GENERAL DYNAMICS
Mission Systems

Non-Proprietary Security Policy
for the FIPS 140-2 Level 2 Validated

Fortress Mesh Points

April 4, 2017 Version 1.7

This security policy of General Dynamics Mission Systems, for the FIPS 140-2 validated Fortress Mesh Points (FMP), defines general rules, regulations, and practices under which the FMP was designed and developed and for its correct operation. These rules and regulations have been and must be followed in all phases of security projects, including the design, development, manufacture service, delivery and distribution, and operation of products.

Hardware:

ES210: Tactical Mesh Point

ES2440: High Capacity Mesh Point

ES520 (V1 & V2): Deployable Mesh Point

ES820: Vehicle Mesh Point

Firmware: 5.4.5

REVISION HISTORY

Rev	Date	Description
1.0	May, 2016	Initial Draft
1.1	May, 2016	Various updates and edits
1.2	May, 2016	Various updates and edits
1.3	May, 2016	Formatting changes
1.4	May, 2016	Minor updates and edits
1.5	Sept, 2016	Several updates in response to lab review.
1.6	Feb, 2017	Updates to: Section 3.0 Identification and Authentication Policy Section 4.0 Cryptographic Keys and CSP. Section 6.0 Physical Security Policy Section 7.0 FIPS Mode. Various TLS and RSA updates.
1.7	April, 2017	Minor updates

Contents

LIST OF FIGURES AND TABLES

1.0 Introduction

Security policy for General Dynamics Mission Systems' Fortress Mesh Point product line.

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

Table 1: Security Level of Security Requirements

Security Requirement Security	Level
Cryptographic Module Specification	2
Cryptographic 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	2

2.0 Identification and Authentication Policy

The TOE supports up to 10 total users that can be defined. Each user is assigned a role as defined below.

2.1 Role-based Authentication

There are three Crypto Officer Roles. Please note that the configuration model supports assigning the roles below to users defined below. In this case, the role is a property of a defined user.

When creating a Crypto Officer, one of the roles described below must be selected along with a unique username and password. Although each operator has a unique username and password, since selecting a role is also required, therefore this system should be considered as having role-based authentication.

- Crypto Officer Roles
  - Log Viewer: account users can view only high-level system health indicators and only those log messages unrelated to configuration changes.
  - Maintenance[1]: account users can view complete system and configuration information and perform a few administrative functions but cannot make configuration changes.
  - Administrator: the main manager/administrator of the FMP.

- User Roles
  There are three User Roles.
  - MSP End User: This role will utilize another MSP secure controller to establish a secure connection over an untrusted network.
  - RSN End User: This role will utilize either a RSN (802.11i) secure client loaded on a workstation or a RSN (802.11i) secure controller like a VPN to establish a secure connection over an untrusted network.
  - IPsec End User: This role will utilize either an IPsec/L2TP client loaded on a workstation or an IPsec/L2TP controller like a VPN to establish a secure connection.

2.2 Services

The following list summarizes the services that are provided by the FMP:

- Encrypt/Decrypt (MSP | RSN | IPsec) PDU Services: use the encryption services of the FMP for passing of data.
- Show Status: observe status parameters of the FMP.
- View Log: view log messages.
- Write Configuration: change parameters in the FMP including changing the FIPS Mode, Bypass Setting, Zeroization and setting passwords;
- Read Configuration: read parameters in the FMP
- Diagnostic: execute some network diagnostic and self-tests services of the FMP;
- Upgrade: Upgrade the unit with a new release of firmware.

2.3 Authentication and Authentication Data

All roles must be authenticated before they can use module services. This can be processed either internally by the module or externally using an EAP authentication server.

[1] The Maintenance User is a CO and is not the same as a maintenance user as defined in FIPS 140-2.

2.3.1 Authentication Methods

All roles must be authenticated if they use FMP services.

For Crypto-Officer authentication, a User Name and Password must be presented. The module forces the Crypto-Officer to change the default password at first login. The FMP will not accept new passwords that do not meet specified requirements.

A Crypto Officer can utilize two secure communication methods to access the FMP:

- Directly connected terminal
- Secure SSH (SSH-2.0-OpenSSH_5.8) connection

A Crypto Officer can apply up to nine rules for administrative passwords that allow stronger passwords. These can be reviewed in the User Guide. Both modules having the same Access ID authenticate the MSP user. The RSN End User will use either a Shared Secret or will be authenticated by the use of an external EAP Server (i.e. RADIUS). The Authentication Data for each of these roles are shown in following table.

Table 2: Authentication Data

Operator	*Type of Authentication*	*Connect Using*	*Authentication Data*
Log Viewer	Password	Direct Connect Secure SSH	The possible character space is 91 characters and the password length is between 8 and 32 characters. (The default Log Viewer settings require a minimum of 15 characters).
Maintenance	Password	Direct Connect Secure SSH	The possible character space is 91 characters and the password length is between 8 and 32 characters. (The default Maintenance settings require a minimum of 15 characters).
Administrator	Password	Direct Connect Secure SSH	The possible character space is 91 characters and the password length is between 8 and 32 characters. (The default Administrator settings require a minimum of 15 characters).
MSP End User	Access ID	MSP	16-byte Access ID when in FIPS Mode. (In non-FIPS mode, users may select 8-bytes.
RSN End User	Secret ECDSA	RSN RSN	FIPS mode requires a 64 byte hexadecimal string (256 bits). Certificate base authentication supports ECDSA P-256 and ECDSA P-384.
IPsec/L2TP End User	Secret ECDSA	IPsec/L2TP IPsec/L2TP	FIPS mode requires a 32-256 byte hexadecimal string (128-1024 bits). Certificate base authentication supports ECDSA P-256 and ECDSA P-384.

2.3.2 Authentication Server Methods

The Crypto Officer can also be authenticated by using an Authentication Server. The Authentication Server can be the one built into the FMP, one on another FMP or it can be an external Authentication Server.

The service(s) available are determined by the FMP's configuration for authentication services as determined by the settings in Authentication Servers and/or Local Authentication.

To use an external server (RADIUS) for administrator authentication, it must be configured to use General Dynamic's Fortress Vendor-Specific Attributes (see User Guide for more information).

2.3.3 Authentication Strength

The probability of guessing the authentication data is shown in following table.

Mechanism	Role	Strength of Mechanism
Username & Password	Administrator Maintenance Log Viewer	The FMP requires that all variants of the Crypto Officer manually enter the username and password. There are 91 distinct characters allowed in the password, and the password may be between 8 and 32 characters. Assuming the low end of that range (8 chars), the probability of a successful random guess is 1 in 91^8 attempts. (or 1 in 4.70E+15) The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (4.70E+15/ (400*60)) or 1 in 1.96E+11. Note: The maximum number of login attempts can be set between 1 and 9 and lockout duration between 0 and 60 minutes.
MSP Shared Secret	MSP End User	The MSP shared secret is a 16 byte (128 bit) value. The probability of a random match is 1 in 2^128, or 3.40E+38. The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (3.40E+38/ (400*60)) or 1 in 1.42E+34.
RSN Shared Secret	RSN End User	FIPS mode requires the RSN shared secret be entered as a 64 byte hexadecimal string (256 bits). The probability of a random match is 1 in 2^256, or 1.16E+77. The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (1.16E+77/(400*60)) or 1 in 4.82E+72.
IPsec Shared Secret	IPsec End User	FIPS mode requires the IPsec shared secret be entered as (32-256) byte hexadecimal string. Assuming the shortest length (32 hexadecimal string) that converts to 128-bits. The probability of a successful random guess is 1 in 2^128, or 3.40E+38. The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (3.40E+38/ (400*60)) or 1 in 1.42E+34.
Certificate Based	RSN End User IPsec End User	Certificate base authentication supports ECDSA P-256 and ECDSA P-384. For ECDSA P-256 the security bit strength is 128 bits, which means the probability of a random attempt succeeding is 1 in 2^128, or 3.40E+38. The FMP authentication channels support at most 400 authentications attempt per sec. The probability of a successful random guess within one minute is: (3.40E+38/ (400*60)) or 1 in 1.42E+34.

Table 3: Probability of guessing the authentication data

2.3.4 Administrative Accounts

The users are configured by adding administrative accounts to a Role. These are configured through the CLI. For instance the product can have multiple administrative accounts each having a unique Username and Password and each being assigned to a particular role (i.e., Log Viewer, Maintenance or Administrator). When a user is logged into the FMP he will have all the rights of the Role he has been assigned.

3.0 Cryptographic Keys and CSP

Keys and CSPs generated in non-FIPS mode cannot be used in FIPS mode, or vice versa. The FMP will require the admin to reboot the box after FIPS mode is enabled or disabled.

3.1 For MSP

The FMP contains a number of cryptographic keys and Critical Security Parameters (CSP) for MSP as shown in the following table. All keys are generated using FIPS approved algorithms and methods as defined in SP800-56A. All keys are kept in RAM in plaintext, zeroized when unit reboots, and are never stored to disk.

Table 4: MSP Keys

Key	Key Type	Generation	Use	Implementation(s)
Module Secret Key (Hardkey)	AES-CBC: 128, 192, or 256 bit.	Uses manually entered or generated Access ID (128 bits) as input for the SP 800-90A HMAC DRBG.	Used to encrypt static Diffie-Hellman public key requests and responses over the wire.	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)
Static Private Key	Diffie-Hellman: 256 bits ECDH: 384 bits	Automatically generated using the SP 800-90A HMAC DRBG.	Along with received Diffie-Hellman Static Public Key from partner is used to generate the Static Secret Encryption Key	Fortress Cryptographic Implementation (Cryptlib)
Static Public Key	Diffie-Hellman: 2048 bits ECDH: 384 bits	Automatically generated using Diffie-Hellman or ECDH.	Sent to communicating Module in a packet is encrypted with HardKey.	Fortress Cryptographic Implementation (Cryptlib)
Static Secret Encryption Key	AES-CBC: 128, 192, or 256 bit.	Automatically generated using Diffie Hellman or ECDH.	Used to encrypt dynamic public key requests and responses over the wire.	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)
Dynamic Private Key	Diffie-Hellman: 256 bits ECDH: 384 bits	Automatically generated using the SP 800-90A HMAC DRBG.	Along with received Dynamic Public Key from partner is used to generate the Dynamic Secret Encryption Key	Fortress Cryptographic Implementation (Cryptlib)
Dynamic Public Key	Diffie-Hellman: 2048 bits ECDH: 384 bits	Automatically generated using Diffie-Hellman or ECDH.	Sent to communicating module in a packet encrypted with the Static Secret Encryption Key	Fortress Cryptographic Implementation (Cryptlib)
Dynamic Secret Encryption Key (DKey)	AES-CBC: 128, 192, or 256 bit.	Automatically generated using Diffie Hellman or ECDH.	Used to encrypt all packets between two communicating Modules over the wire	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)
Static Group Key (SGK)	AES-CBC: 128, 192, or 256 bit.	See Below for Full Text. Generated using the SP 800-90A HMAC DRBG.	Used to encrypt user-data frames until the unicast Dynamic Secret Encryption Key is computed.	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)

The static group key (SGK) computation must be deterministic. That is, each node joining the network specified by the Access ID must be able to compute the same static group key without communicating with other nodes on the network. This means that the SGK must be determined solely based on the Access ID for the network.

Note that the static group key (SGK) is generated by using the Access ID (128 bits) merged with a MSP constant to seed an instance of an SP800-90A DRBG. .

Since the Access ID is 128 bits, this means that there is at most 128 bits of entropy in the static group key.

3.2 For RSN

An RSN or 802.11i wireless secure LAN can use either a PSK or an EAP generated master key. If a PSK is used, each peer must configure the correct hex value. This PSK becomes the Master Key. If the EAP method is used, the Master Key is generated through the EAP process and it's correctly given to both the Client and FMP.

RSN are FIPS capable portions of the IEEE 802.11 specification for wireless LAN networks. The keys for RSN are shown in the following table.

AES-CCMP uses AES-CCM (allowed) in the 802.11i protocols (allowed). IEEE802.11i protocols are allowed in FIPS mode. Please see IG 7.2

All keys are kept in RAM in plaintext, zeroized when unit reboots, and are never stored to disk

Table 5: RSN Keys

Key	Key Type	Generation	Use	Implementation(s
Pairwise Master Key (PMK)	HMAC-SHA256	Using the key generation procedure as defined in the IEEE 802.11 specification. PSK(manual entered password). OR EAP Method: PMK is created using key material generated during EAP authentication.,	Authentication and to derive (PTK)	Fortress Cryptographic Implementation (Cryptlib)
Pairwise Transient Key (PTK)	For AES-CCM, 384 bit key comprised of three 128 bit keys: Data Encryption/Integrity key, EAPOL-Key Encryption key, and EAPOL-Key Integrity key.	PRF(PMK | AP nonce |STA nonce| AP MAC|STA MAC) PRF = RSN KDF CAVP #112	Provides a set of keys used to protect link between end user station and FMP.	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)
Group Master Key (GMK)	SP 800-90A DRBG Generated 256 bit key.	Using the key generation procedure as defined in the IEEE 802.11 specification. Random number generated on the AP via SP 800-90A DRBG.	Used to derive (GTK).	Fortress Cryptographic Implementation (Cryptlib)
Group Transient Key (GTK)	For RSN/TKIP and WPA, AES 256 bit key comprised of two 128 bit keys: Group Encryption key and Group Integrity key. For AES-CCM, 128 bit key comprised of Group Encryption/Integrity key.	PRF(GMK | APMac | GNonce) PRF = RSN KDF CAVP #112	Used to protect multicast and broadcast (group) messages sent from FMP to associated end user station. . The AP sends the new GTK to each STA in the network using the PTK.	Fortress Cryptographic Implementation (Cryptlib) Fortress Cryptographic Implementation (FPGA)

3.3 For IPsec

An IPsec tunnel is created over an established AES encrypted RSN/802.11i wireless secure link. If the connection is over the external Ethernet port then the IPsec tunnel is established over the current networking environment. Please note, no parts of the IPsec protocol, other than the KDF, have been tested by the CAVP.

The AES-GCM IV is implemented as a 64-bit deterministic value which does not repeat per encryption key, this method is compliant with IG A.5 & Section 8.2.1 of SP800-38D.
Only IPsec ECC keys are FIPS compliant, RSA keys are not permitted in FIPS mode.
Refer to section '7.0 FIPS Mode' regarding FIPS required IPsec settings.

All keys are kept in RAM in plaintext, zeroized when unit reboots, and are never stored to disk

Table 6: IPsec Keys

Key	Key Type	Generation	Use	Implementation(s
DH Private Key	ECDH: 256/384 bits	Seed is automatically pulled from SP 800-90A DRBG	Used to calculate the DH Key	Fortress Cryptographic SSL
DH Public Key	ECDH: 256/384 bits	The DH Private Key is fed to the Diffie-Hellman function to automatically generate this key	Used for digital signature to authenticate the peer	Fortress Cryptographic SSL
ECDSA Private Key	ECDSA: 256/384 bits	Seed is automatically pulled from SP 800-90A DRBG	Used to calculate the ECDSA certificate Key	Fortress Cryptographic SSL
ECDSA Public Key	ECDSA: 256/384 bits	The ECDSA Private Key is fed to the ECDSA function to automatically generate this key	Used for digital signature to authenticate the peer	Fortress Cryptographic SSL
IKE-SKEYSEED	HMAC-SHA256 or HMAC-SHA384 Sz=(7*hash)	IKE-KDF (CAVP #937) As defined in SP800-135r1 Section 4.1 Internet Key Exchange	Generate IPsec SAs for ESP traffic	Fortress Cryptographic Implementation (Cryptlib) for hmac Fortress KAS Implementation for KDF Fortress Cryptographic Implementation (FPGA)
PSK	Manual by admin per peer. (128bit – 1024bit)	Admin may manually configure a pass-phrase.	Used for peer authentication, alternative to certificate authentication.	Fortress Cryptographic Implementation (Cryptlib)
Session Key	AES-GCM: 256 bits	Diffie-Hellman generated shared secret.	Used to encrypt/decrypt packets.	Fortress Cryptographic SSL

3.4 For SSH

The SSH (SSH-2.0-OpenSSH_5.8) protocol uses the cryptographic algorithms of the OpenSSH protocol. The cryptographic keys for SSH are shown in the following table. Please note, no parts of the SSH protocol, other than the KDF, have been tested by the CAVP.

All keys are kept in RAM in plaintext, zeroized when unit reboots, and are never stored to disk

Table 7: SSH Crypto Keys

Key	Key Type	Generation	Use	Implementation(s
ECDSA Private Key	ECDSA KEY 256 & 384 bits	Generated via openssl upon the 1st boot after a factory reset.	The private key is used to generate signatures.	Fortress Cryptographic -SSL
ECDSA Public Key	ECDSA KEY 256 & 384 bits	Generated via openssl upon the 1st boot after a factory reset.	The public key is used to verify signatures.	Fortress Cryptographic -SSL
SSH Key Block	SSH KDF key block (SHA1, SHA256)	SSH-KDF (CAVP #938) as defined in SP800-135r1 Section 5.2 (SSH Key Derivation Function)	The Key Block is the keying material that is generated for the AES encryption key. Encrypt Data Packets	Fortress Cryptographic- SSL (for hash) Fortress KAS Implementation for KDF.

3.5 Critical Security Parameters

There are other critical security parameters present in the FMP as shown in the following table.

The non-volatile CSPs are stored encrypted and are zeroized when the FMP is restored to factory default; the volatile CSPs are stored in plaintext and are zeroized when the unit is rebooted.

Table 8: Other Keys and Critical Security Parameters

CSP	Non-Volatile Storage	Type	Generation	Use	Implementation(s)
Access ID 32 Hex Digits	Y	Seed	This key can be generated or entered by the CO. The administrator should use an approved DRBG when in FIPS Mode. Auto generation uses an instance of SP800-90A DRBG.	MSK, SGK & privD-H Group key component and used for authentication	Admin provided or Fortress Cryptographic Implementation (Cryptlib)
Log Viewer Password	Y	Password SHA256	8 to 32 Characters, entered by the Crypto Officer	To authenticate the Log View	Fortress Cryptographic Implementation (Cryptlib)
Maintenance Password	Y	Password SHA256	8 to 32 Characters, entered by the Crypto Officer	To authenticate the maintenance user	Fortress Cryptographic Implementation (Cryptlib)
Administrator Password	Y	Password SHA256	8 to 32 Characters, entered by the Crypto Officer	To authenticate the Administrator	Fortress Cryptographic Implementation (Cryptlib)
Firmware Upgrade Key	Y	RSA Public Key SHA256	Public RSA key (2048-bit) used to validate the signature of the firmware upgrade image that has been loaded from an external workstation.	Verify the signature that is attached to the upgrade package	Fortress Cryptographic SSL
Firmware Load Key	Y	RSA Public Key SHA256	Public RSA key (2048-bit) used to validate the signature of the firmware image that has been loaded from the internal flash drive at boot time.	Verify the signature that is attached to the firmware load package	Fortress Cryptographic SSL
HMAC DRBG entropy	N	Seed	Automatically Generated by NDRNG. Size=2*Configured Security Strength	Entropy used as input to SP 800-90A HMAC DRBG	Fortress Cryptographic Implementation (Cryptlib)
HMAC DRBG V Value	N	Counter	Automatically generated by DRBG	Internal V value used as part of SP 800-90A HMAC DRBG	Fortress Cryptographic Implementation (Cryptlib)
HMAC DRBG Key	N	Seed	Automatically generated by DRBG Size=2*Configured Security Strength	Key value used for the HMAC of the SP 800-90A HMAC DRBG	Fortress Cryptographic Implementation (Cryptlib)
HMAC DRBG init_seed	N	Seed	Automatically generated by NDRNG Size=2*Configured Security Strength	Initial seed value used in SP 800-90A HMAC DRBG	Fortress Cryptographic Implementation (Cryptlib)

HMAC DRBG entropy	N	Seed	Automatically Generated by NDRNG Size=2*Configured Security Strength	Entropy used as input to SP 800-90A HMAC DRBG	Fortress Cryptographic	SSL
HMAC DRBG V Value	N	Counter	Automatically generated by DRBG	Internal V value used as part of SP 800-90A HMAC DRBG	Fortress Cryptographic	SSL
HMAC DRBG Key	N	Seed	Automatically generated by DRBG Size=2*Configured Security Strength	Key value used for the HMAC of the SP 800-90A HMAC DRBG	Fortress Cryptographic	SSL
HMAC DRBG init_seed	N	Seed	Automatically generated by NDRNG Size=2*Configured Security Strength	Initial seed value used in SP 800-90A HMAC DRBG	Fortress Cryptographic	SSL

3.6 Known Answer and Conditional Tests

3.6.1 Known Answer Tests

This section describes the known answer tests run on the system. The tests are organized by module against which they are run.

Table 9: Known Answer Tests

Known Answer Tests for CRYPTLIB	
Algorithm	**Modes/States/Key sizes/**
AES	**ECB(e/d; 128,192,256);** **CBC(e/d; 128,192,256)**
SHS	**SHA-1 (BYTE-only)** **SHA-256 (BYTE-only)** **SHA-384 (BYTE-only)** **SHA-512 (BYTE-only)**
HMAC	**HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS) SHS** **HMAC-SHA256 (Key Size Ranges Tested: KS=BS) SHS** **HMAC-SHA384 (Key Size Ranges Tested: KS=BS) SHS** **HMAC-SHA512 (Key Size Ranges Tested: KS=BS) SHS**
DRBG 800-90A	**Hash Based DRBG** **[HMAC_DRBG: SHA256, SHA512]**

Known Answer Tests for KAS	
DH	**DH (Key sizes tested: 2048)**

ECDH	**ECDH-secp (Key Size Range: 384 bits)**

Known Answer Tests for FPGA

The FPGA algorithms are tested indirectly with packet KAT tests.

(Encrypt;Decrypt) for each (MSP-Legacy, MSP-Suite B, ESP-Suite B, CCMP)

Algorithm	Modes/States/Key sizes/
AES	**CBC (e/d: 256)** **GCM (e/d: 256)** **CCM (e/d: 128)**
HMAC	**HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) SHS** **HMAC-SHA384 (Key Size Ranges Tested: KS<BS) SHS**

Known Answer Tests for OPENSSL

Algorithm	Modes/States/Key sizes/
AES	**ECB(e/d: 128)**
SHS	**SHA-1 (BYTE-only)** **SHA-256 (BYTE-only)** **SHA-384 (BYTE-only)** **SHA-512 (BYTE-only)**
HMAC	**HMAC-SHA1 (Key Sizes : 160) SHS** **HMAC-SHA256 (Key Sizes : 160) SHS** **HMAC-SHA384 (Key Sizes : 160) SHS** **HMAC-SHA512 (Key Sizes : 160) SHS**
RSA	**ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-256**
ECDSA	**Sig(gen);Sig(ver);secp256r1 (P-284)** **Sig(gen);Sig(ver);secp384r1(P-384)**
DSA	**Sig(gen);Sig(ver)** **(SHA384 Key:2048)**

DRBG 800-90A	**Hash Based DRBG:** **[SHA-1 , SHA-256 , SHA-384, SHA-512]**

3.6.2 Conditional Tests

This section describes the conditional tests run on the system.

Table 10 Conditional Tests

Tests	Condition
'Known Answer Tests' (Table 8)	**Power on self-test;** **FIPS mode change;** **Any security policy change**
Firmware Integrity Upgrade Test **RSA SIG(ver); 2048 , SHS: SHA-256**	**Firmware upgrade.**
Firmware Integrity Load Test **RSA SIG(ver); 2048 , SHS: SHA-256**	**Firmware image loaded at boot time.**
Pairwise Consistency Tests: **RSA(ALG[RSASSA-PKCS1_V1_5]** **SIG(gen); SIG(ver); 2048 , SHS: SHA-1** **DH(2048)** **ECDH(secp384)** **ECDSA([gen,ver], [secp256,secp384], [sha1])**	**Power on self-test;** **FIPS mode change;** **Any security policy change**
MSP Bypass Test	**Power on self-test;** **FIPS mode change;** **Change to the bypass mode** **Initialization of MSP peer**
CCMP Bypass Test	**Power on self-test;** **FIPS mode change;** **Change to the bypass mode** **Wireless interface initialization**
ESP Bypass Test	**Power on self-test;** **FIPS mode change;** **Change to the bypass mode**
Random Number Generation: **NDRNG** **DRBG (Performs the HMAC_DRBG Health tests (Instantiate, Generate, and Reseed) as described in SP800-90A Section 11.3 Health Testing).**	**Power on self-test;** **Every generation of a random number**

3.7 Algorithm Certifications

This section describes the current list of certified algorithms and their certification numbers.

Table 11 Certifications

ALGO	Cert #	Crypto Implementation	Standard	Use	Operational Environment	Modes
AES	1519	Fortress Cryptographic Implementation V2.0	FIPS 197 SP 800-38A	Encrypt/Decrypt IPsec, WPA2,MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	ECB (e/d; 128 , 192 , 256) CBC (e/d; 128 , 192 , 256);
	1520	Fortress Cryptographic Implementation FPGA V2.0	FIPS 197 SP 800-38A SP 800-38D	Encrypt/Decrypt IPsec, WPA2,MSP	Xilinx Spartan FPGA	CBC (e/d; 128, 192, 256) GCM (e/d;KS: 128 ,256) CCM (KS: 128)
	3506	Fortress Cryptographic Implementation SSL V2.1	FIPS 197 SP 800-38A	Encrypt/Decrypt IPsec (IKE) WPA2 (establishment) SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	ECB (e/d; 128, 192 , 256) CBC (e/d; 128, 192, 256) CFB8 (e/d; 128, 192, 256) CFB128 (e/d; 128, 192, 256) OFB (e/d; 128, 192, 256)
SHS	1357	Fortress Cryptographic Implementation V2.0	FIPS 180-4	Message Digest IPsec, WPA2,MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)
	1358	Fortress Cryptographic Implementation FPGA V2.0	FIPS 180-4	Message Digest IPsec, WPA2,MSP	Xilinx Spartan FPGA	SHA-1 (BYTE-only) SHA-384 (BYTE-only)

	2891	Fortress Cryptographic Implementation SSL V2.1	FIPS 180-4	Message Digest IPsec, WPA2,MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)
HMAC	889	Fortress Cryptographic Implementation V2.0	FIPS198-1	Msg Authentication IPsec, WPA2,MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512
	890	Fortress Cryptographic Implementation FPGA V2.0	FIPS198-1	Msg Authentication IPsec, WPA2,MSP	Xilinx Spartan FPGA	HMAC-SHA1 HMAC-SHA384
	2238	Fortress Cryptographic Implementation SSL V2.1	FIPS198-1	Msg Authentication SSH WPA2 (establishment) IPsec (IKE)	RMI Alchemy MIPS Processor Broadcom XLS Processor	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512
ECDSA	716	Fortress Cryptographic Implementation SSL V2.1	FIPS186-4	Signature Verify IPsec WPA2 (establishment) SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	SigVer: P-256: (SHA-1, 256) P-384: (SHA-1, 384)
ECDSA	833	Fortress Cryptographic Implementation SSL V2.1	FIPS186-4	Key Agreement IPsec WPA2 (establishment) SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	FIPS186-4: PKG: CURVES(P-256 P-384 ExtraRandomBits) PKV: CURVES(P-256 P-384)
ECDSA	CVL 573	Fortress Cryptographic Implementation SSL V2.1	FIPS186-4	Signature Generation IPsec (IKE) WPA2 (establishment)	RMI Alchemy MIPS Processor Broadcom XLS Processor	ECDSA SigGen Component: P-256, P-384
RSA	1800	Fortress Cryptographic Implementation SSL V2.1	FIPS186-2	Signature Verify SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	ALG[RSASSA-PKCS1_V1_5] SIG(ver): 2048, SHS: SHA-1

	1967	Fortress Cryptographic Implementation SSL V2.1	FIPS186-4	Signature Generation SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	ALG[ANSIX9.31] Sig(Gen): (2048 SHA(256 , 384)) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(256 , 384))
DRBG 800-90A	874	Fortress Cryptographic Implementation SSL V2.1	SP 800-90A	Deterministic Rnd Bit Generation SSH WPA2 (establishment) IPsec (IKE)	RMI Alchemy MIPS Processor Broadcom XLS Processor	HMAC_Based DBRG: SHA-1, SHA-256, SHA-384, SHA-512
	66	Fortress Cryptographic Implementation V2.0	SP 800-90A	Deterministic Rnd Bit Generation IPsec, MSP	RMI Alchemy MIPS Processor Broadcom XLS Processor	HMAC_Based DBRG: SHA-256, SHA-512
KAS	95	Fortress KAS Implementation V2.0	SP800-56A	Key Agreement IPsec (IKE) MSP (ECDH and DH)	RMI Alchemy MIPS Processor Broadcom XLS Processor	FFC: SHA-256 ECC: P-256 SHA-256 HMAC ED: P-384 SHA-384 HMAC
RSN-KDF	KBKDF 112	Fortress KAS Implementation V2.0	SP800-108	Deriving Keys WPA2	RMI Alchemy MIPS Processor Broadcom XLS Processor	**CTR_Mode:** Length(Min32, Max2048) MACSupported([HMACSHA1] [HMACSHA256]) LocationCounter([AfterFixedData,BeforeFixedData]) rlength([8,16]))
SSH-KDF	CVL 938	Fortress KAS Implementation V2.0	SP800-135	Deriving Keys SSH	RMI Alchemy MIPS Processor Broadcom XLS Processor	SSH(SHA1,SHA-256)

IKE-KDF	CVL 937	Fortress KAS Implementation V2.0	SP800-135	Deriving Keys IPsec (IKE)	RMI Alchemy MIPS Processor Broadcom XLS Processor	IKEv1: AUTH(DSA , PSK)) 256 (SHA 1 , 256 , 384 , 512) 384 (SHA 1 , 256 , 384 , 512) 2048 (SHA 1 , 256 , 384 , 512) IKEv2: 256 (SHA 1 , 256 , 384 , 512) 384 (SHA 1 , 256 , 384 , 512) 2048 (SHA 1 , 256 , 384 , 512)
DSA	1053	Fortress Cryptographic Implementation SSL V2.1	FIPS186-4	IPsec (IKE)	RMI Alchemy MIPS Processor Broadcom XLS Processor	FIPS186-4: KeyPairGen: (2048, 224), (2048, 256), (3072, 256)

The only modes listed are those actually utilized by the modules.

3.8 Non-approved Algorithms

Algorithm	Feature	Allowed in FIPs mode
MD5	NTP,RADIUS	Yes, this is allowed in the approved mode of operation when used as part of a key transport scheme where no security is proved by the algorithm.
NDRNG (FPGA-TRNG)	All	Yes. Used to gather entropy from hardware via two free-running oscillators.
RNG X9.31	MSP	No, provides backwards protocol compatibility when legacy mode is enabled and FIPS is disabled.
RSA KeyGen (FIPS 186-2)	IPsec,TLS,WPA2	No. Admin is not permitted to enable GUI or generate key pairs of type RSA. Refer to Section 7.0.
DSA KeyGen	SSH	No. Disabled while in FIPS mode.
TLS KDF	TLS	No. Admin is not permitted to enable TLS protocol (GUI) while in FIPS mode. Refer to Section 8.0
SNMP KDF	SNMP	No. Admin is not permitted to enable SNMP while in FIPS mode. Refer to Section 8.0

The protocols TLS and SNMP shall not be used when operating in FIPS mode. In particular, none of the keys derived using the TLS or SNMP KDFs can be used in the Approved mode.

4.0 Access Control Policy

The same Crypto Officer may not be simultaneously logged in. However, the module supports concurrent login of different crypto-officer variants. An administrator and maintenance or other combination of crypto-officers may be logged in at the same time.

4.1 Roles and access to service

In general a Crypto Officer is allowed to login and manage the FMP and end users can use cryptographic services. The following table shows a list of services and the roles which have access to them as shown in the following table.

Table 12: Roles each Service is authorized to perform

Role/Services	Encrypt/Decrypt [MSP | RSN | IPsec] PDU Services	Show Status	View Log	Write Configuration (including Bypass, Setting FIPS Mode, Setting Passwords, and Zeroization)	Read Configuration	Diagnostic (including self tests)	Upgrade
Administrator	√	√	√	√	√	√	√
Maintenance		√	√		√	√	
Log Viewer			√				
MSP End User	√						
RSN End User	√						
IPsec End User	√						

4.2 Roles and access to Keys or CSPs

The FMP doesn't allow access to the encryption keys; these are protected within the operating environment.

The following table lists the services that involve using cryptographic keys.

Table 13: Roles who have Access to Keys or CSPs

Service	Access to Cryptographic Keys and CSPs	R	W	E
Encrypt/Decrypt [MSP | RSN | IPsec] PDU Services	[MSP,RSN,IPsec] Session Keys			√
Show Status	No access to crypto material			
Log View	No access to crypto material			
Write Configuration	Change own, Maintenance, and Log viewer password		√	
	Set Access ID *–random* (1) This set option will display the generated Access ID before it's confirmed and written to the database.	√ (1)	√	
	Set Access ID Set Bypass Set FIPS Mode Zeroization Set IEEE 802.11 PSK Digital Signature Generation and Verification		√	
Read Configuration	None of the configured crypto material can be read directly. Only an encrypted copy of these configured materials can be retrieved for the purpose of backing up the configuration.			
Diagnostics	No access to crypto material			
Upgrade	Upgrade Key			√

W = Write access, R = Read access, E = Execute access

4.3 Zeroization

All keys and Critical Security Parameters are stored in a database and zeroized when:

- Restoring the factory defaults
- Manually replaced with new values.
- FMP is rebooted (for keys and CSPs stored in volatile memory)

Please refer to the appropriate User Guide to determine the actual zeroization process.

Table 14: Defaults and Zeroization

CSP	Reset value
Access ID	All Zeros
Administrator Password	Default Password
Log Viewer Password	Default Password
Maintenance Password	Default Password
PSK	All Zeros

4.4 Upgrades

4.4.1 Introduction

The FMP firmware can be upgraded in FIPS mode. The validated upgrade image is downloaded from a workstation via using the CLI. The upgrade image is integrity checked and stored on the internal flash and booted. The previous image is kept stored on flash and can be selected as the boot image in case of problems with the upgrade image.

4.4.2 Selecting Software Image

The FMP stores two, user-selectable copies (or images) of the FMP software on separate partitions of the internal flash memory. Please refer to the User Guide to determine how to select the image for execution.

5.0 Physical Security Policy

5.1 Hardware

The software executes one the following hardware platforms:

- ES210
- ES520 Version 1
- ES520 Version 2
- ES820
- ES2440

5.2 Physical Boundary

All hardware platforms are or will be manufactured to meet FIPS 140-2, L2 requirements.

The FMP Firmware is installed by General Dynamics on a production-quality, FCC certified hardware device, which also define the FMP's physical boundary.

The cryptographic boundary does not include the IO related devices (serial, Ethernet, wireless adapters …) or the network stack code. The cryptographic boundary is concerned with the crypto algorithms, protocols, storage, and authentication. Refer to 'Figure 1 Physical Boundary vs Cryptographic Boundary'.

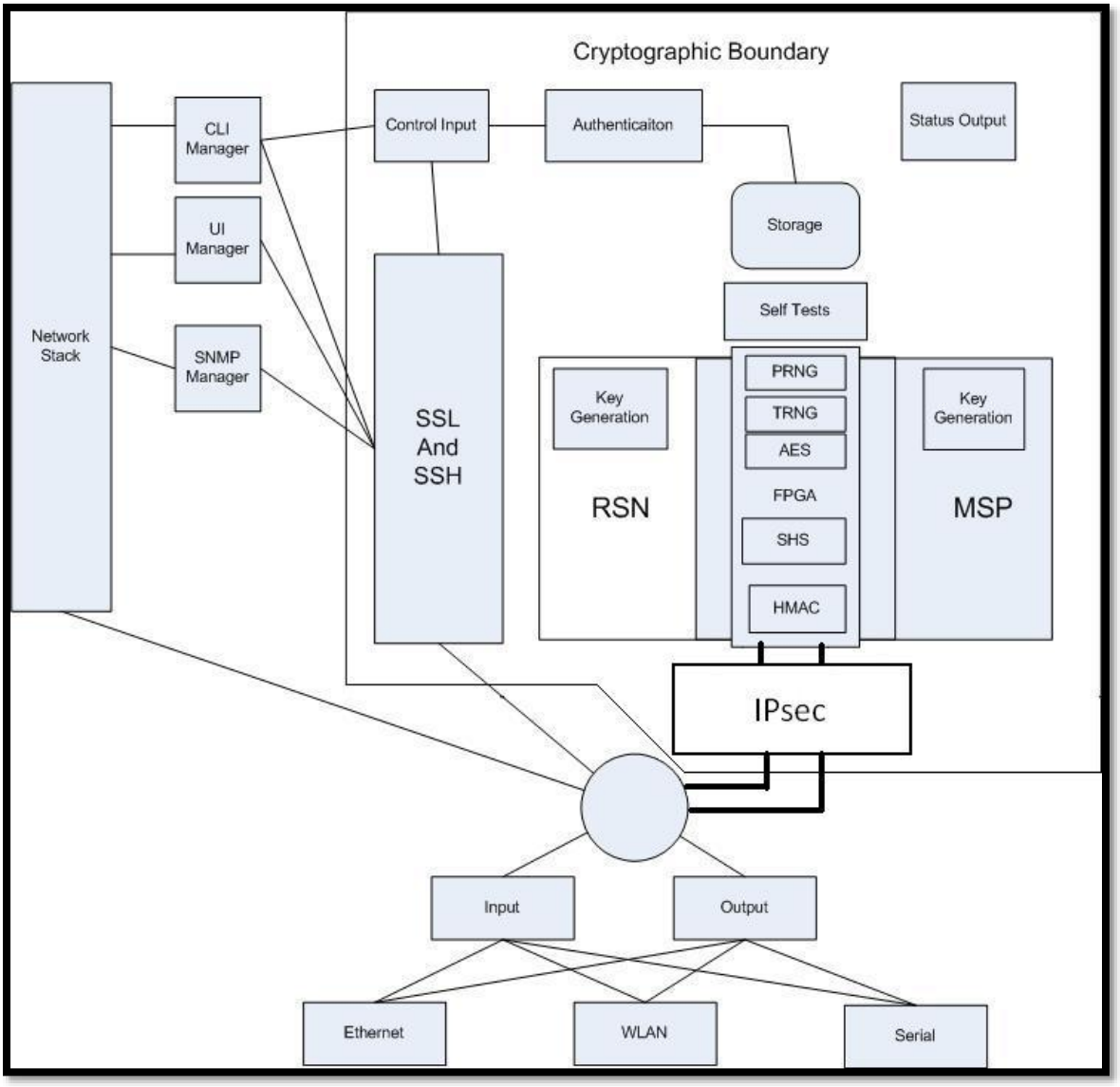

Figure 1 Physical Boundary vs Cryptographic Boundary

5.3 Tamper Evidence Application

These hardware platforms use Loctite 425 blue adhesive to cover screws for tamper evidence as shown in the following figures (1-5). The adhesive is applied during manufacturing. If the glue is removed or becomes damaged it's recommended that the unit be returned to General Dynamics to reapply.

5.4 Tamper Evidence Inspections

The following table details the recommended physical security activities that should be carried out by the Crypto Officer.

Table 15: Recommended Physical Security Activities

Physical Security Object	*Recommended Frequency of Inspection*	*Inspection Guidance*
Appropriate chassis screws covered with Loctite 425 blue epoxy coating.	Daily	Inspect screw heads for chipped epoxy material. If found, remove FMP from service.
Overall physical condition of the FMP	Daily	Inspect all cable connections and the FMP's overall condition. If any discrepancy found, correct and test the system for correct operation or remove FMP from service.

The host hardware platform server must be located in a controlled access area. Tamper evidence is provided by the use of Loctite 425 blue epoxy material covering the chassis access screws.

See the following figures for the appropriate chassis screws.

Figure 2: ES2440 Tamper Evidence (2 screws)

Figure 3: ES820 Tamper Evidence (3 screws)

Figure 4: ES210 Tamper Evidence (2 screws)

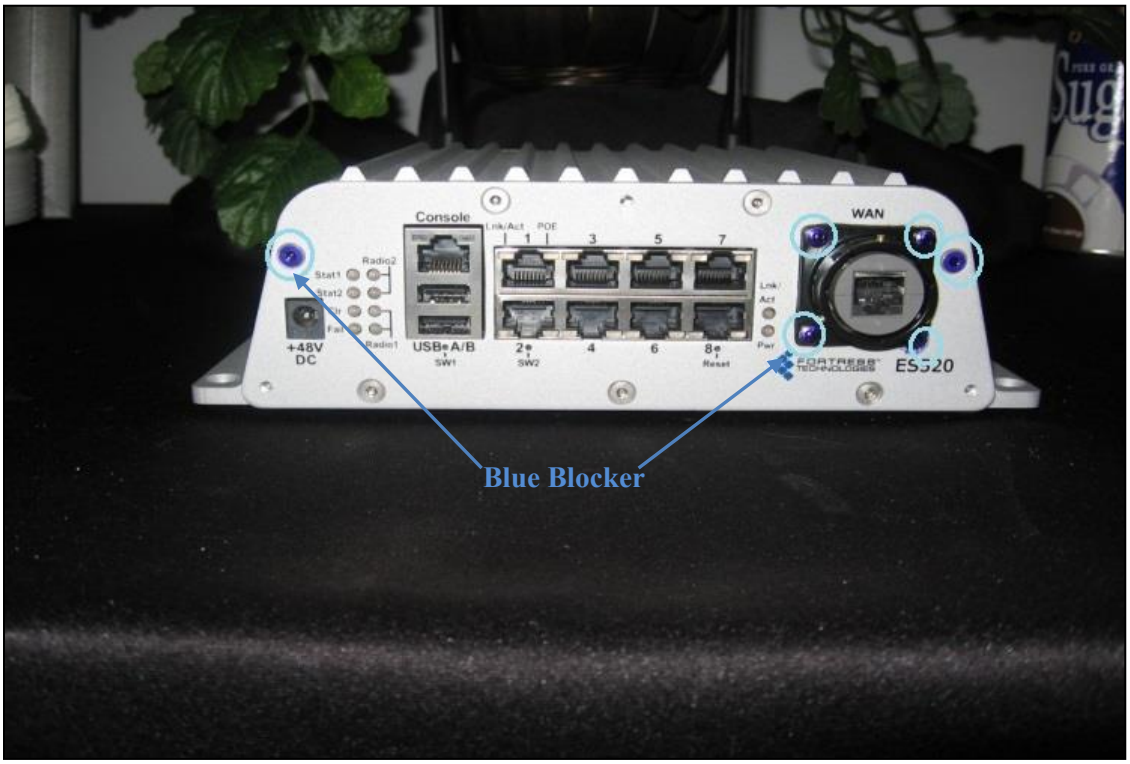

Figure 5: ES520 Version 1 Tamper Evidence (6 screws)

Figure 6: ES520 Version 2 Tamper Evidence (3 screws)

5.5 Tamper Detection

If evidence of tampering is detected:

- Immediately power down the device.
- Disconnect the device from the network.
- Notify the appropriate administrators of a physical security breach.

6.0 Security Policy for Mitigation of Other Attacks Policy

No special mechanisms are built in the FMP; however, the cryptographic module is designed to mitigate several specific attacks above the FIPS defined functions. Additional features that mitigate attacks are listed here:

- The MSP Dynamic Secret Encryption Key is changed at least once every 24 hours, with 4 hours being the factory default duration: Mitigates key discovery.
- In the MSP, the second Diffie-Hellman key exchange produces a dynamic common secret key in each of the modules by combining the other module's dynamic public key with the module's own dynamic private key: *Mitigates "man-in-the-middle" attacks*.
- In MSP, RSN and IPsec key exchanges after the first Diffie-Hellman exchange are encrypted: *Mitigates encryption key sniffing by hackers.*
- In MSP compression and encryption of header information inside of the frame, making it impossible to guess. MSP, RSN, or IPsec uses strong encryption further protects the information. Any bit flipping would be useless in this frame to try to change the IP address of the frame: *Mitigates active attacks from both ends*.
- In both MSP and RSN encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
- In MSP Multi-factor Authentication: The FMP guards the network against illicit access with "multi-factor authentication", checking three levels of access credentials before allowing a connection. These are:
    - *Network authentication* requires a connecting device to use the correct shared identifier for the network
    - *Device authentication* requires a connecting device to be individually recognized on the network, through its unique device identifier.
    - *User authentication* requires the user of a connecting device to enter a recognized user name and password.

7.0 FIPS Mode

The following are the requirements for FIPS mode:

1. The module settings shall be initialized to factory default.
    - Use CLI command: *reset factory*
2. Module must be in FIPS Mode.
    - FIPS operating mode is the default mode of FMP. The FMP Normal operating mode does not comply with FIPS.
    - FIPS can be disabled or enabled through the Command Line Interface (CLI) by the Administrator. When FIPS is disabled FIPS tests are not executed.
    - The operating mode can be determined by whether the CLI prompt displays a FIPS suffix; (e.g.: MPunit1-**FIPS**#), while Normal operating mode displays only the hostname and single-character. (e.g.: MPunit1#).
    - The CLI command 'show fips' reports the current FIPS mode state (On or OFF) and status of self-tests. For FIPS compliance FIPS state must be 'on' and status must be 'ok'.
3. You must verify the unit has the proper seals as described in section '6.0 Physical Security Policy'.
4. The Access ID for a mesh network shall be generated using an approved DRBG.
5. The GUI must be disabled; by default the GUI is enabled.
    - Use CLI command 'set *gui off*' to disable, and command '*show gui'* to confirm status is off.
6. The SNMP module must be disabled; by default SNMP is disabled.
    - Use CLI command '*set snmp -enable n'* to disable, and command *'show snmp'* to confirm SNMP is disabled.
7. The PSK shall be entered using hex values for RSN and IPsec, the passphrase method shall not be used in the FIPS mode.
8. IPsec has to be configured as:
    - SuiteB128 or SuiteB256 only, 'legacy' mode is not FIPS compliant.
        - Use CLI command: set ipsec -crypto [SuiteB256] [SuiteB128].
    - SA sessions must be limited by KB usage.
        - Use CLI command: set ipsec –salifeKB <N> where N is >=1 and <=256,000,000.
9. Only keypairs of EC384 and EC256 are FIPS compliant, RSA2048 keys are not FIPS compliant.
    - The CLI commands '*generate keypair'* and '*generate csr*' shall only be invoked with values of ec384 or ec256 specified for the –type parameter.

8.0 Customer Security Policy Issues

General Dynamics Mission Systems expects that after the FMP's installation, any potential *customer* (government organization or commercial entity or division) *employs its own internal security policy* covering all the rules under which the FMP(s) and the customer's network(s) must operate. In addition, the customer systems are expected to be upgraded as needed to contain appropriate security tools to enforce the internal security policy.

9.0 Acronyms

Table 16: Acronyms

Acronym	Description
DRBG	Deterministic Random Bit Generator
FMP	Fortress Mesh Point
MSP	Mobile Security Protocol Fortress proprietary encryption protocol.
PDU	Protocol Data Unit. (a network frame)
PSK	Pre-Shared Key
RSN	Robust Secure Network Also known as WPA2.