MOTOROLA

Motorola Network Router (MNR) S6000 FIPS 140-2 Non-Proprietary Security Policy

Document Version 2.9

Revision Date: 7/16/2014

TABLE OF CONTENTS

1. Module Overview

The MNR S6000 router, also referred to as the S6000, is a multi-chip standalone cryptographic module encased in a commercial grade metal case made of cold rolled steel. The module cryptographic boundary is the router's enclosure which includes all components, including the encryption module which is a separate part. Figure 1 illustrates the cryptographic boundary of the MNR S6000 router. In the photo, blank plates cover slots that can hold optional network interface cards that are external to the boundary of the module. The FIPS validated firmware versions are PS-16.6.0.69 and GS-16.6.0.69. (The firmware versions have identical FIPS 140-2 security relevant functionality. They differ only in non-security relevant features.)

Configurations	**S6000 Base Unit**		**S6000 Encryption Module**		**FW Version**
	HW P/N	**Revision**	**HW P/N**	**Revision**	
	CLN1780L	Rev E	CLN 8261D	Rev N	GS-16.6.0.69 or PS-16.6.0.69

Table 1 - MNR S6000 Router Version Numbers

Previous Validation Versions – FIPS 140-2 Cert. #1547

Configurations	**S6000 Base Unit**		**S6000 Encryption Module**		**FW Version**
	HW P/N	**Revision**	**HW P/N**	**Revision**	
	CLN1780H	Rev A	CLN 8261D	Rev L	GS-16.0.1.44 or PS-16.0.1.44

Table 2 - MNR S6000 Router Versions from FIPS 140-2 Cert. #1547

Previous Validation Versions – FIPS 140-2 Cert. #1013

S6000 Base Unit			**S6000 Encryption Module**			**FW Versions**
HW P/N	**Tanapa Number**	**Revision**	**HW P/N**	**Tanapa Number**	**Revision**	
ST6000C	CLN1780D	Rev B	ST6016A	CLN8261D	Rev H	PS-15.1.0.75, GS-15.1.0.75, PS-15.1.0.76, GS-15.1.0.76, PS-15.2.0.20, GS-15.2.0.20, PS-15.4.0.60, GS-15.4.0.60, PS-15.6.0.27, GS-15.6.0.27, PS-15.7.0.60 or GS-15.7.0.60
ST6000C	CLN1780C	Rev A	ST6016A	CLN8261D	Rev H	

Table 3 - MNR S6000 Versions from FIPS 140-2 Cert. #1013

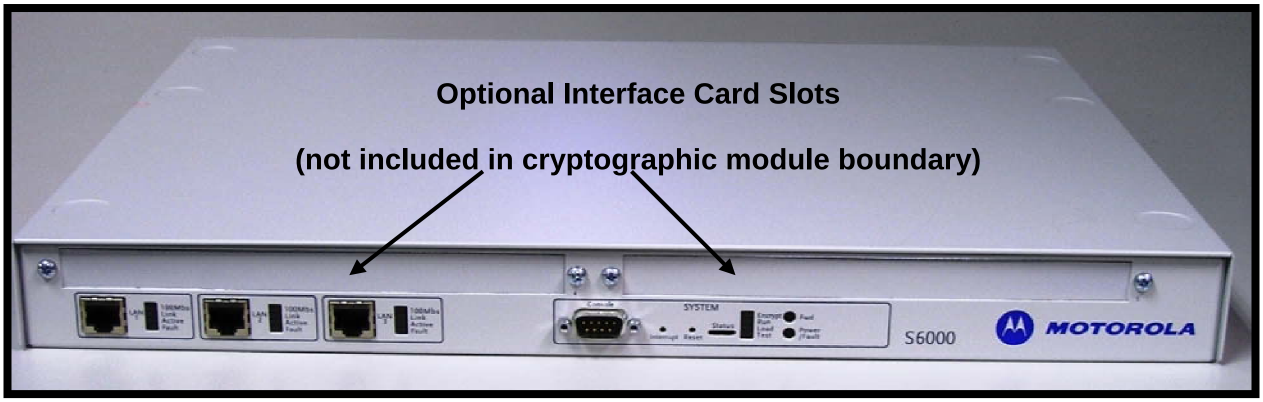
Optional Interface Card Slots
(not included in cryptographic module boundary)
S6000
MOTOROLA

Figure 1– MNR S6000 Router Cryptographic Module Boundary

2. Security Level

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

Security Requirements Section	Level
Cryptographic Module Specification	3
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

Table 4 – Module Security Level Specification

3. Modes of Operation

Approved mode of operation

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

Hardware Implementations

a. Triple-DES – CBC mode (168 bit) for IPsec and FRF.17 encryption (Cert. #275)

b. AES - CBC mode (128, 192, 256 bit) for IPsec and FRF.17 encryption (Cert. #173)

c. HMAC-SHA-1 for IPsec and FRF.17 authentication (Cert. #39)

d. SHA-1 for message hash (Cert. #258)

Firmware Implementations

a. Triple-DES – CBC mode (168 bit) for IKE and SSHv2 encryption (Cert. #1493)

b. AES – CBC (128, 192, 256-bit), ECB (128-bit), and CFB128 (128-bit) modes for IKE, SSHv2 and SNMPv3 encryption (Cert. #2395)

c. HMAC-SHA-1 for IKE, SSHv2 and SNMPv3 authentication (Cert # 1486)

d. SHA-1 and SHA-256 for message hash (Cert # 2057)

e. RSA PKCS#1 v1.5 – for digital signature verification (1024- and 2048-bit). (Cert. #1239)

f. SP800-90A Hash_Based Deterministic Random Bit Generator (DRBG) (Cert. #399)

g. KDF for SSH (CVL Cert. #99)

h. KDF for SNMPv3 (CVL Cert. #122)

i. KDF for IKEv1/IKEv2 (CVL Cert. #315)

The MNR S6000 router 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 methodology provides 112 bits of encryption strength)
- Hardware non-deterministic RNG (NDRNG): Provides seed for approved deterministic RBG

Non-FIPS approved algorithms

In a Non FIPS mode of operation, the cryptographic module provides non-FIPS Approved algorithms as follows:

- DES for encryption/decryption
- DSA 1024-bit – for public/private key pair generation and digital signatures (non-compliant)
- Non approved SW RNG (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) (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 5 below. For details on individual router 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 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>** The PSK must be at least 80 bits in length with at least 80 bits of entropy.
3.	Configure IPsec and FRF.17 selector lists using the command **ADD –CRYPTO SelectorLIst**
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-3DES, 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-3DES, 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.	For each port for which encryption is required, enable encryption on that port using **SETDefault [!<portlist>] –CRYPTO CONTrol = Enabled**
8.	DSA keys must not be used in FIPS mode.
9.	FIPS-140-2 mode achieved

Table 5 – FIPS Approved mode configuration

To review the cryptographic configuration of the router, use the following command:

SHOW –CRYPTO CONFiguration

This command shows a detailed summary of the cryptographic configuration and allows a user to verify that encryption is enabled on user-determined ports and that only FIPS-Approved algorithms are used for encryption and authentication.

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 have 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 6 below provides a listing of the physical ports and logical interfaces for the MNR S6000 router.

The S6000 base system consists of a motherboard, supporting three Ethernet interfaces, mounted in an enclosure with a power supply. The base system also includes a console port and may be configured with any combination of one or two optional LAN or WAN I/O interface cards. The optional LAN/WAN interface cards are not part of the validated module boundary.

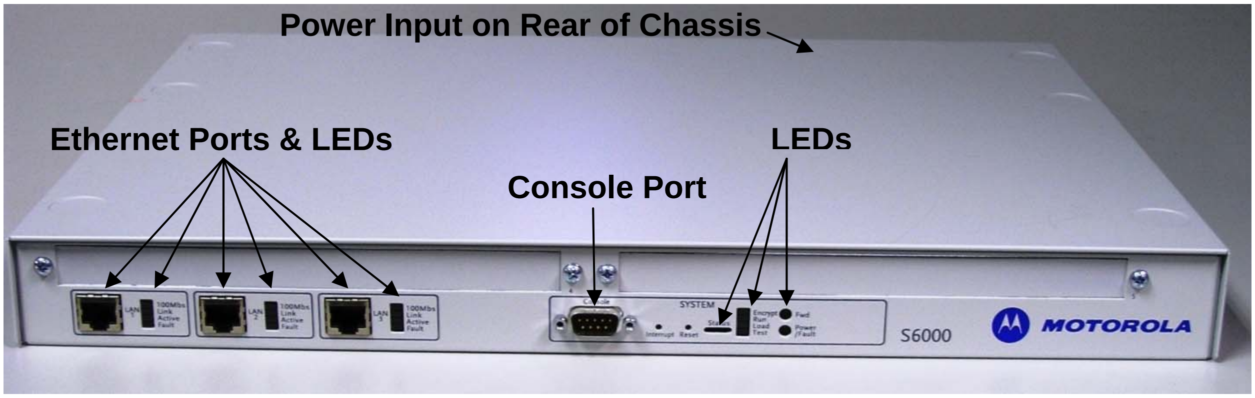

Figure 2 – MNR S6000 Ports

Physical Port	**Qty**	**Logical interface definition**	**Interface Card**	**Comments**
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	
LEDs	7	Status output	N/A	Provides LED status output on network traffic, power, and errors

Table 6 – S6000 physical ports and logical interfaces

5. Identification and Authentication Policy

Assumption of roles

The MNR S6000 router supports the following distinct operator roles:

1. Crypto Officer (SuperUser)
2. Admin
3. Network Manager
4. User
5. Maintenance

Roles #1-4 require authentication via username and password when accessing the router via any interface. (See Table 8.) 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. The unauthenticated maintenance role (#5) is entered only via the router console port.

6. MotoAdmin
7. MotoMaster
8. MotoInformA/B

Roles #6-8 are specific to SNMPv3 operations. Each SNMPv3 user has its own pair of encryption and authentication passphrases. (See Table 8.)

The role-based authentication capabilities will be described here, although the role based-authentication is not required to comply with Level 1 requirements.

The module stores operator identity information internally for all roles.

When a router power cycles, sessions are terminated. A user must reauthenticate to access the router.

Multiple concurrent operators. Each operator has an independent session with the router, either though Telnet, 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 7 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.	A user 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.
Maintenance	None (see comment)	N/A	Maintenance role can be entered via the external console port (unauthenticated) or via EOS software command (requires Network Manager authentication)
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 7 – Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
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 unsuccessful login attempts, a user is locked out for two minutes, ensuring that that the probability is less than one in 100,000 that random multiple attempts will succeed or a false acceptance will occur within a one minute time period.
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 1/80^8 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.

Table 8 – 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 router
- 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 all operators

* 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 not requiring operator intervention.
- Monitor: Perform various hardware 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.

Roles and Services

Service	**Crypto Officer (Super User)**	**Network Manager**	**User**	**Admin**	**Maintenance**	**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				
Unauthenticated Show Status	X	X	X	X	X			
Power-up Self-Tests	X	X	X	X	X			
Monitor	X				X			
Access Control	X	X	X	X				

Table 9 – 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	Used for authentication of packets sent/received to RADIUS Server, up to 32 characters.
Hash-DRBG Seed	Initial seed for FIPS-approved deterministic DRBG
Hash-DRBG Internal State	Internal state/context for FIPS-approved deterministic DRBG. The critical security parameters are the values V and C.
Passwords • Network Manager Password (Root) • Admin • User Accounts	7 (to 15) character password used to authenticate to module

Table 10 – 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 11 – Public Keys

Definition of CSPs Modes of Access

Table 12 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	-	-	-	*EG*	-	-	-	-	*Z*	-	-	-	-	-	-	-	-
Ephemeral Phase-2 DH private key	-	-	-	*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
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	-	-	-	-	-	-	-	-
SNMPv3 Passphrase	-	-	*EW*	-	-	-	-	-	*Z*	-	-	*E*	-	-	-	-	-
SNMPv3 Session Keys	-	-	-	-	-	-	-	-	-	-	-	*EGZ*	-	-	-	-	-
RADIUS Secret	-	-	-	-	-	-	-	-	Z	-	-	-	-	-	-	-	EW
Passwords	-	-	EG	-	-	-	-	-	Z	-	-	-	-	-	-	-	E
Hash-DRBG Seed	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-
Hash-DRBG Internal State	-	-	-	EG	-	-	-	-	Z	-	-	-	-	-	-	-	-

Table 12 – Services to CSP Access mapping

7. Operational Environment

The MNR S6000 router does not contain a modifiable operational environment.

8. Security Rules

The cryptographic module's design corresponds to the example cryptographic module's 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 MNR S6000 router provides eight distinct operator roles: Crypto Officer (SuperUser), Admin, Network Manager, User, MotoAdmin, MotoMaster, MotoInformA/B, and Maintenance. The Crypto Officer role uses the root account.
2. The MNR S6000 router encrypts message traffic using the AES or Triple-DES algorithm.
3. The MNR S6000 router performs the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:

      Hardware Implementation:

      a. AES-CBC Encrypt and Decrypt Known Answer Tests
      b. Triple-DES-CBC Encrypt and Decrypt Known Answer Tests
      c. HMAC-SHA-1 Known Answer Test (Includes SHA-1 KAT)

      Firmware Implementation

      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 deterministic DRBG and Hardware NDRNG.
      b. Firmware load test – RSA signature verification of externally loaded code.
      c. Alternating bypass tests – when enabling FRF.17 and IPsec encryption or 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 MNR S6000 router is in an idle state, the operator can command the router to perform the power-up self-test by power-cycling or rebooting the router.
6. Data output is inhibited during key generation, self-tests, zeroization, and error states.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. 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.

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 Network Manager (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 5.

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.

Before entering or exiting the Maintenance Role or non-FIPS mode, the operator shall use the Zeroization Service to zeroize all CSPs. The Zeroization Service should also be invoked prior to removing a router from service for repair.

10. Physical Security Policy

Physical Security Mechanisms

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

11. Mitigation of Other Attacks Policy

The module 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.