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

Fortress Mesh Points

Hardware:

ES210: Tactical Mesh Point

ES2440: High Capacity Mesh Point

ES440: Infrastructure Mesh Point

ES520 (V1 & V2): Deployable Mesh Point

ES820: Vehicle Mesh Point

Firmware: 5.4.1

December, 2012

This security policy of Fortress Technologies, Inc., 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.

REVISION HISTORY

Rev	Date	Author	Description
1.0	June, 2011	Tony Margalis	Initial Draft
1.1	Nov, 2011	Michael Chapman	Updated for 5.4.1
1.2	Dec, 2011	Michael Chapman	Minor Changes
1.3	July, 2012	Michael Chapman	Updated based on lab questions
1.4	Oct, 2012	J.Pacheco	Updated based upon lab interactions
1.5	Dec, 2012	J.Pacheco	Included ECDSA cert and KAT
1.6	Dec, 2012	J.Pacheco	Updated conditional test list
1.7	Jan, 2013	J.Pacheco	Updated based upon lab comments
1.8	Jan, 2013	J.Pacheco	More updates
1.9	Jan, 2013	J.Pacheco	Small correction
1.10	Jan, 2013	J.Pacheco	Further corrections
1.11	Feb, 2013	J.Pacheco	Adjustment

Contents

LIST OF FIGURES AND TABLES 4
1.0 IDENTIFICATION AND AUTHENTICATION POLICY 5
1.1 ROLE-BASED AUTHENTICATION 5
1.2 SERVICES 6
1.3 AUTHENTICATION AND AUTHENTICATION DATA 6
1.3.1 Authentication Methods 6
1.3.2 Authentication Server Methods 7
1.3.3 Authentication Strength 8
1.3.4 Administrative Accounts 9
1.4 CRYPTOGRAPHIC KEYS AND CSP 9
1.5 FOR MSP 9
1.6 FOR RSN 10
1.7 FOR IPSEC 11
1.8 FOR SSL AND SSH 12
1.9 OTHER CRITICAL SECURITY PARAMETERS 13
1.10 KNOWN ANSWER AND CONDITIONAL TESTS 14
1.10.1 Known Answer Tests 14
1.10.2 Conditional Tests 15
1.11 ALGORITHM CERTIFICATIONS 16
1.12 NON-APPROVED BUT ALLOWED ALGORITHMS 18
2.0 ACCESS CONTROL POLICY 19
2.1 ROLES EACH SERVICE IS AUTHORIZED TO PERFORM 19
2.2 ROLES, SERVICES AND ACCESS TO KEYS OR CSPS 19
2.3 ZEROIZATION 21
2.4 UPGRADES 21
2.4.1 Introduction 21
2.4.2 Selecting Software Image 21
3.0 PHYSICAL SECURITY POLICY 22
3.1 HARDWARE 22
3.2 TAMPER EVIDENCE APPLICATION 22
3.3 TAMPER EVIDENCE INSPECTIONS 22
4.0 SECURITY POLICY FOR MITIGATION OF OTHER ATTACKS POLICY 28
5.0 FIPS MODE 28
6.0 CUSTOMER SECURITY POLICY ISSUES 29

List of Figures and Tables

Figure 1: ES210 Tamper Evidence 23
Figure 2: ES210 Block Diagram 23
Figure 5: ES2440 Tamper Evidence 24
Figure 6: ES2440 Block Diagram 24
Figure 7: ES440 Tamper Evidence 25
Figure 8: ES440 Block Diagram 25
Figure 9: ES520 Version 1 Tamper Evidence 25
Figure 10: Block Diagram ES520 Version 1 25
Figure 11: ES520 Version 2 Tamper Evidence 26
Figure 12: Block Diagram ES520 Version 2 26
Figure 13: ES820 Tamper Evidence 26
Figure 14: ES820 Block Diagram 26

Table 1: Authentication Data 7
Table 2: Probability of guessing the authentication data 8
Table 3: MSP Keys 9
Table 4: RSN Keys 10
Table 5: IPsec Keys 11
Table 6: SSL and SSH Crypto Keys 12
Table 7: Other Keys and Critical Security Parameters 13
Table 8: Known Answer Tests 14
Table 9 Certifications 16
Table 10: Roles each Service is authorized to perform 19
Table 11: Roles who has Access to Keys or CSPs 20
Table 12: Defaults and Zeroization 21
Table 13: Recommended Physical Security Activities 23

1.0 Identification and Authentication Policy

The TOE supports up to 8 total roles that can be defined.

1.1 Role-based Authentication

There are five 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

  Advanced and Simple Views:

  - 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.

  Legacy Views:

  - Operator: account users can view complete system and configuration information and perform a few administrative functions but cannot make configuration changes.
  - csscaisi: the main manager/administrator of the FMP.

There are three non-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 non-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.

- Non-Crypto Officer Roles

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

- MSP End User: This role will utilize either a MSP secure client loaded on a workstation or a MSP secure controller like the FMP 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/L2PT client loaded on a workstation or an IPSec/L2PT controller like a VPN to establish a secure connection.

1.2 Services

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

- Encryption: use the encryption services of the FMP;
  - Roles Allowed: All
- Show Status: observe status parameters of the FMP;
  - Roles Allowed: Only Crypto Officer Roles
- View Log: view log messages;
  - Roles Allowed: Only Crypto Officer Roles
- Write Configuration: change parameters in the FMP including changing the FIPS Mode, Bypass Setting, Zeroization and setting passwords;
  - Roles Allowed: Administrator and csscaisi
- Read Configuration: read parameters in the FMP;
  - Roles Allowed: Administrator, csscaisi, maintenance, and operator
- Diagnostic: execute some network diagnostic and self tests services of the FMP;
  - Roles Allowed: Administrator, csscaisi, maintenance, and operator
- Upgrade: Upgrade the unit with a new release of firmware.
  - Roles Allowed: Administrator, csscaisi

1.3 Authentication and Authentication Data

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

1.3.1 Authentication Methods

All roles must be authenticated if they use FMP services.

For Crypto Officer authentication, a username 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 four secure communication methods to access the FMP. They are:

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

SNMP is authenticated since it's enabled and configured within an already authenticated secure SSL, direct connect or secure SSH 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 AccessID 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 1: Authentication Data

Operator	*Type of Authentication*	*Connect Using*	*Authentication Data*
Log Viewer	Password	HTTP over TLS (HTTPS)	The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters.
Maintenance	Password	HTTP over TLS (HTTPS)	The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters.
Administrator	Password	HTTP over TLS (HTTPS) Direct Connect Secure SSH SNMP	The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters.
operator	Password	HTTP over TLS (HTTPS)	The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 15 characters.
csscaisi	Password	HTTP over TLS (HTTPS)	The possible character space is 91 characters and the password length is between 8 and 32 characters with the default being 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	Master Key or Secret	RSN	16 bytes
IPSec/L2TP	Secret	IPSec/L2TP	16-32 bytes

1.3.2 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 Fortress's Vendor-Specific Attributes (see the user guide for more information).

1.3.3 Authentication Strength

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

Table 2: Probability of guessing the authentication data

Role	Probability of guessing the authentication data	Probability of guessing the authentication data with multiple attempts
Log Viewer **Maintenance** **Administrator** **operator** **csscaisi**	$\frac{90}{91^8(91^{25}-1)}$	The FMP requires that all variants of the Crypto Officer manually enter the password. Manual entry limits the number of attempts to eight per minute. There are 91 distinct characters allowed in the password, and the password may be between 8 and 32 characters, the total number of distinct passwords is $\sum_{n=8}^{32} 91^n$, or $\frac{91^8(91^{25}-1)}{90}$. Therefore, the probability of a randomly chosen password between 8 and 32 characters being the authentication data is $\frac{90}{91^8(91^{25}-1)}$ The maximum number of login attempts can be set between 1 and 9 and lockout duration between 0 and 60 minutes.
MSP End User	$\frac{90\ N}{91^8(91^{25}-1)}$ In which N is 120x10^6	User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Access ID this represents 120x10^6 password attempts per minute. $\frac{90\ N}{91^8(91^{25}-1)}$ In which N is 120x10^6
RSN End User	$\frac{90\ N}{91^8(91^{25}-1)}$ In which N is 120x10^6	Shared Secret: User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Shared Secret this represents 120x10^6 attempts per minute. $\frac{90\ N}{91^8(91^{25}-1)}$ In which N is 120x10^6
		Using EAP: User authentication attempts are limited by accessing a EAP based authentication. The best this could be is no better than the shared secret thus the same rational applies.
IPsec End User	$\frac{90\ N}{91^8(91^{25}-1)}$	Shared Secret: User authentication attempts are limited by FLASH read/write speed to less than 16.7 MB/sec. For a 16 Byte Shared Secret this represents 120x10^6 attempts per

	In which N is 120x10^6	minute.

1.3.4 Administrative Accounts

The FMP uses role based authentication. These are configured by adding administrative accounts configured through the GUI. 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.

1.4 Cryptographic Keys and CSP

1.5 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 SP800-56. All keys are kept in RAM and never stored to disk.

Table 3: MSP Keys

Key	Key Type	Generation	Use
Module Secret Key (Hardkey)	AES: 128, 192, or 256 bit.	Uses manually entered AccessID as material which is a shared secret. Not a valid FIPS key.	Used to mask static Diffie-Hellman public key requests and responses over the wire.
Static Private Key	Diffie-Hellman: 160 or 224 bits ECDH: 384 bits	Automatically generated using the DRBG 800-90.	Along with received Diffie-Hellman Static Public Key from partner is used to generate the Static Secret Encryption Key
Static Public Key	Diffie-Hellman: 1024 or 2048 bits ECDH: 384 bits	Automatically generated using Diffie-Hellman or ECDH.	Sent to communicating module in a packet masked with the Module Secret Key.
Static Secret Encryption Key	AES: 128, 192, or 256 bit.	Automatically generated using Diffie Hellman or ECDH.	Used to encrypt dynamic public key requests and responses over the wire.
Dynamic Private Key	Diffie-Hellman: 160 or 224 bits ECDH: 384 bits	Automatically generated using the DRBG 800-90.	Along with received Dynamic Public Key from partner is used to generate the Dynamic Secret Encryption Key
Dynamic Public Key	Diffie-Hellman: 1024 or 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
Dynamic Secret Encryption Key (DKey)	AES: 128, 192, or 256 bit.	Automatically generated using Diffie Hellman or ECDH.	Used to encrypt all packets between two communicating modules over the wire

Static Group Key (SGK)	AES: 128, 192, or 256 bit.	See Below for Full Text.	Used to encrypt user-data frames until the unicast Dynamic Secret Encryption Key is computed.

The static group key (SGK) computation must be deterministic. That is, each node joining the network specified by the AccessID 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 AccessID for the network.

Note that the static group key (SGK) is generated by using the AccessID and a constant to seed an instance of an approved X9.31 RNG. The X9.31 RNG is then used to produce 128, 192, or 256 bits which are then used as the SGK.

In FIPS mode, the initial AccessID is generated by using an approved DRBG. When joining an established network, the AccessID is manually entered by the Crypto Officer.

1.6 For RSN

An RSN or 802.11i wireless secure LAN can use either a Preshared Secret Key (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 generate 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). The P stands for protocol. IEEE802.11i protocols are allowed in FIPS mode. Please see IG 7.2

All keys are kept in RAM and never stored on disk.

Table 4: RSN Keys

Key	Key Type	Generation	Use
Pairwise Master Key (PMK)	256 bit key.	Using the key generation procedure as defined in the IEEE 802.11 specification. Pre-shared key: Manual entry of PMK (64-hex digits). EAP Method: PMK is created using key material generated during authentication, which is then transferred to FMP using RADIUS protocol.	Used to derive pairwise transient key (PTK).
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	Using the key generation procedure as defined in the IEEE 802.11[2] specification.	Used to protect link between end user station and FMP.

[2] Using the Pseudo Random Function defined in IEEE 802.11i (8.5.1.1), HMAC-SHA1

	key.		
Group Master Key (GMK)	256 bit key.	Using the key generation procedure as defined in the IEEE 802.11 specification.	Used to derive group transient key (GTK).
Group Transient Key (GTK)	For RSN/TKIP and WPA, 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.	Using the key generation procedure as defined in the IEEE 802.11 specification.	Used to protect multicast and broadcast (group) messages sent from FMP to associated end user station. .
Pseudo Random Key **(PRK)**	HMAC 128-bit	DRBG 800-90	IEEE802.11i HMAC SHA-1 PRF function

1.7 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. IPSec uses a Preshared Secret Key (PSK) for key generation.

All keys are kept in RAM and never stored on disk.

Table 5: IPsec Keys

Key	Key Type	Generation	Use
DH Private Key	Diffie-Hellman:160 or 224 bits	Seed is automatically pulled from DRBG 800-90 PRNG	Used to calculate the DH Key
DH Public Key	Diffie-Hellman: 1024 or 2048 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
ECDSA Private Key	ECDSA: 256 or 384 bits	Seed is automatically pulled from DRBG 800-90 PRNG	Used to calculate the ECDSA Key
ECDSA Public Key	ECDSA Key	The ECDSA Private Key is fed to the ECDSA function to automatically generate this key	Used for digital signature to authenticate the peer

1.8 For SSL and SSH

The SSL protocol (TLS 1.0) is used to establish a FIPS secured connection from a management workstation running a standard Internet Browser to either the FMP GUI or the CLI. The SSH (SSH-2.0-OpenSSH_5.8) protocol uses the cryptographic algorithms of the OpenSSH protocol. The cryptographic keys for SSL and SSH are shown in the following table. All keys are kept in RAM and never stored on disk.

Table 6: SSL and SSH Crypto Keys

Key	Key Type	Generation	Use
RSA Private Key **SSL**	RSA Key 2048 bit	Automatically Generated	The RSA private key is used to generate signatures.
RSA Public Key **SSL**	RSA Key 2048 bits (1024 for signature verification)	Automatically Generated	The RSA public key is used to verify signatures.
DH Private Key **SSL & SSH**	Diffie-Hellman: 160 or 224 bits	Seed is automatically pulled from DRBG 800-90 PRNG.	Used along to calculate the Pre-Master Secret from DH
DH Public Key **SSL & SSH**	Diffie-Hellman: 1024 or 2048 bits	The DH Private Key is fed to the Diffie-Hellman function to automatically generate this key	Used along to calculate the Pre-Master Secret from DH
Key Block **SSL & SSH**	Generic Key Information	Automatically generated by SSL Protocol	The Key Block is the keying material that is generated for the AES encryption key. 1
Secret Encryption Key (SSH and SSL Session Key)	AES: 128, 192, 256 bit	The Secret Encryption Key derivation functions use non-approved but allowed algorithms (see section 1.12).	Encrypt data packets

1.9 Other Critical Security Parameters

There are other critical security parameters that present in the FMP as shown in the following table. The Pre-Master secret from the client and DH and the Master Secret for DH are kept in RAM, and all other critical security parameters are in Non-Volatile Storage.

Table 7: Other Keys and Critical Security Parameters

CSP	Type	Generation	Use
Access ID 32 Hex Digits	Seed	Generated by the approved RNG when in FIPS Mode	MSK, SGK & privD-H Group key component and used for authentication
Pre-Master Secret (S) from client	Secret	A 48 byte secret is generated from the client, which is wrapped with a 2048-bit RSA key, resulting in 112 bits of encryption strength	Used to develop the Master Secret
Pre-Master Secret (S) from DH	Diffie-Hellman Key	Diffie-Hellman: Both client and server	Used to develop the Master Secret
Master Secret	Secret	By TLS Protocol	This is the key that is used to encrypt the data
Log Viewer Password	Password	8 to 16 Characters, entered by the Crypto Officer	To authenticate the Log View
Maintenance or operator Password	Password	8 to 16 Characters, entered by the Crypto Officer	To authenticate the operator
Administrator or csscaisi Password	Password	8 to 16 Characters, entered by the Crypto Officer	To authenticate the Maintenance
SNMPV3 Authentication Pass phrase	Pass phrase	8 to 64 Characters	To authenticate the use of SNMPV3
D-H Prime Number	Intermediate Crypto Value	Hard Code Value	The D-H Algorithm
Upgrade Key	RSA Public Key	Public RSA key (256 byte) used to decrypt the SHA hash value that is attached to the firmware image that has been loaded from an external workstation.	Verify the signature that is attached to the upgrade package
Load Key	RSA Public Key	Public RSA key (256 byte) used to decrypt the SHA hash value that is attached to the firmware image that has been loaded from the internal flash drive	Verify the signature that is attached to the load package
PRNG ANSI X9.31 Seed (OpenSSL)	TRNG Random Seeding information	Automatically Generated by TRNG for seeding X9.31 PRNG	Seed the OpenSSL X9.31 PRNG
PRNG ANSI X9.31 Key K1, K2 (OpenSSL)	Triple-DES	Automatically Generated by TRNG	Seed key for OpenSSL X9.31 PRNG
PRNG ANSI X9.31 Seed	TRNG Random	Automatically Generated by TRNG for	Seed the FPGA X9.31 PRNG

(FPGA)	Seeding information	seeding X9.31 PRNG	
PRNG ANSI X9.31 Key K1, K2 (FPGA)	Triple-DES	Automatically Generated by TRNG	Seed key for FPGA X9.31 PRNG
Configuration Data Base Key (Not a CSP)	AES	Hardcoded	Used to obfuscate the Data Base however not a CSP.
Pre-Shared Key	Component	Manual Entry	Used to create the PTK and the PMK
HMAC Key	SSL	Generate within the SSL package	SSL module integrity
HMAC DRBG entropy	Seed	Automatically Generated by TRNG	Entropy used as input to SP 800-90 HMAC DRBG
HMAC DRBG V Value	Counter	Automatically generated by DRBG	Internal V value used as part of SP 800-90 HMAC DRBG
HMAC DRBG Key	Seed	Automatically generated by DRBG	Key value used for the HMAC of the SP 800-90 HMAC DRBG
HMAC DRBG init_seed	Seed	Automatically generated by TRNG	Initial seed value used in SP 800-90 HMAC DRBG

1.10 Known Answer and Conditional Tests

1.10.1 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 8: 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-384 (BYTE-only)** **SHA-256 (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 800-90	**Hash Based DRBG** **[HMAC_DRBG: SHA-1 , SHA-256 , SHA-384, SHA-512]**
DH	**(Key Size Range Tested: 1024 and 2048)**
ECDH	**ECDH-secp (Key Size Range: 384 bits)**
ECDSA	**secp256r1 (P-254) and secp384r1(P-384)**
Known Answer Tests for FPGA	

Algorithm	Modes/States/Key sizes/
AES	**CBC(e/d; 128,192,256)** **CCM (KS: 128)** **(Assoc. Data Len Range: 22 - 30)** **(Payload Length Range: 1 - 32)** **(Nonce Length(s): 13)** **(Tag Length(s): 8)**
SHS	**SHA-1 (BYTE-only)** **SHA-384 (BYTE-only)**
HMAC	**HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) SHS** **HMAC-SHA384 (Key Size Ranges Tested: KS<BS) SHS**
ANSI X9.31 PRNG	**ANSI X9.31 PRNG** **[TDES-2Key];**
Known Answer Tests for OPENSSL	
Algorithm	**Modes/States/Key sizes/**
AES	**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	**SHA-1 (BYTE-only)** **SHA-224 (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-SHA224 (Key Size 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**
RSA Signature Generation	**ALG[RSASSA-PKCS1_V1_5]; SIG(gen);**
RSA Signature Verification	**ALG[RSASSA-PKCS1_V1_5]; SIG(ver); 2048 , SHS: SHA-1**

1.10.2 Conditional Tests

This section describes the conditional tests run on the system.

Conditional tests	
Tests	**Condition**
Pairwise Consistency Tests:	**Generating new RSA key pair**

RSA(ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-1).	**Power on self-test; FIPS mode change; Any security policy change**
Software Load Test	**Software image load/install**
Broadcast Bypass Test	**Power on self-test; FIPS mode change; Any security policy change; Change to the bypass mode**
Guest Create Bypass Test	**Power on self-test; FIPS mode change; Any security policy change; Change to the bypass mode**
Unknown Destination Address Bypass Test	**Power on self-test; FIPS mode change; Any security policy change; Change to the bypass mode**
Unknown Host to Guest Bypass Test	**When the bypass mode is changed to "off"**
Receive Clear Packet on an Encrypted Interface Bypass Test	**Power on self-test; FIPS mode change; Any security policy change; Change to the bypass mode**
CCMP Bypass Test	**Power on self-test; FIPS mode change; Any security policy change; Change to the bypass mode**
Manual Key Entry Test	**At every key or component entry**
Random Number Generation: DRBG, PRNG, TRNG	**Power on self-test; Every generation of a random number**

1.11 Algorithm Certifications

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

Table 9 Certifications

Certifications for CRYPTLIB					
Algorithm	**Cert #**	**Implementation**	**Operational Environment**	**Val Date**	**Modes/States/Key sizes/ Description/Notes**
AES	1519	**Fortress Cryptographic Implementation**	AMD Alchemy MIPS Processor	12/6/2010	**ECB(e/d; 128,192,256);** **CBC(e/d; 128,192,256)**
SHS	1357	**Fortress Cryptographic Implementation**	AMD Alchemy MIPS Processor	12/6/2010	**SHA-1** (BYTE-only) **SHA-256** (BYTE-only) **SHA-384** (BYTE-only) **SHA-512** (BYTE-only)
HMAC	889	**Fortress Cryptographic Implementation**	AMD Alchemy MIPS Processor	12/6/2010	**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 800-90	66	**Fortress Cryptographic Implementation**	AMD Alchemy MIPS Processor	12/6/2010	**Hash_Based DRBG** **[HMAC_DRBG: SHA-1 , SHA-256 , SHA-384, SHA-512]**
KAS	10	**Fortress Cryptographic Implementation**	AMD Alchemy MIPS Processor	12/6/2010	**FFC: SCHEMES [dhEphem (KARole(s): Initiator/ Responder) (FC: SHA256)** **ECC: SCHEMES { EphemeralUnified (EC:P-256 SHA256 HMAC) (ED: P-384 SHA384 HMAC))]**
ECDSA	371	**Fortress Cryptographic Implementation**	AMD Alchemy MIPS Processor	12/6/2012	**secp256r1 (P-256) and secp384r1(P-384)**

Certifications for FPGA

Algorithm	Cert #	Implementation	Operational Environment	Val Date	Modes/States/Key sizes/ Description/Notes
AES	694	**Fortress SWAB FPGA Algorithms**	Xilinx Spartan FPGA	1/17/2008	**CBC(e/d; 128,192,256)** **CCM (KS: 128)** **(Assoc. Data Len Range: 22 - 30)** **(Payload Length Range: 1 - 32)** **(Nonce Length(s): 13)** **(Tag Length(s): 8**
SHS	721	**Fortress SWAB FPGA Algorithms**	Xilinx Spartan FPGA	1/17/2008	**SHA-1** (BYTE-only)
HMAC	371	**Fortress SWAB FPGA Algorithms**	Xilinx Spartan FPGA	1/17/2008	**HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) SHS** **HMAC-SHA384 (Key Size Ranges Tested: KS<BS) SHS**
RNG	#406	**Fortress SWAB FPGA Algorithms**	Xilinx Spartan FPGA	1/17/2008	**ANSI X9.31 [TDES-2Key];**

Certifications for OPENSSL

Algorithm	Cert #	Implementation	Operational Environment	Val Date	Modes/States/Key sizes/ Description/Notes
AES	688	**Fortress SWAB 5.0 SSL**	AMD Alchemy MIPS Processor	12/31/2007	**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	717	**Fortress SWAB 5.0 SSL**	AMD Alchemy MIPS Processor	12/31/2007	**SHA-1** (BYTE-only) **SHA-224** (BYTE-only) **SHA-256** (BYTE-only) **SHA-384** (BYTE-only) **SHA-512** (BYTE-only)

HMAC	367	**Fortress SWAB 5.0 SSL**	AMD Alchemy MIPS Processor	12/31/2007	**HMAC-SHA1 (Key Sizes Ranges Tested: KS=BS) SHS** **HMAC-SHA224 (Key Size 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**
RNG	402	**Fortress SWAB 5.0 SSL**	AMD Alchemy MIPS Processor	12/31/2007	**ANSI X9.31 [TDES-2Key]**
RSA	439	**Fortress Secure Bridge Algorithms (SSL)**	AMD Alchemy MIPS	11/4/2008	**FIPS186-2 ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048 , SHS: SHA-1**

.

1.12 Non-Approved but Allowed Algorithms

This section enumerates the algorithms in used which are not approved, but which are allowed:

- Per IG 7.2, IG 7.8, and IG D.8, a non-Approved but allowed legacy KDF is used in the 802.11i, TLS/SSL, and SSH protocols.
- MD5
- NDRNG – the module's TRNG acts as an entropy source for the Approved RNG and DRBG.
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)

The KDF in Counter Mode function as defined in SP 800-108 (section 5.1) is used to derive the secret keys as required by IG 7.10, for use in the 802.11i key agreement scheme.

2.0 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.

2.1 Roles each Service is authorized to Perform

In general a Crypto Officer is allowed to login and manage the FMP and end users can use cryptographic services as shown in the following table.

Table 10: Roles each Service is authorized to perform

Role/Services	Encryption	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			√				
csscaisi		√	√	√	√	√	√
operator		√	√		√	√	
MSP End User	√						
RSN End User	√						
IPSec End User	√						

2.2 Roles, Services and Access to Keys or CSPs

The FMP doesn't allow the access of encryption keys and most critical security parameters. These are protected within the operating environment. The FMP does allow the configuration of some important parameters and passwords as detailed in the following table.

Table 11: Roles who has Access to Keys or CSPs

Service	Role	Access to Cryptographic Keys and CSPs	R	W	E
Encryption and Decryption	MSP RSN	Access ID PreShared Secret (IEEE) All Keys			√
Digital Signature Generation and Verification	RSN	Keys	√		√
Key Generation	RSN	Key creation only		√	√
Show Status	Administrator Maintenance Logviewer csscaisi operator	None	√		
View Log	Administrator Maintenance Logviewer csscaisi operator	None	√		
Write Configuration	Administrator	Change own, Maintenance, and Logveiwer password		√	
	csscaisi	Change own and operator password		√	
	Administrator csscaisi	Set Access ID Set Bypass Set FIPS Mode zeroization Set SNMP Passphase Set IEEE 802.11 Preshared Key		√	
Read Configuration	Administrator Maintenance Csscaisi operator	None	√		
Diagnostic **(including self tests)**	Administrator Maintenance csscaisi operator	None			√

Upgrade	Administrator csscaisi	Upgrade Key			√

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

2.3 Zeroization

All keys and Critical Security Parameters (CSP)s are stored in a database and zeroed when restoring the defaults. Other configuration values are returned to their factory default. Please refer to the appropriate User Guide to determine the actual zeroization process.

Table 12: Defaults and Zeroization

CSP	Reset value
AccessID	All Zeros
Administrator Password	Default Password
Log Viewer Password	Default Password
Maintenance Password	Default Password
CAISI Password	Default Password
operator Password	Default Password
SNMPV3 Authentication Pass phrase	FSGSnmpAdminPwd.
Preshared Key	All Zeros

2.4 Upgrades

2.4.1 Introduction

The FMP firmware can be upgraded in FIPS mode. The validated upgrade image is downloaded from a workstation via using the GUI. 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.

2.4.2 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.

3.0 Physical Security Policy

3.1 Hardware

The FCB executes the following hardware platforms:

- ES210
- FC-X
- ES2440
- ES440
- ES520 Version 1
- ES520 Version 2
- ES820

Refer to the figures below.

3.2 Tamper Evidence Application

ES210, ES2440, ES440, ES820

The hardware uses 3/8 X 3/4 inch tamper evidence destructible vinyl tape as shown in the following figures. The tape is applied during manufacturing. If the tape is removed or becomes damaged it's recommended that the unit be returned to Fortress to reapply.

FC-X, ES520V1 and ES520V2

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

3.3 Tamper Evidence Inspections

The FMP Firmware is installed by Fortress Technologies on a production-quality, FCC certified hardware device, which also define the FMP's physical boundary. All hardware platforms are or will be manufactured to meet FIPS 140-2, L2 requirements. The following table details the recommended physical security activities that should be carried out by the Crypto Officer.

The host hardware platform server must be located in a controlled access area. Tamper evidence is provided by the use of epoxy potting material covering the chassis access screws or by vinyl tape.

If using vinyl tape, the tape is applied to the edge of the panel. If using epoxy potting material then some screws on the front and back panel are covered with the material for tamper evidence, see the following figures.

Table 13: Recommended Physical Security Activities

Physical Security Object	*Recommended Frequency of Inspection*	*Inspection Guidance*
Appropriate chassis screws covered with epoxy coating.	Daily	Inspect screw heads for chipped epoxy material. If found, remove FMP from service.
Tape appropriately Applied	Daily	Inspect the tape to make sure it securely in place.
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.

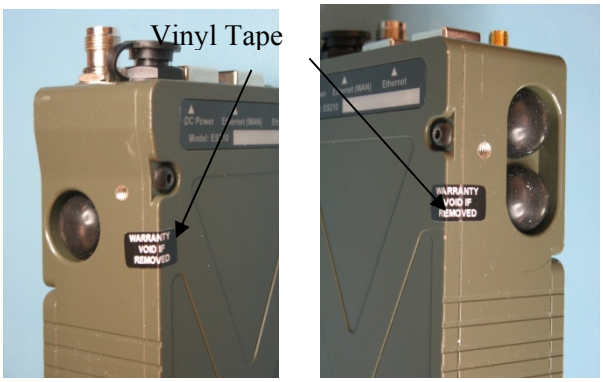

Figure 1: ES210 Tamper Evidence

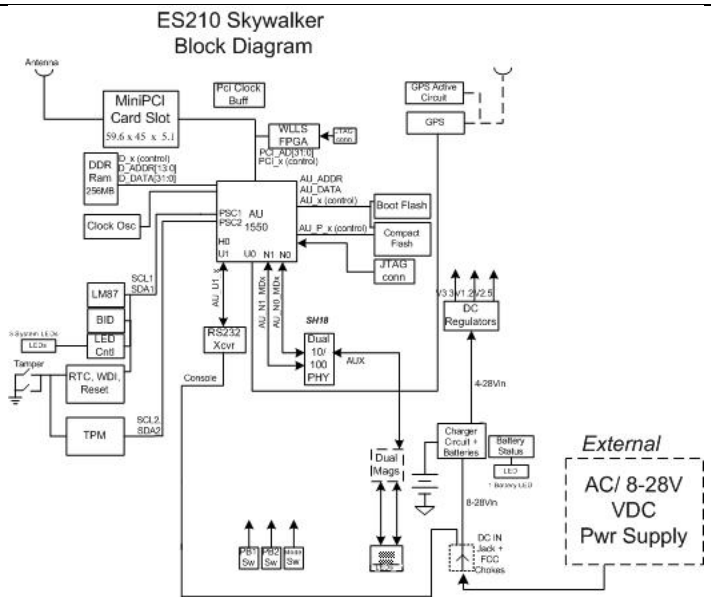

Figure 2: ES210 Block Diagram

Figure 3: ES2440 Tamper Evidence

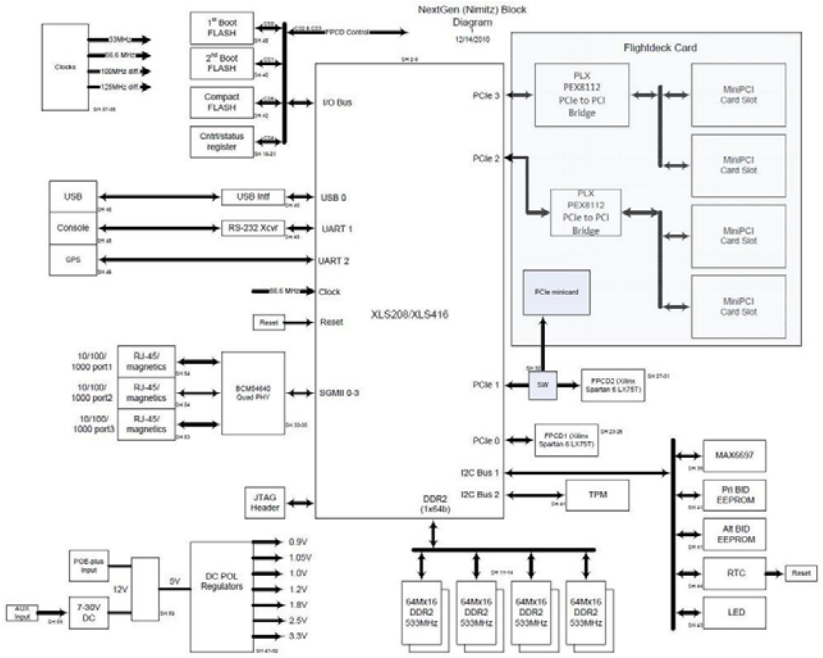

Figure 4: ES2440 Block Diagram

Figure 5: ES440 Tamper Evidence

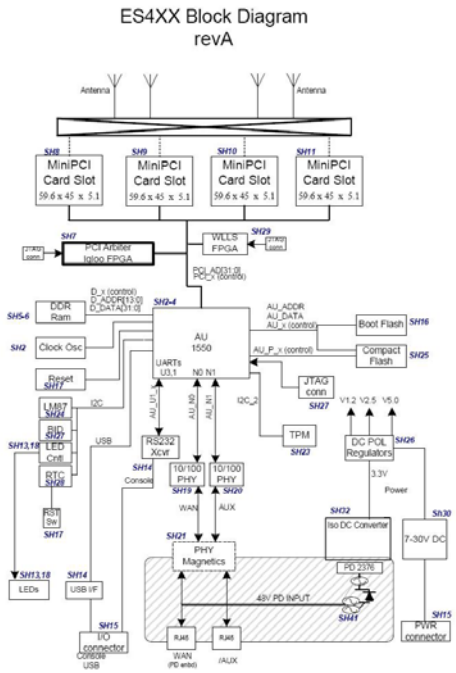

Figure 6: ES440 Block Diagram

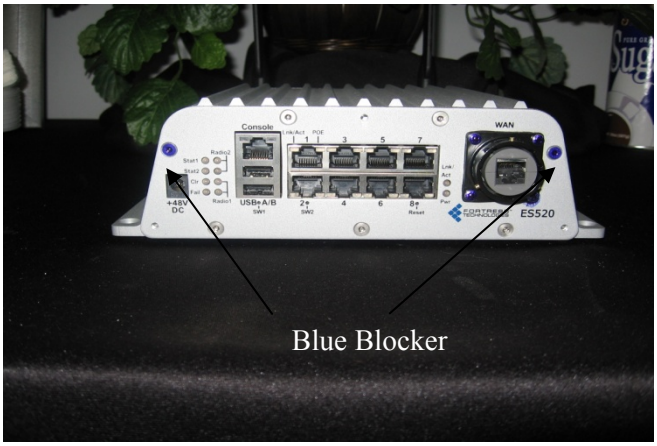

Figure 7: ES520 Version 1 Tamper Evidence

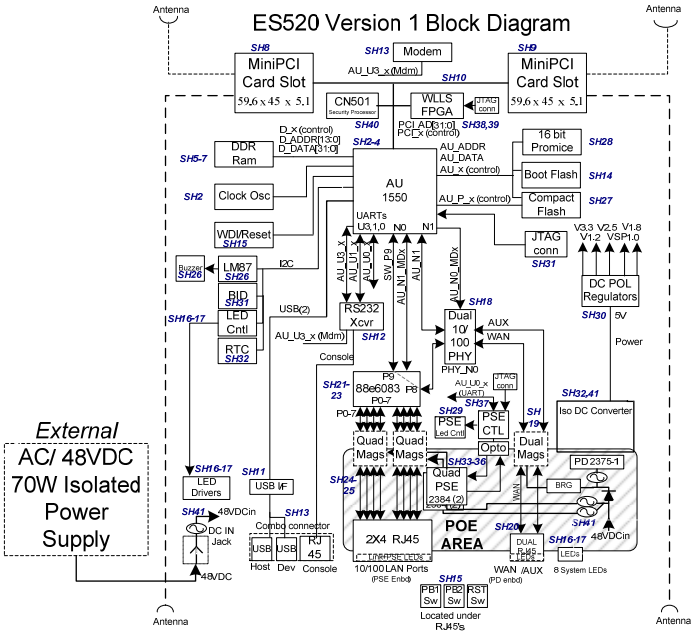

Figure 8: Block Diagram ES520 Version 1

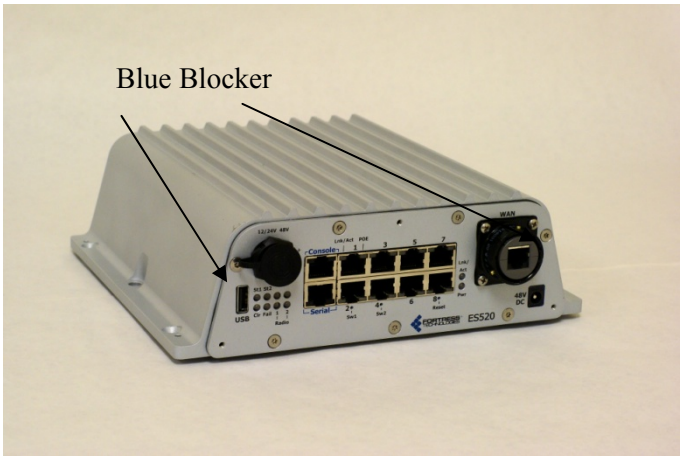

Figure 9: ES520 Version 2 Tamper Evidence

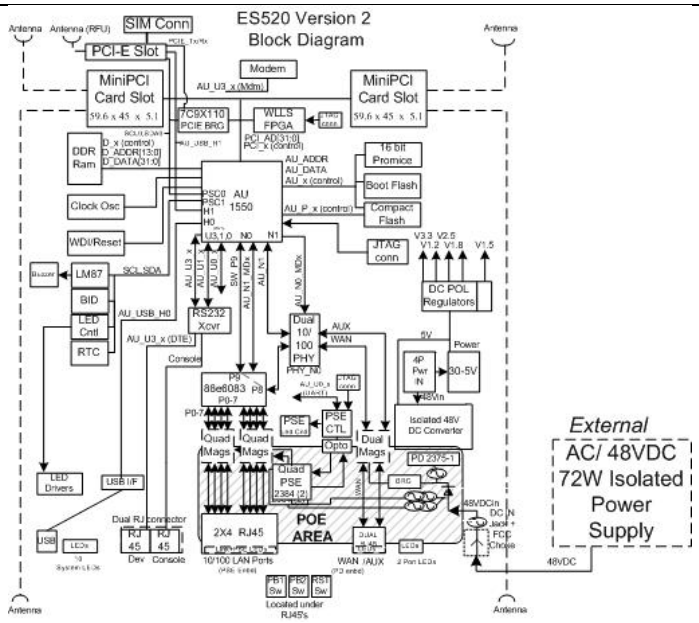

Figure 10: Block Diagram ES520 Version 2

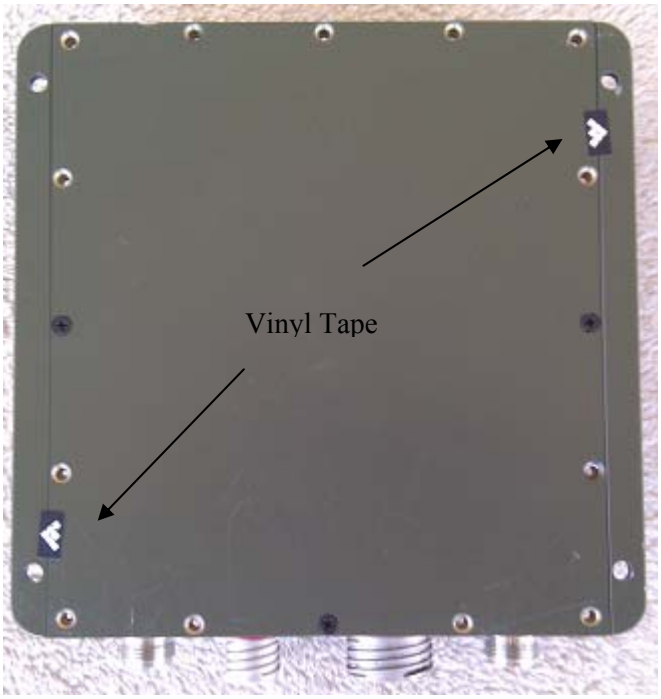

Figure 11: ES820 Tamper Evidence

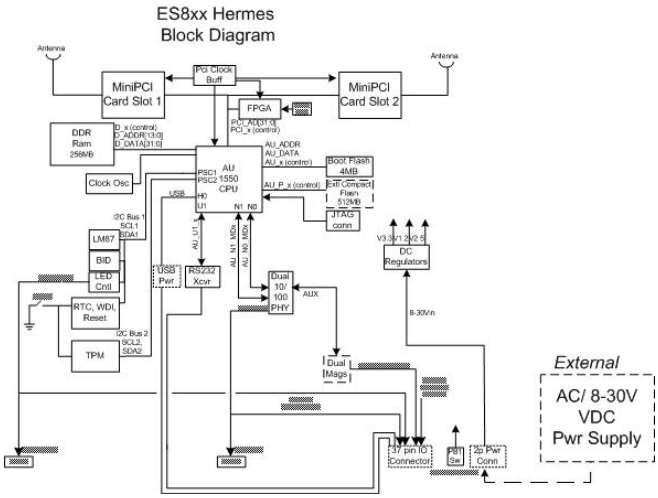

Figure 12: ES820 Block Diagram

4.0 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:

1. 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.
2. 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*.
3. In MSP, RSN and IPsec key exchanges after the first Diffie-Hellman exchange are encrypted: *Mitigates encryption key sniffing by hackers.*
4. In MSP compression and encryption of header information inside of the frame, making it impossible to guess. MSP, RSN, IPsec or SSL 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*.
5. 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.*
6. 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:
    a) *Network authentication* requires a connecting device to use the correct shared identifier for the network
    b) *Device authentication* requires a connecting device to be individually recognized on the network, through its unique device identifier.
    c) *User authentication* requires the user of a connecting device to enter a recognized user name and password.

5.0 FIPS Mode

The following are the requirements for FIPS mode:

a. At module start-up the module shall be set to FIPS Mode.
b. The AccessID shall be generated using the approved RNG option or to the network AccessID value if joining an established network. A valid FIPS network shall use an approved RNG generated AccessID.
c. The Pre-Shared Key shall be entered using 64-hex values. The passphrase method shall not be used in the FIPS mode of operation.
d. You must verify the unit has the proper seals and/or security tape as described in section 4.2 and 4.3.

The FMP comes up in the FIPS operating mode during module initialization. FIPS can be disabled or enabled through the GUI or through the Command Line Interface (CLI) by the Administrator. When FIPS is disabled FIPS tests are not executed.

- On the GUI the Mode Indicator (Left Top of the GUI Screen) will show whether the unit is in Normal or FIPS module. To change operating mode on the GUI:
    - Log on to the Bridge GUI through an Administrator-level account and select Configuration -> Security from the menu on the left. On the Security screen click EDIT.
    - In the Edit Security screen's Security Settings frame change the Operating Mode to Normal or FIPS.
- To change operating mode on the CLI
    - The operating mode can be determined by whether the command prompt displays FIPS; Normal operating mode displays only the hostname and single-character command prompt (> or #).
    - FIPS operating mode is the default Bridge mode of FMP: Bridge CLI operation. The FMP Normal operating mode does not comply with FIPS.
    - Change between operating modes with the set fips command. To turn FIPS operating mode on:
        - # set fips on
- To place the Bridge in Normal operating mode, turn FIPS operating mode off:
    - FIPS# set fips off
- You must be logged on to an administrator-level account to change the operation mode.
- You must verify the unit has the proper seals and/or tape as described in the Security Policy.

6.0 Customer Security Policy Issues

Fortress Technologies, Inc. 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.