has read only access to a subset of module configuration and status indications.	Role-based operator authentication.	Username and Password
User	A user of the module that has read only access to a subset of module configuration and status indications.	Role-based operator authentication.	Username and Password
Maintenance	Maintenance role can be entered via the external console port (unauthenticated) or via EOS software command (requires Network Manager authentication)	Unauthenticated maintenance role is entered only via the router console port	None

Role ID	Role Description	Authentication Type	Authentication Data
MotoAdmin (MO)	A SNMPv3 user who can issue any command from the SNMP V3 User Manager menu.	Role-based operator authentication.	Passphrase
MotoMaster (MM)	A SNMPv3 user who can change its own passphrases from the SNMP V3 User Manager menu.	Role-based operator authentication.	Passphrase
MotoInformA/B (MI)	A SNMPv3 user who receives and transmits reliable messages over SNMPv3.	Role-based operator authentication.	Passphrase

3.2 Authentication Methods

Username and Password

Passwords are alphanumeric strings consisting of 7 to 15 characters chosen from the 94 standard keyboard characters. 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.

Passphrase

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 (! “ % & ” ( ) * + , - . /: ; < = > ?).

The probability that a random attempt will succeed or a false acceptance will occur is 1/81^8 which is less than 1/1,000,000. The timing of the SNMPv3 authentication protocol as implemented limits the probability of randomly guessing a SNMPv3 passphrase in 60 seconds to less than 1 in 100,000. Based on processing speeds, roughly 12 authentication attempts via passphrase are possible in a one (1) minute period. Therefore the probability that a false acceptance will occur in a one minute period is 12/81^8.

3.3 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Table 10 – Authenticated Services

Service	Description	CO	NM	Admin	User	Main.	MO	MM	MI
Firmware Update	Load firmware images digitally signed by RSA (2048 bit) algorithm	X	X						
Key Entry	Enter Pre-Shared Keys (PSK)	X	X						
User Management	Add/Delete and manage operator passwords	X	X						
Reboot	Force the module to power cycle via a command	X	X						
Zeroization	Actively destroy all plaintext CSPs and keys	X	X						
Crypto Configuration	Configure IPsec and FRF.17 services	X	X						
IKE	Key establishment utilizing the IKE protocol	X	X						
IPSec	IPsec protocol	X	X						
FRF.17 Tunnel Establishment	Frame Relay Privacy Protocol	X	X						
Alternating Bypass	Provide some services *with* cryptographic processing and some services *without* cryptographic processing	X	X						
SSHv2	For remote access to the gateway	X	X						
Network Configuration	Configure networking capabilities	X	X						
SNMPv3	Network management, including traps and configuration	X	X				X	X	X
Enable Ports	Apply a security policy to a port	X	X						
File System	Access file system	X	X						
Authenticated Show Status	Provide status to an authenticated operator	X	X	X	X				

Service	Description	CO	NM	Admin	User	Main.	MO	MM	MI
Access Control	Provide access control for Crypto-Officer, Network Manager, Admin, and User	X	X	X	X				

Table 11 – Unauthenticated Services

Service	Description
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
Monitor	Perform various HW support services

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

Table 122 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 12 – CSP Access Rights within Services

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 Keys	-	*W*	-	*E*	-	-	-	-	*Z*	*RW*	-	-	-	-	*EW*	*E*	-
SKEYID	-	-	-	*EG*	-	-	-	*Z*	*Z*	-	-	-	-	-	-	-	-
SKEYID_d	-	-	-	*EG*	-	-	-	-	*Z*	-	-	-	-	-	-	-	-

SKEYID_a	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SKEYID_e	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SKEYSEED	-	-	-	EG	-	-	-	Z	Z	-	-	-	-	-	-	-	-
SK_d	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SK_ai	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SK_ar	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SK_ei	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SK_er	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SK_pi	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
SK_pr	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
Ephemeral DH Phase-1 private key (a)	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
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 Passphrases	-	-	EW	-	-	-	-	-	Z	-	-	E	-	-	-	-	-
SNMPv3 Session Keys	-	-	-	-	-	-	-	-	-	-	-	EGZ	-	-	-	-	-
DRBG Seed	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
DRBG Internal State	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-

4 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 13 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 the error state. KAT failure is indicated by the device not being able to power up.

Table 13 – Power Up Self-tests

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code in flash
AES (Hardware implementation)	KATs: Encryption, Decryption Modes: CBC Key sizes: 128 bits
AES (Firmware implementation)	KATs: Encryption, Decryption Modes: ECB, CBC Key sizes: 128, 192, 256 bits
DRBG	KATs: HASH DRBG Security Strengths: 256 bits
HMAC (Hardware implementation)	KATs: Generation, Verification SHA sizes: SHA-1 Includes hardware SHA-1 KAT
HMAC (Firmware implementation)	KATs: Generation, Verification SHA sizes: SHA-1
RSA	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits
SHA	KATs: SHA-1, SHA-256
TDES (Hardware implementation)	KATs: Encryption, Decryption Modes: TCBC, Key sizes: 3-key
TDES (Firmware implementation)	KATs: Encryption, Decryption Modes: TCBC, Key sizes: 3-key

Table 14 – Conditional Self-tests

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
Firmware Load	RSA 2048 signature verification performed when firmware is loaded.
RSA Pairwise Consistency	Pair-wise consistency test for public and private key generation (RSA)
DRBG Health Checks	Performed conditionally per SP 800-90 Section 11.3. Required per IG C.1.
Bypass Test	Bypass Test performed when the service Alternating Bypass is called.

5 Physical Security Policy

The MNR S6000 router is composed of industry standard production-grade components.

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The Motorola MNR S6000 Gateway has not been designed to mitigate against other attacks outside the scope of FIPS 140-2.

8 Security Rules and Guidance

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

1. The Motorola MNR S6000 Gateway provides eight distinct operator roles: Crypto-Officer (Super User), Admin, Network Manager, User, Maintenance, MotoAdmin, MotoMaster, and MotoInformA/B. The Crypto-Officer role uses the Super User account.
2. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
4. Power up self-tests do not require any operator action.
5. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

7. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
8. The module does not support a maintenance interface or role.
9. The module does not support manual key entry.
10. The module does not have any external input/output devices used for entry/output of data.
11. The module does not enter or output plaintext CSPs.
12. The module does not output intermediate key values.

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.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011

Table 16 – Acronyms and Definitions

Acronym	Definition
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
PIM	Protocol Independent Multicast
RNG	Random Number Generator
SHA	Secure Hash Algorithm
SSH	Secure Shell

Acronym	Definition
SNMP	Simple Network Management Protocol
Tanapa	The part number that is built and stocked for customer orders