MOTOROLA SOLUTIONS

Motorola Network Router (MNR) S6000

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 5.7

Date: 4/27/2021

MOTOROLA SOLUTIONS

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	CLN1780N Rev AB	18.2.2.03
2	S6000 Encryption Unit	CLN8261D Rev NB	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

MOTOROLA SOLUTIONS

- FIPS 198-1
- SP 800-135
- FIPS 186-4
- FIPS 180-4
- SP 800-56A rev3
- SP 800-132

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.
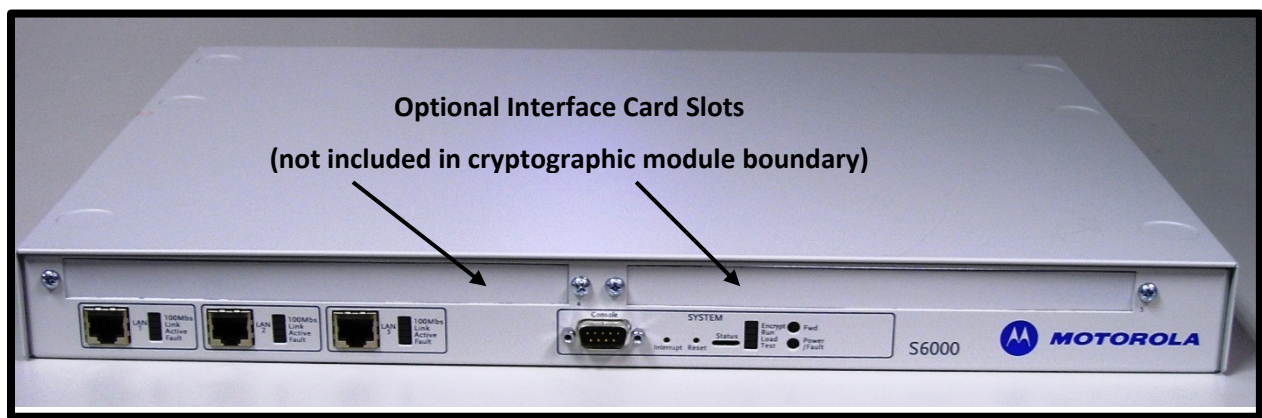
Figure 1 – Motorola Network Router (MNR) S6000

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 FIPS mode 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*.

Table 4 – FIPS Approved Mode Configuration

Step	Description
1.	To ensure the module does not retain any CSPs between mode changes, issue the **ZEROize** command.
2.	Enable FIPS mode by issuing the SETD -SYS FIPS=ON command.
3.	Create a new KEK using the KEKGenerate command.
4.	Change the Crypto-Officer and User passwords using the **SysPassWord** command. Recreate all necessary local users using the **UserManager** menu.
5.	Ensure the module is not configured to use IKEv2 (only v1 is supported in FIPS mode).
6.	Configure the parameters for the IKE negotiations using the **ADD -CRYPTO IKEProfile** command. For FIPS mode, only the following values are allowed: Diffie-Hellman Group (Group 14 required for 112-bit key strength, Group 19 for 128-bit key strength or Group 20 for 192-bit key strength), Encryption Algorithm (AES), Hash Algorithm (SHA, SHA-256 or SHA-384), and Authentication Method (PreSharedKey, RSA-Signature, ECDSA-256 or ECDSA-384).
7.	If PreSharedKey is used as Authentication Method, electronically establish via the local console port the pre-shared key (PSK) to be used for the IKE protocol using: **ADD -CRYPTO FipsPreShrdKey <peer_ID> <pre-shared_key> <pre-shared_key>** For FIPS mode, minimum key length is 14 bytes.

8.	If RSA-Signature, ECDSA-256 or ECDSA-384 is used as Authentication Method:
	
	    a. Unlock PKI database using:
	       SETD -PKI CONTrol = Unlocked
	    b. Generate key pair using:
	       ADD -PKI KeyPair [<profile>] [<RSA|ECDSA>] <256|384|2048>
	    c. Set identity of the device by executing at least one of the following commands:
	       SETD -PKI DNSName = <dns-name>
	       SETD -PKI IPADDress = <ip-address>
	       SETD -PKI EmailADDress = <email-address>
	       SETD -PKI SubjectName = <subject-name>
	    d. Generate CSR using:
	       ADD -PKI CertReq <certreq-profile>
	    e. Use external CA to generate certificate from CSR
	    f. Install chain of certificates using:
	       ADD -PKI CERTificate <profile> <Self|TrustedCA|UnTrusted> InputFile <local-file-name>
	    g. Lock PKI database using:
	       SETD -PKI CONTrol = Locked

9.	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-AES) and Authentication Transform (ESP-SHA).

MOTOROLA *SOLUTIONS*

Step	Description
10.	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-AES) and Authentication Transform (FRF-SHA)
11.	Configure the selector list using command(s): **ADD -CRYPTO SelectorLIst \<slctrlist_name> \<priority> [\<actions>] \<filters> (\<src_ipaddr/mask> | \<src_ip_range>) (\<dst_ipaddr/mask> | \<dst_ip_range>)** The selector list defines the rules for network traffic to be protected. In particular, the selector list can be defined to protect all network traffic.
12.	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.
13.	If PIM authentication (RFC 4601) is enabled, configure Manual Key set using the **ADD -CRYPTO ManKeySet** command. For FIPS mode, minimum authentication key length is 14 bytes.
14.	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.
15.	If SSHv2 is enabled, generate RSA 2048 bit keys using **GenSshKey RSA 2048**.
16.	If Radius server is used for user authentication: • Add a radius secret using the **setd -ac secret** command. • Configure IPsec tunnel between the module and the Radius server as described in steps:6-12.
17.	For each port for which encryption is required, enable encryption on that port using: **SETDefault [!\<portlist>] -CRYPTO CONTrol = Enabled**
18.	DSA keys must not be used in FIPS mode.
19.	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.
20.	**Copy** command must not be used to transfer files outside the module in FIPS mode. SCP protocol can be used instead of.
21.	Telnet access to the module should be blocked by issuing the following command: **SETDefault -SYS NetAccess = NoTelnet.**
22.	FIPS-140-2 mode achieved.

Note: To switch the Module to a non-approved mode, perform Step 1 to zeroize the CSPs and use the **SETD -SYS FIPS=OFF** command.

MOTOROLA *SOLUTIONS*

2 Cryptographic Functionality

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

Table 5 – 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	173
AES (Firmware Implementation)	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, CFB128, CTR Key sizes: 128 (ECB, CBC, CFB, CTR), 192 (ECB, CBC, CTR), 256 (ECB, CBC, CTR) bits	C1721
DRBG	[SP 800-90A] Functions: Hash DRBG Security Strengths: 256 bits	C1721
ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification, Public Key Validation. Curves: P-256 with SHA-256, P-384 with SHA-384	C1721
HMAC (Hardware Implementation)	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1 Key Size: 160 bits	39
HMAC (OpenSSL Firmware Implementation)	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512 Key Size: minimum 160 bits, maximum 1160 bits	C1721
HMAC (OpenSSH Firmware Implementation)	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-256 Key Size: minimum 160 bits, maximum 640 bits	C1722
KDF, Existing Application-Specific (CVL)	[SP 800-135]	
	SSH KDF	C1722
	SNMP-KDF	C1723

MOTOROLA SOLUTIONS

Algorithm	Description	Cert #
	IKEv1 KDF	C2054
KTS	[SP800-38F §3.1] Functions: Key Unwrap Modes: AES-CTR + HMAC-SHA-1 (160 bits) or HMAC SHA-256, AES-CBC + HMAC SHA-1(160 bits) or HMAC SHA-256	AES C1721 HMAC C1721, C1722
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; with SHA-1 (Verify only), SHA-256 and SHA-384	C1721
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, SHA-384, SHA-512	C1721

Table 6 – Approved Cryptographic Functions Tested with Vendor Affirmation

Algorithm	Description
CKG	[SP 800-133] In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.
KAS	[SP 800-56A rev3] Functions: Key Pair Generation, Full Validation Modes: FFC, ECC Roles: Initiator, Responder Parameter sets for FFC mode: DH Groups 14, 16 and 18 Parameter sets for ECC mode: DH Groups 19 and 20

MOTOROLA *SOLUTIONS*

Algorithm	Description
PBKDF2	[SP 800-132] This function is used only in the Password Storage component. The 64-byte long Master Key is calculated from the variable length PBKDF Password and 16 random bytes of salt, using HMAC-SHA-512 as a Pseudorandom Function and the iteration count set to 1000. The PBKDF Password is either 16 bytes of the hashed (MD5) user password (for Crypto Officer and Admin roles) or concatenated user name and variable length (7-15 bytes) user password (for Network Manager and User roles). The Master Key (equivalent to Data Protection Key – Option 1a is chosen as described in the referenced Special Report) is stored together with the randomly generated salt for each user and it is used in the process of user's authentication. For Crypto Officer and Admin roles, the probability that a random attempt of guessing PBKDF Password will succeed is $1/256^{16}$ which is less than $1/10^{38}$. Note however that the user cannot pass the PBKDF Password directly to the algorithm, since it is internally calculated from the user's password. In this case the probability that a random attempt of guessing PBKDF Password will succeed is given in Section 3.2 of this document. For Network Manager and User roles, the probability that a random attempt of guessing PBKDF Password will succeed is given in Section 3.2 of this document. The derived keys from the PBKDF may only be used in storage applications.

Table 7 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
HMAC-MD5	Used in Radius in approved mode but no security is claimed
NDRNG	[Annex C] Hardware Non-Deterministic RNG; minimum of 32 bits per access. The NDRNG output (256-bits) is used to seed the FIPS Approved DRBG.

Table 8 – Protocols Allowed in FIPS Mode

Protocol	Description
IKE v1	[IG D.8 and SP 800-135] Cipher Suites: • Oakley Group 14 DH key agreement or Oakley Group 19 and 20 ECDH key agreement • PreSharedKey, RSA-Signature, ECDSA-256 or ECDSA-384 authentication • AES CBC encryption • SHA-1, SHA-256 or SHA-384 hashing • HMAC as PRF

MOTOROLA SOLUTIONS

Protocol	Description
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 and SHA-256, DH groups 16 and 18 SHA-512 key establishment, AES CBC or CTR encryption, HMAC-SHA-1 MAC, HMAC-SHA-256 MAC

Note: The IKEv1, SNMPv3 and SSH protocols, other than the KDF, have not been tested by the CMVP or CAVP as per FIPS 140-2 Implementation Guidance D.11.

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

- DES
- Triple-DES
- FIPS 186-4 RSA Signature Generation: 4096-bit keys with SHA-2
- 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
- IKEv2 KDF (non-compliant)
- Non-SP 800-38F Compliant Key Wrap: AES-ECB Key Wrap and Key Unwrap (key wrapping; key establishment methodology provides 128 bits of encryption strength)

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 3.

Table 9 – 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	Minimum 14 bytes long key used to authenticate peer to peer during IKE session
PKI private key	2048-bit RSA or 256/384-bit ECDSA key used for certificate request signing and IKEv1 authentication

MOTOROLA SOLUTIONS

CSP	Description / Usage
SKEYID	HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-384 (160-384 bits), 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	HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 (160-384 bits) of Preshared Session key, DH keys and cookies Phase 1 key used to derive keying material for IKE SAs
SKEYID_a	HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 (20-48 bytes) of SKEYID_d, DH keys and cookies Key used for integrity and authentication of the phase 1 exchange
SKEYID_e	HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 of SKEYID_a, DH keys and cookies Key used for AES data encryption of phase 1 exchange
Ephemeral DH Phase-1 private key (a)	2048/6144/8192-bit key generated for IKEv1 Phase 1 key establishment
Ephemeral ECDH Phase-1 private key	256/384-bit key generated for IKEv1 Phase 1 key establishment
Ephemeral DH Phase-2 private key (a)	Phase 2 2048/6144/8192-bit Diffie-Hellman private keys used in PFS for key renewal
Ephemeral ECDH Phase-2 private key	Phase 2 256/384-bit Elliptic Curve Diffie-Hellman private keys used in PFS for key renewal
IPsec Session Enc Key	128/256-bit AES-CBC keys are used to encrypt IPsec ESP packets
IPsec Session Auth Key	160-bit key HMAC-SHA-1 is used to authenticate IPsec ESP packets
FRF.17 Session Enc Key	128/256-bit AES-CBC keys are used to encrypt FRF.17 Mode 2
FRF.17 Session Auth Key	160-bit key HMAC-SHA-1 is used to authenticate FRF.17 Mode 2
SSH-RSA Private Key	2048-bit RSA Key used to authenticate oneself to peer
SSH Session Enc Key	128/192/256-bit AES-CBC or AES-CTR keys are used to encrypt SSH packets
SSH Session Auth Key	256-bit HMAC-SHA-1 key is used to authenticate SSH packets
SSH DH Private Key	Generated for SSH key establishment
SNMPv3 Passphrases	Passphrases, with a minimum length of 14 bytes, used in generation of SNMPv3 session keys

MOTOROLA SOLUTIONS

CSP	Description / Usage
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. By default RADIUS connection is not used. To enable it at least the following commands need to be executed: SETDefault -AC PrimACcntSrvr = <radius_server_ip_address> SETDefault -AC RESolutionOrder = Radius SETDefault -RAS SecurityType = Radius Only then, when the user will try to log in, the module will exchange packets with the RADIUS server.
Hash-DRBG Seed	Initial 256-bit 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 10 – 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 ECDH public key	(256/384-bit) Generated for IKEv1 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)
IKE ECDH phase-2 public key	(256/384-bit) Phase 2 Elliptic Curve Diffie-Hellman public keys used in PFS for key renewal (if configured)
SSH DH Key	(2048-bit) Generated for SSH key establishment
PKI public key	(RSA 2048-bit or ECDSA 256/384-bit) Generated for IKEv1 authentication

MOTOROLA *SOLUTIONS*

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports eight distinct operator roles, Crypto-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. Authentication as the Crypto Officer and Network Manager means also authentication as User role and allows to drop down to the User privilege level without a password.

Table 11 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 (via console), or over SNMPv3 (via Ethernet port) when specified. 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 11 – 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
MotoAdmin (MO)	A SNMPv3 user who can issue any command from the SNMP V3 User Manager menu.	Role-based operator authentication.	Passphrase

Role ID	Role Description	Authentication Type	Authentication Data
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. Assuming 1 ms for processing each authentication attempt, the probability that a false acceptance will occur in a one-minute period is $60000/81^8 = 3.24/10^{11}$ and it is less than $1/10^5$. One authentication attempt takes about 100 ms in real-life scenario.

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 12 – 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						

MOTOROLA SOLUTIONS

Service	Description	CO	NM	Admin	User	Main.	MO	MM	MI
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						
PKI	Peer to peer authentication for IKEv1	X	X						
IPSec Tunnel Establishment	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				
Access Control	Provide access control for Crypto-Officer, Network Manager, Admin, and User	X	X	X	X				

MOTOROLA *SOLUTIONS*

Table 13 – 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 (by Reboot service, or by physically power cycling the module)
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 14 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 14 – CSP Access Rights within Services

CSP	Firmware Update	Key entry	User Management	IKE	PKI	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	-	-	-	-	REW	E	-
PKI private key	-	-	-	R	EG	-	-	-	-	Z	-	-	-	-	-	RW	-	-
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	-	-	-	-	-	-	-	-
Ephemeral ECDH Phase-1 private key	-	-	-	EG	-	-	-	-	-	Z	-	-	-	-	-	-	-	-
Ephemeral DH Phase-2 private key (a)	-	-	-	EG	-	-	-	-	-	Z	-	-	-	-	-	-	-	-
Ephemeral ECDH Phase-2 private key	-	-	-	EG	-	-	-	-	-	Z	-	-	-	-	-	-	-	-

MOTOROLA *SOLUTIONS*

Key																		
IPsec Session Enc Key	-	-	-	EG	-	E	-	-	-	Z	-	-	-	-	-	-	-	-
IPsec Session Auth Key	-	-	-	EG	-	E	-	-	-	Z	-	-	-	-	-	-	-	-
FRF.17 Session Enc Key	-	-	-	EG	-	-	E	-	-	Z	-	-	-	-	-	-	-	-
FRF.17 Session Auth Key	-	-	-	EG	-	-	E	-	-	Z	-	-	-	-	-	-	-	-
SSH-RSA Private Key	-	-	-	-	-	-	-	EG	-	Z	EG	-	-	-	-	RW	-	-
SSH Session Enc Key	-	-	-	-	-	-	-	EG	-	Z	-	-	-	-	-	-	-	-
SSH Session Auth Key	-	-	-	-	-	-	-	EG	-	Z	-	-	-	-	-	-	-	-
SSH DH Private Key	-	-	-	-	-	-	-	EG	-	Z	-	-	-	-	-	-	-	-
Passwords	-	-	EW	-	-	-	-	-	-	Z	-	-	-	-	-	RW	-	E
RADIUS Secret	-	-	-	-	-	-	-	-	-	Z	-	-	-	-	-	RW	-	EW
SNMPv3 Passphrases	-	-	EW	-	-	-	-	-	-	Z	-	-	E	-	-	RW	-	-
SNMPv3 Session Keys	-	-	-	-	-	-	-	-	-	-	-	-	EGZ	-	-	-	-	-
DRBG Seed	-	-	-	EG	-	-	-	-	-	Z	-	-	-	-	-	-	-	-
DRBG Internal State	-	-	-	EG	-	-	-	-	-	Z	-	-	-	-	-	-	-	-

*For the "File System" service, access to all available keys is limited to the input and output of the ciphertext key block (encrypted with KEK) and password bank (hashed with PBKDF2) as well as on-module backup and restoration.

MOTOROLA *SOLUTIONS*

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 15 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 15 – 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, CTR Key sizes: 128, 192, 256 bits
DRBG	KATs: HASH DRBG Security Strengths: 256 bits
DRBG Health Checks	Performed on power-up per SP 800-90A Section 11.3. - all health tests performed.
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, SHA-256, SHA-384, SHA-512 Performed independently for HMAC Cert. #C1721 and for HMAC Cert. #C1722 (SHA-1, SHA-256 only).
RSA	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits
ECDSA	KATs: Signature Generation, Signature Verification: Curves: P-256, P-384
SHA	KATs: SHA-1, SHA-256, SHA-384, SHA-512
PBKDF2	KATs: Password hash generation

Table 16 – Conditional Self-tests

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

MOTOROLA *SOLUTIONS*

Test Target	Description
RSA Pairwise Consistency	Pair-wise consistency test for public and private key generation (RSA)
ECDSA Pairwise Consistency	ECDSA Full Validation (as specified in SP 800-56A) for peer's ephemeral public key. It is performed by recipient during key agreement and just after ECDSA key pair is generated.
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 Alternating Bypass Mode

The cryptographic module supports an alternating bypass mode. The following two independent actions are needed to activate bypass:

1. Using the Crypto Configuration service, the operator must disable encryption.

2. The user must apply that configuration to a virtual or physical port.

The module confirms the operator's decision by asking for confirmation, and the module checks the configuration file for valid configuration before entering bypass mode.

8 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.

9 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 1 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.

MOTOROLA *SOLUTIONS*

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 supports a maintenance interface.

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.

MOTOROLA *SOLUTIONS*

10 References and Definitions

The following standards are referred to in this Security Policy.

Table 17 – 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*, March 2019

Table 18 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
CSR	Certificate Signing Request
CTR	Counter
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
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

MOTOROLA *SOLUTIONS*

Acronym	Definition
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KEK	Key Encrypting Key
MNR	Motorola Network Router
NDRNG	Non-Deterministic Random Number Generator
OSPF	Open Shortest Path First
PBKDF	Password-based Key Derivation Function
PFS	Perfect Forward Secrecy
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
SNMP	Simple Network Management Protocol
Tanapa	The part number that is built and stocked for customer orders

MOTOROLA *SOLUTIONS*