Enhanced Bandwidth Efficient Modem (EBEM) Cryptographic Module Non-Proprietary Security Policy

Document Number 1179470, Rev. 006
November 12, 2015

Prepared by:

ViaSat

ViaSat, Inc.
6155 El Camino Real
Carlsbad, CA 92009

Record of Review and History

Document Number	Rev.	Rationale	Release Date	Affected Pages
1148155	001	Initial Release in Agile	October 31, 2012	All
1179470	001	Updated for Simplex Encryption/TxPI/AH ECP	March 13, 2015	All
1179470	002	Updated in response to InfoGard and CMVP Comments for Simplex Encryption/TxPI/AH ECP	August 7, 2015	All
1179470	003	Updated in response to InfoGard and CMVP Comments	October 7, 2015	All
1179470	004	Updated in response to CMVP Comments	October 16, 2015	All
1179470	005	Updated in response to CMVP Comments	October 27, 2015	3, 5
1179470	006	Updated for FW v02.07.02.	November 12, 2015	1, 3, 4

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Module Overview

The Enhanced Bandwidth Efficient Modem (EBEM) Cryptographic Module is a multi-chip standalone module as defined in the Federal Information Processing Standards (FIPS) 140-2. The module has multiple configurations as shown below:

Category	Hardware Version	Firmware Versions
Strategic	P/N 1010162, Version 1	02.07.02
	P/N 1010162 with ESEM, Version 1 (also referred to as P/N 1091549, Version 1)	02.07.02
	P/N 1075559, Version 1	02.07.02
	P/N 1075559 with ESEM, Version 1 (also referred to as P/N 1091551, Version 1)	02.07.02
	P/N 1047117: Tamper seal applied over the ESEM	N/A
Tactical	P/N 1010163, Version 1	02.07.02
	P/N 1010163 with ESEM, Version 1 (also referred to as P/N 1091550, Version 1)	02.07.02
	P/N 1075560, Version 1	02.07.02
	P/N 1075560 with ESEM, Version 1 (also referred to as P/N 1091552, Version 1)	02.07.02
	P/N 1047117: Tamper seal applied over the ESEM	N/A

The cryptographic boundary is realized as the external surface of the EBEM enclosure. The EBEM is a high-speed, high performance, flexible and compatible Single Channel Per Carrier (SCPC) modem. The EBEM incorporates the latest technology in advanced modulation and coding, while providing backwards interoperability with the majority of existing SCPC modems. It offers optimal power and bandwidth efficiency with 16-ary modulation and Turbo-coding. It supports a large range of user data rates, from 64 kbps up to 155 Mbps.

Figure 1: Image of the Cryptographic Module
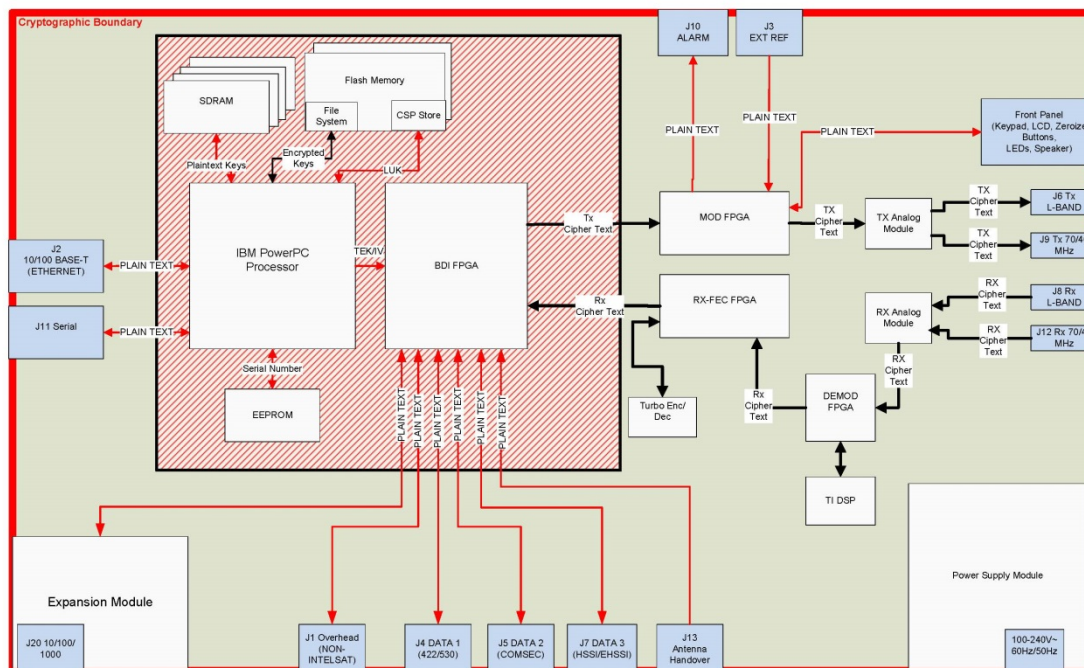
Figure 2: Block Diagram

2. Security Level

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

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
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	N/A

3. Modes of Operation

Approved mode of operation

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

Table 2**: Approved Algorithms and CAVP Validated Cryptographic Functions**

CAVP Algorithm Implementation	Algorithm	Description	Cert. #
EBEM AES CTR 1	AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption (in FPGA for data) Modes: ECB (Encryption only), CTR (Encryption and Decryption) Key sizes: 256 bits	3449
EBEM AES CTR 2	AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption (in FPGA for data) Modes: ECB (Encryption only), CTR (Encryption and Decryption) Key sizes: 256 bits	3450
EbemCrypto	AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption (in Processor for CSPs) Modes: ECB Key sizes: 256 bits	3448
	AES Key Wrap	[SP 800-38F] Functions: Wrap, Unwrap (for CSPs) Key sizes: 256 bits Caveat: Key establishment methodology provides 192 or 256 bits of encryption strength.	3448 (KTS)
	DRBG	[SP 800-90A] Functions: CTR DRBG Security Strengths: 256 bits	844
	ECDSA	[FIPS 186-2] Functions: Signature Verification (for ESEM configuration files) Curves/SHA sizes: P-521 with SHA-1 <u>Note</u>: *CAVP Tested as FIPS 186-4 per CAVP guidelines but still considered FIPS 186-2 because of curve/SHA size used.*	697
	ECDSA	[FIPS 186-4] Functions: Signature Verification (for firmware images, and feature files) Curves/SHA sizes: P-521 with SHA-512	697

	ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification (for key transport messages) Curves/SHA sizes: P-384 with SHA-384	697
	HMAC	[FIPS 198-1] Functions: Generation, Verification (for SMAT and PBKDF2 authentication) SHA sizes: SHA-1, SHA-384, SHA-512	2196
	KAS	[SP 800-56A] Schema: Ephemeral Unified Parameter sets/Key sizes: EE Supports 256 bits of security.	60
	KAS	[SP 800-56A] Schema: One Pass DH Parameter sets/Key sizes: ED Supports 192 bits of security.	60
	SHA	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1 (not used in sig gen), SHA-384, and SHA-512	2846
NetSNMP KDF	KDF	[SP 800-135] Functions: SNMP KDF	455 (CVL)
OpenSSH KDF	KDF	[SP 800-135] Functions: SSH KDF	454 (CVL)
OpenSSL SHA	SHA	[FIPS 180-4] Functions: non-Digital Signature Applications SHA sizes: SHA-1, SHA-256, SHA-512	2690
SHA-256 uClibc	SHA	[FIPS 180-4] Functions: non-Digital Signature Applications SHA sizes: SHA-256	2689

In FIPS mode, the cryptographic module supports the following non-Approved, but allowed algorithms and protocols:

- NDRNG – Hardware Non-Deterministic RNG. The NDRNG output is used to seed the FIPS Approved DRBG. The NDRNG produces entropy in 128-byte blocks.

- The following are protocols and algorithms for which "no security is claimed". These are considered *plaintext communication channels* for the purposes of this module. This is allowed in FIPS mode because the ViaSat EBEM's proprietary FIPS Approved key establishment and encryption algorithms (as shown in *Table 2*) protect sensitive information that is sent over the Telnet, SSH, SNMPv1, SNMPv3, FTP, and SFTP protocols.

- o Telnet – no security is claimed. Uses no algorithms.
- o SSH – no security is claimed. Uses the following algorithms:
    - ▪ Protocol Defined Algorithm Names:
        - • Ciphers: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc
        - • Key Exchange Algorithms: ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group-exchange-sha-256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1
        - • Public Key Algorithms: Ssh-dss, Ssh-rsa, Ecdsa-sha2-nistp256, Ecdsa-sha2-nistp384, Ecdsa-sha2-nistp521
        - • MACs: hmac-sha1, hmac-sha2-256, hmac-sha2-512
    - ▪ Corresponding FIPS Algorithms:
        - • Ciphers: AES (non-compliant), TDES (non-compliant)
        - • Key Exchange Algorithms: ECDH (non-compliant), DH (non-compliant), SHA (non-compliant)
        - • Public Key Algorithms: DSA (non-compliant), RSA (non-compliant), ECDSA (non-compliant), SHA (non-compliant)
        - • MACs: HMAC (non-compliant), SHA (non-compliant)
- o SNMPv1 – no security is claimed. Uses no algorithms.
- o SNMPv3 – no security is claimed. Uses the following algorithms:
    - ▪ Protocol Defined Algorithm Names: HMAC-MD5, HMAC-SHA, AES, DES
    - ▪ Corresponding FIPS Algorithms: HMAC (non-compliant), SHA (non-compliant), AES (non-compliant), MD5, DES
- o FTP – no security is claimed. Uses no algorithms.
- o SFTP – no security is claimed. Uses the following algorithms:
    - ▪ Same as SSH above.

- SP 800-132 PBKDF2 – no security is claimed. Anything imported into the module encrypted using PBKDF keys is considered *plaintext* for the purposes of this module. This is allowed in FIPS mode because the ViaSat EBEM's proprietary FIPS Approved key establishment and encryption algorithms (as shown in *Table 2*) protect sensitive information that is sent encrypted by PBKDF keys. Corresponding FIPS Algorithm: PBKDF (non-compliant).

- EC Diffie-Hellman (key agreement; key establishment methodology provides 160 bits of encryption strength). Ephemeral Unified KAS parameter set EE when used with SHA-1 in crypto compatibility mode. (*This is part of our transition plan to eventually eliminate SHA-1 support while maintaining backward compatibility with older SW/FW versions.*)

The EBEM cryptographic module does not contain a Non FIPS Approved mode. The FIPS Approved mode of operation is indicated by the firmware version. If the version is one that has a FIPS certificate, then the user knows they are operating in a FIPS Approved mode of operation. The unauthenticated service "Display status" allows a user to view the firmware version by scrolling to "General→SW Version".

4. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- J1 OVERHEAD (NON-INTELSAT): Data input, data output
- J3 EXT REF: Control input
- J4 DATA 1 (422/530): Data input, data output, control input
- J5 DATA 2 (COMSEC): Data input, data output, control input
- J7 DATA 3 (HSSI): Data input, data output
- J6 TX L-BAND: Data output, status output
- J8 RX L-BAND: Data input, control input
- J9 TX 70/140 MHz: Data output, status output
- J12 RX 70/140 MHz: Data input, control input
- J20 10/100/1000 (only available with ESEM installed): Data input, data output, status output (status is only PADQ link quality packets during an active PPPoE session)
- 100-240V~ 60Hz/50Hz: Power port, power input
- J13 ANT HANDOVER (only available in Tactical versions): Control input
- J10 ALARM: Status output
- J11 SERIAL: Data input, data output, control input, status output
- J2 10/100 BASE-T: Data input, data output, control input, status output
- Keypad: Control input, data input
- LCD: Status output, Data output
- Zeroize buttons: Control input
- LEDs: Status outputs
- Speaker: Status outputs

5. Identification and Authentication Policy

Assumption of roles

The EBEM cryptographic module supports five distinct operator roles (Operator, Administrator, Cryptographic-Officer, Peer Modem, and ViaSat, Inc.). The cryptographic module shall enforce the separation of roles using role-based and identity-based operator authentication.

Table 3: Roles and Required Identification and Authentication

Role	Description	Type of Authentication	Authentication Data
Operator	A "User" from the FIPS 140-2 perspective.	Identity-based	User name and Password
Administrator	A "User" from the FIPS 140-2 perspective.	Identity-based	User name and Password

Role	Description	Type of Authentication	Authentication Data
Cryptographic-Officer (CO)	The "Crypto Officer" from the FIPS 140-2 perspective. The CO may only access the module via the Front Panel.	Identity-based	User name and Password
Peer Modem	The modem at the other end of the RF link, with whom the TEK negotiation occurs.	Role-based	HMAC Key, also referred to as SMAT (Shared Modem Authentication Token)
		Identity-based	Identity and Authentication (IA) FIPS 186-4 ECDSA Signature Key Pair
ViaSat, Inc.	Signer of firmware image files and feature files. A ViaSat trust anchor used to validate authenticity when loading these files on modem.	Identity-based	FIPS 186-4 ECDSA Signature Key
ViaSat, Inc.	Signer of ESEM configuration files. A ViaSat trust anchor used to validate authenticity when loading these files on modem.	Identity-based	FIPS 186-2 ECDSA Signature Key

Table 4: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	The password is a minimum of 8-characters chosen from upper and lowercase letters, 10 digits, and 10 special characters. The probability that a random attempt will succeed or a false acceptance will occur is $1/72^8$ which is less than $1/1,000,000$. The module will lockout after a maximum of 5 consecutive failed login attempts. The probability of successfully authenticating to the module within one minute is $5/72^8$ which is less than $1/100,000$.
HMAC Key	The probability that a random attempt will succeed or a false acceptance will occur is $1 / 2^{160}$ which is less than $1/1,000,000$. The HMAC key must be manually entered at the front panel. No more than 10 unique authentication attempts can occur in any one minute period. The probability of successfully authenticating to the module within one minute is $10 / 2^{160}$ which is less than $1/100,000$.
FIPS 186-4 ECDSA IA Signature Key	Using the EBEM's ECDSA implementation, the probability that a random attempt will succeed is the strength of the embedded SHA-384 function, or $1 / 2^{192}$, which is less than $1/1,000,000$. The IA key pair takes 20 seconds to fill so no more than 3 attempts can occur in any one minute period. The probability of successfully authenticating to the module within a one minute period is $3 / 2^{192}$ (which is $< 1/100,000$) due to a maximum of three attempts per minute.
FIPS 186-4 ECDSA Firmware/Feature Signature Key	Using the EBEM's ECDSA implementation, the probability that a random attempt will succeed is the strength of the embedded SHA-512 function, or $1 / 2^{256}$, which is less than $1/1,000,000$. If the signature verification fails, the user must reboot before transferring a different firmware image to the modem and trying the validation again. The probability of successfully authenticating to the module within a one minute period is $1 / 2^{256}$ (which is $< 1/100,000$) due to a maximum of one attempt per minute.

Authentication Mechanism	Strength of Mechanism
FIPS 186-2 ECDSA Signature Key	Using the EBEM's ECDSA implementation, the probability that a random attempt will succeed is the strength of the embedded SHA-1 function, or $1 / 2^{80}$, which is less than 1/1,000,000. It takes more than one second to FTP/SFTP a new configuration file to the modem. The probability of successfully authenticating to the module within a one minute period is also $60 / 2^{80}$ (which is < 1/100,000) due to a maximum of 60 attempts per minute.

6. Access Control Policy

Roles and Services

Table 5: Services Authorized for Roles

Service	Description	Operator	Administrator	Cryptographic Officer	Peer Modem	ViaSat, Inc.	Unauthenticated
Telnet, SSH, SNMPv1, SNMPv3, FTP, or SFTP	Remotely connect to the EBEM using Telnet, SSH, SNMPv1, SNMPv3, FTP or SFTP. These protocols are used to establish access to the module for the Operator and Administrator to perform other services, as described in this table.	X	X				
Circuit Establishment	Set up an encrypted or unencrypted circuit	X	X				
Encryption Establishment and Authentication	Use HMAC (with SMAT) or ECDSA signature verification (with IA PKC) to authenticate the AES encrypted pipeline.				X		
Disconnect Encrypted circuit	Tear down the link (by command or power cycle).	X	X				
Change one's own password	One may change one's own password after authentication with the module	X	X	X			
Set Admin, Operator User Names & Passwords	Set Administrator and Operator's User Names & Passwords		X	X			
Change Admin and Operator Passwords	Change Administrator and Operator Passwords		X	X			
Enable/disable encryption	Configure module exclusive bypass settings			X			
Set CO User Names & Passwords	Set CO's User Names & Passwords			X			
Change CO Passwords	Change CO Passwords			X			
SMAT Entry	SMAT Entry via front panel			X			

Service	Description	Operator	Administrator	Cryptographic Officer	Peer Modem	ViaSat, Inc.	Unauthenticated
Set Crypto Compatibility Mode	Set encryption compatibility mode.			X			
Encryption	Perform encryption on an established encrypted circuit with a peer modem.				X		
Cryptographically Validate image	Cryptographically validate and load an uploaded firmware image, feature file, or ESEM configuration file.					X	
Zeroize (authenticated)	Actively overwrite all CSPs. Then the module must be powered down.	X	X	X			
Configure System Time	Adjust the module's system time.			X			
Configure Access to Unsecure Protocols	Enable/disable remote access via FTP, SNMPv1, and Telnet.			X			
Configure password policy	Set minimum password length/complexity requirement and password expiration period.			X			
Change configuration or monitor modem	Adjust all modem and ESEM parameters. Monitor status of all modem parameters.	X	X				
View or clear audit log	View or clear audit log, which logs actions of all users and the associated access method.		X				
Upload Image	Upload a firmware image, a feature file, or ESEM configuration file. This will later be validated by the ViaSat, Inc. role.		X				
Issue Trust Anchor	Issue a Trust Anchor certificate to the modem.		X				
Fill Issued Trust Anchor	Fill a Trust Anchor certificate that has been previously issued into the modem.			X			
Delete Trust Anchor	Delete a filled Trust Anchor Certificate			X			

Service	Description	Operator	Administrator	Cryptographic Officer	Peer Modem	ViaSat, Inc.	Unauthenticated
Issue/Fill Simplex PKI Key Material	Issue/Fill key material needed for authentication and key establishment for PKI circuits (except Trust Anchor). This includes: Certificate Authority certificates, CRLs, IA /KE certificates, and IA/KE private keys.		X				
Delete Simplex PKI Key Material	Delete PKI circuit key material including: Certificate Authority certificates, CRLs, IA /KE certificates, and IA/KE private keys.		X	X			
User Login	Login to the modem configuration interfaces (i.e. SSH, Telnet, (S)FTP, Front Panel, and SNMP)						X
Power On	Power on the modem						X
Power Off	Power off the modem						X
Reset	Reset the modem						X
Display Status	Show non-security relevant status of the cryptographic module via the front panel.						X
Zeroize (unauthenticated)	Actively overwrite all Critical Security Parameters (CSPs) through SNMPv1, or the front panel. Then the module must be powered down.						X
Self-Tests	Perform a suite of Power On Self Tests (POSTs). All POSTs are initiated automatically without operator intervention						X
Antenna Handover Service	Command sent from ship to modem to switch antennas						X
Local/Remote	Switch to Local (which only allows commands through the Front Panel) or switch to Remote (which allows access via remote protocols like SSH).						X

Service	Description	Operator	Administrator	Cryptographic Officer	Peer Modem	ViaSat, Inc.	Unauthenticated
Alarm Mute	Mute the audible alarm.						X

Note: Operator and Administrator roles are permitted access to the module via the front panel as well as remote interfaces (Telnet, SSH, FTP, SFTP, SNMPv1, and SNMPv3). Cryptographic Officers are only permitted access to the module via the front panel.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- SMAT (HMAC Key): Used to authenticate the peer modem role (within a given community of modems) during the initial key agreement messages related to secure circuit establishment. This key is used during re-key operations to authenticate a peer modem. The HMAC algorithm in the EBEM modem uses the SMAT as input, so only EBEM modems configured with the same SMAT will correctly authenticate each other. Authentication of peer modem using this parameter takes place while the modems are performing ECC CDH in key agreement, and the authentication is a 160-bit or 256-bit value depending on the crypto compatibility mode.
- DRBG Seed: 384 bytes (3072 bits) of random data generated from an entropy source (non-deterministic) used to initialize the Deterministic Random Bit Generator (per NIST SP 800-90A).
- DRBG Internal State: The internal state of the NIST SP 800-90A CTR DRBG. These are values "V" and "Key".
- SMAT Circuit TxTEK (Transmit Traffic Encryption Key): A 256-bit AES CTR mode traffic encryption key. This key is used to protect data sent over SMAT-authenticated RF circuits from modems to peer modems.
- SMAT Circuit RxTEK (Receive Traffic Encryption Key): A 256-bit AES CTR mode traffic decryption key. This key is used to decrypt protected data sent over SMAT-authenticated RF circuits from peer modems. This key is an exact match of a peer modem's TxTEK for symmetric AES cryptographic communication.
- PKI Circuit TxTEK (Transmit Traffic Encryption Key): A 256-bit AES CTR mode traffic encryption key. This key is used to protect data sent over PKI-authenticated RF circuits from modems to peer modems.
- PKI Circuit RxTEK (Receive Traffic Encryption Key): A 256-bit AES CTR mode traffic decryption key. This key is used to decrypt protected data sent over PKI-authenticated RF circuits from peer modems. This key is an exact match of a peer modem's TxTEK for symmetric AES cryptographic communication.
- PKI Circuit KEK: A 256-bit AES key used to encrypt the TxTEK for PKI-authenticated circuits before it is output in the Key Transport message.

- Static IA Private Key: Used to digitally sign the Ephemeral KE public key sent in Key Transport messages for PKI-authenticated circuit establishment.
- Ephemeral KE Private Key: Used to derive the PKI Circuit KEK to encrypt the TEK sent in Key Transport messages for PKI-authenticated circuit establishment.
- Static KE Private Key: Used to derive the PKI Circuit KEK used to decrypt the TEK received in Key Transport messages for PKI-authenticated circuit establishment.
- SMAT Circuit Ephemeral Private Key: Module's private key used for SMAT-based circuit establishment with peer modem, per NIST SP800-56A C (2e, 0s, ECC CDH).
- Key Fill Ephemeral Private Key: Private key used for Key Fill KEK establishment with LCT, per NIST SP800-56A C (2e, 0s, ECC CDH).
- Key Fill KEK: A 256-bit AES key used to encrypt private keys filled into the modem.
- ECC CDH Primitive Shared Secret: FIPS SP800-56A C(2e, 0s, ECC CDH) and C(1e, 1s, ECC CDH), key agreement schemes and used with the Concatenation KDF to establish key material for SMAT/PKI authenticated circuits and private key fill.
- Bypass Flag: Determines if a circuit is processed as plaintext or 'encryption enabled.'
- Crypto Compatibility Mode: When enabled, uses SHA-1 instead of SHA-512 for the HMAC and the KDF for backward compatibility with modules that did not have SHA-512 implemented. This is part of our transition plan to eventually eliminate SHA-1 support while maintaining backward compatibility with older SW/FW versions.
- CO Password: 8-character minimum, 20-character maximum, chosen from upper and lowercase letters, 10 digits, and 10 special characters; used to authenticate CO and will lockout after 3 to 5 (configurable by CO) failed attempts.
- Administrator Password(s): 8-character minimum, 20-character maximum, chosen from upper and lowercase letters, 10 digits, and 10 special characters; used to authenticate the Administrator and will lockout after 3 to 5 (configurable by CO) failed attempts.
- Operator Password(s): 8-character minimum, 20-character maximum, chosen from upper and lowercase letters, 10 digits, and 10 special characters; used to authenticate the Operator and will lockout after 3 to 5 (configurable by CO) failed attempts.
- Local Unique Key (LUK): A 256-bit AES key used to encrypt CSPs so they can be stored on the RAM or flash file system.

Definition of Public Keys:

The following are the public keys contained in the module.

- Firmware/Feature Trust Anchor – FIPS 186-4 ECDSA Public Key: Used to validate the authenticity of signed code images and/or feature files
- ESEM Configuration File Trust Anchor – FIPS 186-2 ECDSA Public Key: Used to validate the authenticity of ESEM configuration files
- SMAT Circuit Ephemeral Public Key: Module's public key used for SMAT-authenticated circuit establishment with peer modem, per NIST SP800-56A C (2e, 1s, ECC CDH).
- SMAT Circuit Remote Modem's Ephemeral Public Key: Peer Modem's public key used for circuit establishment, per NIST SP800-56A C (2e, 1s, ECC CDH).
- PKI Circuit Trust Anchor – ECDSA Public Key: Used to validate ECDSA signatures of

CA, IA and KE public key certificates for PKI-authenticated circuits.

- PKI CA Public Key – Certificate Authority public key used to validate ECDSA signatures of IA and KE public key certificates for PKI-authenticated circuits.
- Static IA Public Key: Used to digitally sign (per FIPS 186-4 ECDSA) and validate the signature the KE Public Key sent in Simplex Key Agreement messages for PKI-authenticated circuit establishment.
- Ephemeral KE Public Key: Used to derive the PKI Circuit KEK used to encrypt/decrypt the AES-wrapped TEK for PKI-authenticated circuits, per NIST SP 800-56A C (1e, 1s, ECC CDH).
- Receiver Static KE Public Key: Used to derive the PKI Circuit KEK used to encrypt/decrypt the AES-wrapped TEK for PKI-authenticated circuits, (per FIPS 186-4 ECDSA). Received over the air.
- Remote IA Public Key: Used to validate authenticity (digital signature) of received Key Transport messages for PKI-authenticated circuit establishment, (per FIPS 186-4 ECDSA). Received over the air.
- Remote Ephemeral KE Public Key: Used to derive the PKI Circuit KEK used to decrypt the AES-wrapped TEK received in Key Transport messages for PKI-authenticated circuit establishment, per NIST SP 800-56A C (1e, 1s, ECC CDH).
- Key Fill Ephemeral Public Key: Ephemeral public key generated and used when inputting a static private key into the modem (per NIST SP 800-56A C (2e, 0s, ECC CDH).
- LCT Key Fill Remote Ephemeral Public Key: Ephemeral public key received from the LCT and used when inputting a static private key into the modem (per NIST SP 800-56A C (2e, 0s, ECC CDH). Received over an authenticated connection from the LCT.

Definition of CSPs and Public Key Modes of Access

Table 6 defines the relationship between CSPs and only those module services that access CSPs. The modes of access shown in the Table 6 are defined as follows.

- Input (I): the data item is entered into the cryptographic module
- Output (O): the data item is output (Note: CSPs that are output are encrypted).
- Store (S): the data item is set into the persistent storage
- Use (U): the data item is used within its corresponding security function
- Establish (E): the data item is established via a commercially available key establishment technique
- Generate (G): the data item is generated
- Zeroize (Z): the data item is actively overwritten

Table 6: CSP Access Rights within Services

Service	SMAT (HMAC Key)	DRBG Seed and DRBG Internal State	SMAT Circuit TxTEK	SMAT Circuit RxTEK	PKI Circuit TxTEK	PKI Circuit RxTEK	PKI Circuit KEK	Static IA Private Key	Ephemeral KE Private Key	Static KE Private Key	SMAT Circuit Ephemeral Private Key	Key Fill Ephemeral Private Key	Key Fill KEK	ECC CDH Primitive Shared Secret	Bypass Flag	Crypto Compatibility Mode	CO Password	Administrator Password	Operator Password	Local Unique Key
Telnet, SSH, SNMPv1, SNMPv3, FTP, or SFTP																		I,U	I,U	
Circuit Establishment															U			I, U	I, U	
Encryption Establishment and Authentication	U	G, U	E	E	G, O	I	E, U	U	G, U	U	G, U			E, U	U	U		I, U	I, U	
Disconnect Encrypted circuit																		I, U	I, U	
Change one's own password																	I,U, S	I,U, S	I,U, S	U
Set Admin, Operator User Names & Passwords																		I, S	I, S	U
Change Admin and Operator Passwords																		I, S	I, S	U
Enable/disable encryption															I,S		I, U			
Set CO User Names & Passwords																	I, S			U
Change CO Passwords																	I, S			U
SMAT Entry	I, S																I, S			U
Set Crypto Compatibility Mode																I, S	I, U			
Encryption			U	U	U	U														
Cryptographically Validate image																				
Zeroize (Authenticated)	Z	Z	Z	Z	Z			Z		Z					Z	Z	Z	Z	Z	Z
Configure System Time																	I,U			

Service	CSPs																			
	SMAT (HMAC Key)	DRBG Seed and DRBG Internal State	SMAT Circuit TxTEK	SMAT Circuit RxTEK	PKI Circuit TxTEK	PKI Circuit RxTEK	PKI Circuit KEK	Static IA Private Key	Ephemeral KE Private Key	Static KE Private Key	SMAT Circuit Ephemeral Private Key	Key Fill Ephemeral Private Key	Key Fill KEK	ECC CDH Primitive Shared Secret	Bypass Flag	Crypto Compatibility Mode	CO Password	Administrator Password	Operator Password	Local Unique Key
Configure Access to Unsecure Protocols																	I,U			
Configure password policy																	I,U			
Change configuration or monitor modem																		I,U	I,U	
View or clear audit log																		I,U		
Upload Image																		I,U		
Issue Trust Anchor																		I,U		
Fill Issued Trust Anchor																	I,U			
Delete Trust Anchor																		I,U		
Issue/Fill Simplex PKI Key Material		G,U						I,U,S		I,U,S		G,U	E,U	E,U				I,U		U
Delete Simplex PKI Key Material																		I,U		
User Login																	I,U	I,U	I,U	U
Power On		G,U																		G,S
Power Off		Z	Z	Z	Z	Z	Z		Z		Z	Z	Z	Z						
Reset																				
Front Panel Display status															O	O				
Zeroize (Unauthenticated)	Z		Z	Z	Z	Z		Z		Z					Z	Z	Z	Z	Z	Z
Self-tests		G,U												G						
Antenna Handover Service																				
Local/Remote																				
Alarm Mute																				

Table 7: Public Key Access Rights within Services

Service	Public Keys											
	Firmware/ Feature Trust Anchor	ESEM Configuration File Trust Anchor	SMAT Circuit Ephemeral Public Key	SMAT Circuit Remote Modem's Ephemeral Public Key	PKI Circuit Trust Anchor	PKI CA Public Key	Static IA Public Key	Ephemeral KE Public Key	Receiver Static KE Public Keys	Remote IA Public Key	Key Fill Ephemeral Public Key	LCT Key Fill Remote Ephemeral KE Public Key
Telnet, SSH, SNMPv1, SNMPv3, FTP, or SFTP												
Circuit Establishment												
Encryption Establishment and Authentication			G, U, O	I,U	U	U	U, O	G,U, O	U	I,U		
Disconnect Encrypted circuit												
Change one's own password												
Set Admin, Operator User Names & Passwords												
Change Admin and Operator Passwords												
Enable/disable encryption												
Set CO User Names & Passwords												
Change CO Passwords												
SMAT Entry												
Set Crypto Compatibility Mode												
Encryption												
Cryptographically Validate image	I,S	I,S										
Zeroize (Authenticated)												

Service	Public Keys											
	Firmware/ Feature Trust Anchor	ESEM Configuration File Trust Anchor	SMAT Circuit Ephemeral Public Key	SMAT Circuit Remote Modem's Ephemeral Public Key	PKI Circuit Trust Anchor	PKI CA Public Key	Static IA Public Key	Ephemeral KE Public Key	Receiver Static KE Public Keys	Remote IA Public Key	Key Fill Ephemeral Public Key	LCT Key Fill Remote Ephemeral KE Public Key
Configure System Time												
Configure Access to Unsecure Protocols												
Configure password policy												
Change configuration or monitor modem		U										
View or clear audit log												
Upload Image	U											
Issue Trust Anchor					I							
Fill Issued Trust Anchor					I,S							
Delete Trust Anchor												
Issue/Fill Simplex PKI Key Material						I, S	I,S		I,S		G,U, O	I,U
Delete Simplex PKI Key Material												
User login												
Power On												
Power Off			Z	Z				Z		Z	Z	Z
Reset												
Front Panel Display status												
Zeroize (Unauthenticated)												
Self-tests												
Antenna Handover Service												
Local/Remote												
Alarm Mute												

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the EBEM device contains a limited operational environment; the cryptographic module only supports the loading and execution of code ECDSA digitally authenticated firmware signed by ViaSat, Inc.

8. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of FIPS 140-2, Level 2.

- The cryptographic module shall support defined roles with a defined set of corresponding services. The defined roles shall be:
    o Operator
    o Administrator
    o Cryptographic-Officer
    o Peer Modem
    o ViaSat, Inc.
- Separation of roles: The cryptographic module shall require distinct authentication for each role. Simultaneous service is permitted, but authentication is always required when switching between roles
- The cryptographic module shall not support a maintenance role or maintenance interface.
- The purpose, function, service inputs, and service outputs performed by each role shall be defined and appropriately restricted.
- The cryptographic module shall not support the output of plaintext CSPs.
- The cryptographic module design shall ensure that services that do not require authentication do not provide the ability to modify, disclose, or substitute any module CSPs, use Approved security functions, or otherwise affect module security.
- The cryptographic module shall support exclusive bypass capabilities. The cryptographic module shall require two independent internal actions to enter into the bypass state. The authorized operator shall be able to determine when bypass capability is selected as follows: Bypass LED illuminated
- A defined methodology shall be enforced to control access to the cryptographic module prior to initialization. The module shall arrive to the end customer with a default Cryptographic Officer password that shall be changed before any services are allowed.
- Re-authentication shall be required upon power cycling the module.
- The cryptographic module shall support role-based or identity-based authentication for all security relevant services; re-authentication shall be required to change roles.
- Feedback provided during the authentication process shall not weaken the strength of the implemented authentication mechanisms. During password entry, the module shall not display the entered values in a readable form; all inputs will be echoed back to the display as asterisks.
- The cryptographic module's finite state machine shall provide a clear description of all states and corresponding state transitions. The design of the cryptographic module shall disallow the ability to simultaneously occupy more than one state at a time.

- The cryptographic module's physically contiguous cryptographic boundary shall be defined including all module components and connections (ports), information flows, processing, and input/output data. All vendor-defined non-security relevant circuitry shall be argued for exclusion from the cryptographic boundary.
- All cryptographic module data output shall be inhibited when the module is in an error state any during self-tests.
- Data output shall be logically disconnected from the processes performing key generation, manual key entry, and zeroization.
- All physical ports and logical interfaces shall be defined; the cryptographic module shall be able to distinguish between data and control for input and data and status for output. In addition, the cryptographic module shall support a power interface.
- All of the implemented integrated circuits shall be standard quality, production-grade components.
- The cryptographic module shall contain an opaque tamper evident enclosure.
- CSPs shall be protected against unauthorized disclosure, modification, and substitution. Public keys and critical settings shall be protected against unauthorized modification and substitution.
- The cryptographic module shall support key generation using an Approved RNG listed in FIPS PUB 140-2 Annex C.
- The cryptographic module shall enforce an entity association for all keys that are input to/output from the cryptographic module; an entity association shall be enforced for all keys stored within the cryptographic boundary.
- Key establishment techniques supported by the cryptographic module shall be commercially available as allowed under the requirements of FIPS PUB 140-2 Annex D.
- The cryptographic module shall provide the ability to zeroize all plaintext CSPs. Note: To fully complete the Zeroize Service, the unit must be manually power-cycled.
- Power-up self-tests shall not require operator actions. The cryptographic module shall provide an indicator upon successful self-test completion as follows:
    - Fault LED off
- The cryptographic module shall enter an error state upon failure of any self-test and shall provide an indicator upon failure as follows:
    - Fault LED on
- Upon entering an error state, the cryptographic module shall inhibit all data outputs, inhibit cryptographic operations, and shall provide error status. The status output shall not contain any CSPs or other sensitive information that could be used to compromise the cryptographic module.
- The loading of non-FIPS-validated firmware versions will invalidate the FIPS module.
- The tamper evident seals described in Section 10 shall be installed for the module to operate in a FIPS Approved mode of operation.
- The module has the following restrictions on concurrent operators:
    - While a Crypto Officer, Administrator, or Operator is logged into the Front Panel, SSH, SNMPv1, SNMPv3, FTP, and SFTP protocols users cannot configure EBEM modem.
    - While the Peer Modem is authenticated, the Crypto Officer cannot change the Crypto Compatibility Mode.

9. Self-Tests

The cryptographic module shall support the following self-tests:

Table 8: Power Up Self-tests

Test Target	Description
Firmware Integrity	32-bit EDC performed over all executable code
FPGA AES Encrypt	KATs: EBEM AES CTR 1 Encryption only (because CTR mode utilizes ECB encrypt for both encryption and decryption) Modes: ECB Key sizes: 256 bits
FPGA AES Decrypt	KATs: EBEM AES CTR 2 Encryption only (because CTR mode utilizes ECB encrypt for both encryption and decryption) Modes: ECB Key sizes: 256 bits
AES	KATs: EbemCrypto, separate encryption and decryption tests Modes: ECB Key sizes: 256 bits
AES Key Wrap	KATs: Separate wrap and unwrap tests. Key sizes: 256 bits
DRBG	KATs: CTR DRBG Security Strengths: 256 bits
ECDSA	KAT: FIPS 186-2 Signature Verification Curves/Key sizes: P-521 with SHA-1
ECDSA	KAT: FIPS 186-4 Signature Verification Curves/Key sizes: P-521 with SHA-512
ECDSA	PCT: FIPS 186-4 Signature Generation, Signature Verification Curves/Key sizes: P-384 with SHA-384
HMAC	KATs: Generation, Verification SHA sizes: SHA-1, SHA-384, SHA-512
KAS	KATs: Ephemeral Unified, per IG 9.6 – ECCCDH Primitive Computation and KDF using P-521 curve. Parameter Sets/Key sizes: EE
KAS	KATs: One Pass DH, per IG 9.6 – ECCCDH Primitive Computation and KDF using P-384 curve. Parameter Sets/Key sizes: ED
KDF	KATs: SNMP KDF
KDF	KATs: SSH KDF
SHA	KATs: EbemCrypto SHA-1, SHA-384, SHA-512
SHA	KATs: OpenSSL SHA SHA-1, SHA-256, SHA-512
SHA	KATs: SHA-256 uClibc SHA-256

Table 9: Conditional Self-tests

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation (static and ephemeral per IG 9.9).
Firmware Load	FIPS 186-4 ECDSA P-521 with SHA-512 signature verification performed when firmware is loaded.
DRBG Health Checks	Performed conditionally per SP 800-90A Section 11.3. Required per IG C.1.
SP 800-56A Assurances	Pairwise key validation (per IG 9.6)
Exclusive Bypass Test	Bypass Test verifies which mode (Bypass or Encryption) the module is in by checking a flag value, which is stored in FLASH and whose integrity is verified by a 32-bit EDC (CRC).
Manual Key Entry	Manual Key Entry Test performed via Error Detection Code

Table 10: Critical Function Tests

Test Target	Description
BIT	Verification of FPGA loading

10. Physical Security Policy

Physical Security Mechanisms
The EBEM multi-chip standalone cryptographic module includes the following physical security mechanisms.

- Production-grade components
- Production-grade opaque enclosure with 10 (ten) tamper evident seals applied during manufacturing if the Expansion Port on the module has the Blank Plate installed
- Production-grade opaque enclosure with nine (9) tamper-evident seals if the EBEM contains an ESEM card (eight (8) seals applied during manufacturing and one (1) rectangular tamper-evident seal applied by the Crypto-Officer
- Protected vents

Operator Required Actions

The CO is required to periodically inspect the tamper evident seals, enclosure, and vents as shown in Table 11. If suspicious markings are found, the cryptographic module should be zeroized and returned to the manufacturer (contact ViaSat, Inc. at www.viasat.com) for inspection/maintenance.

Table 11: Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	As specified per end user policy	Visually inspect the seals for tears, rips, dissolved adhesive, and other signs of malice.
Opaque enclosure	As specified per end user policy	Visually inspect the enclosure for broken screws, bent casing, scratches, and other questionable markings.
Protected vents	As specified per end user policy	Visually inspect the vents for tears, bent baffles, and other signs of tampering.

The following diagrams depict the tamper seal locations (circled in blue):
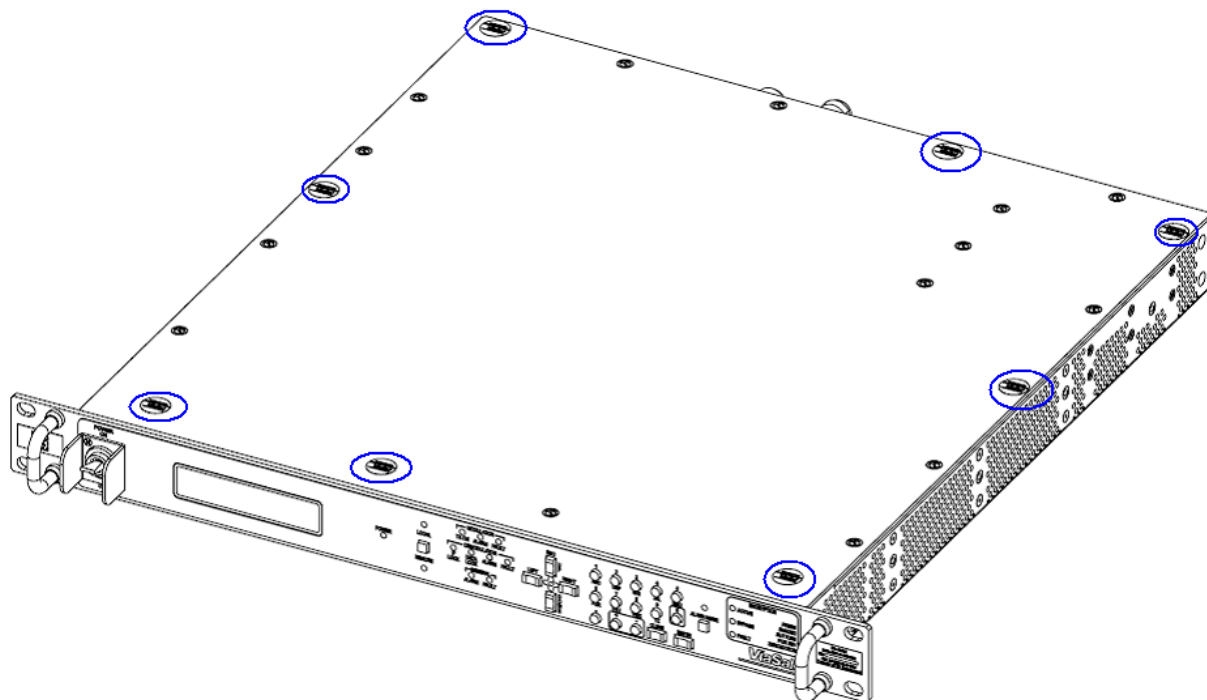
Figure 3: Tamper Seal locations on the Strategic EBEM (8 Seals)
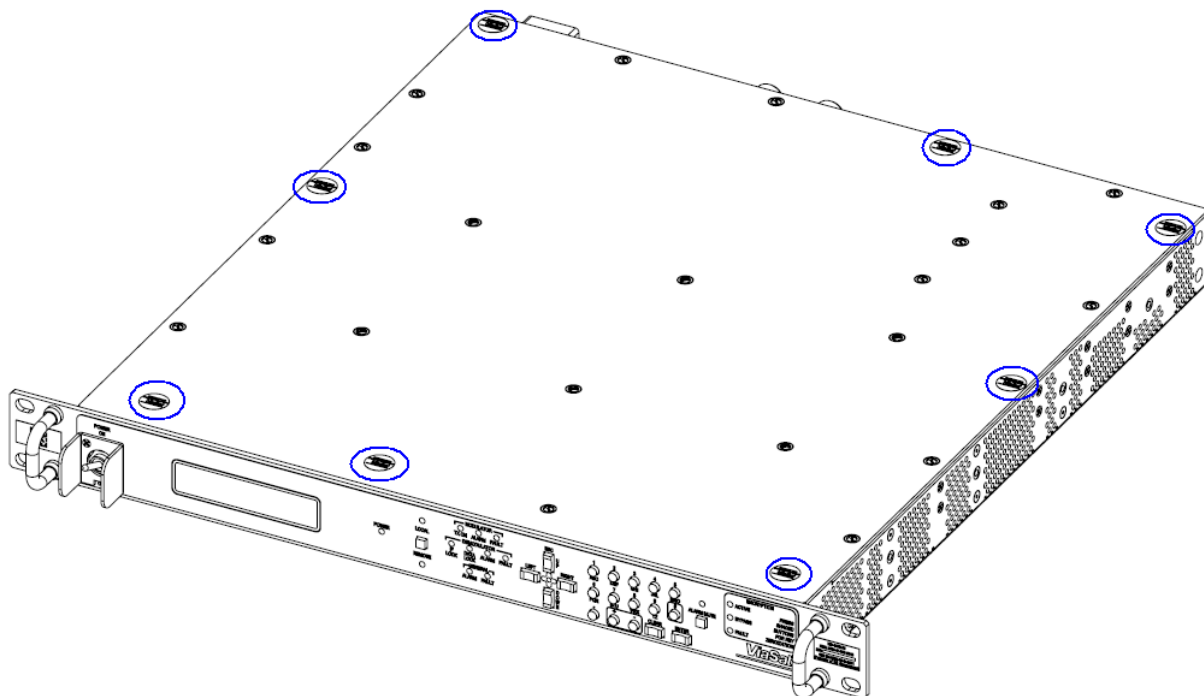
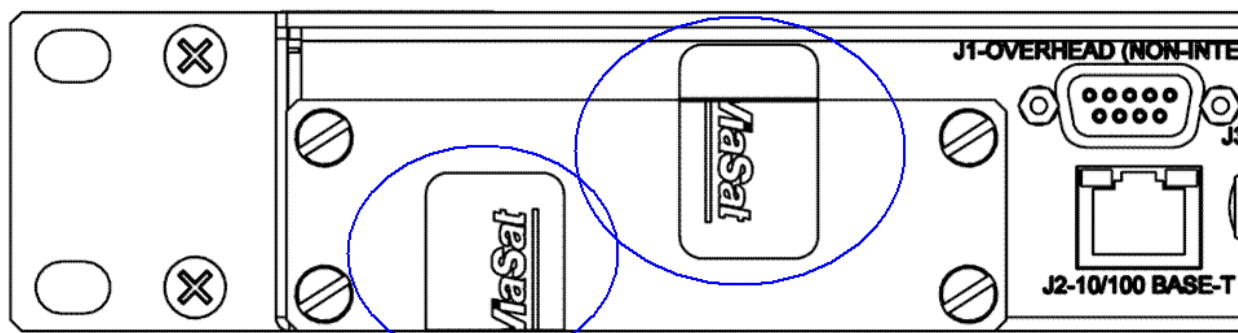**Figure 4: Tamper Seal locations on the Tactical EBEM (8 Seals)**

Figure 5: Tamper Seal Location of Expansion Port with Blank Plate Installed (2 Seals)
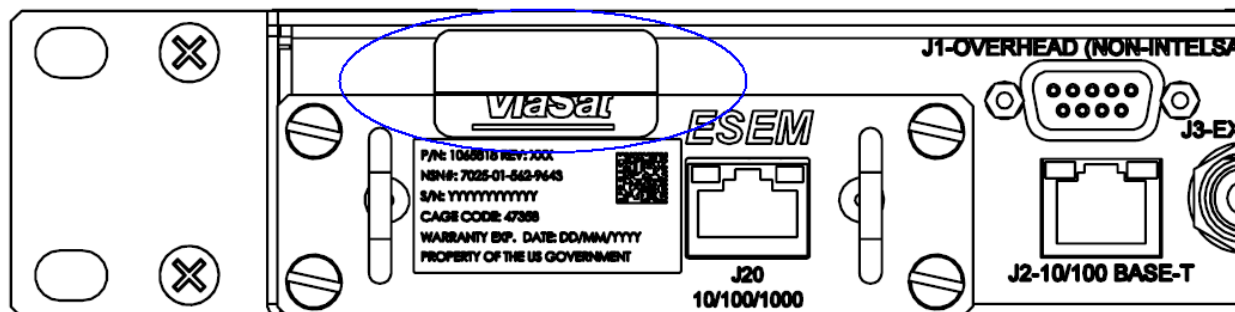

Figure 6: Tamper Seal Location on Expansion Port with ESEM Installed (1 Seal)

All tamper seals are installed at the factory except the one shown in Figure 5 for the ESEM. In the case of an EBEM that contains an ESEM (i.e., as in Figure 5), the one (1) tamper seal must be installed by the CO. Prior to installation, the CO is responsible for securing and having control at all times of any unused seals. Detailed instructions for the ESEM and tamper seal installation are provided in ViaSat, Inc.'s *EBEM Crypto Officer & User Guide and Software/Firmware Installation Guide*, ViaSat document number 1153093, Section 11.

The tamper evident seals shall be installed for the module to operate in a FIPS Approved mode of operation.

Note: The tamper seal applied over the ESEM is HW P/N 1047117; however, the CO cannot order additional tamper seals from ViaSat, Inc. If the device is found to be tampered, the unit should be returned to the factory for a repair inspection.

11. Mitigation of Other Attacks Policy

The module has not been designed to mitigate specific attacks outside of the scope of FIPS 140-2.

12. References

- FIPS PUB 140-2
- FIPS PUB 180-1
- FIPS PUB 180-2
- FIPS PUB 186-4
- FIPS PUB 198
- FIPS PUB 46-3
- FIPS PUB 186-2
- FIPS SP800-56A
- FIPS SP 800-90A
- FIPS SP 800-132
- FIPS SP 800-38F

13. Definitions and Acronyms

Acronym	DEFINITION
AES	Advanced Encryption Standard
BIT	Built-in Test
CAVS	Cryptographic Algorithm Validation System
CO	Cryptographic Officer
CSP	Critical Security Parameter (as defined per FIPS 140-2)
CTR	Counter (i.e. AES Counter mode)
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EBEM	Enhanced Bandwidth Efficient Modem
ECB	Electronic Code Book
ECC CDH	Elliptic Curve Cryptography Co-factor Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESEM	Ethernet Service Expansion Module
FIFO	First-in, First-out (data buffer)
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
FW	Firewall
HMAC	Hash Message Authentication Code
IA	Identity and Authentication
KAT	Known Answer Test
KDF	Key Derivation Function
KW	Key Wrap (AES Key Wrap without Padding from SP 80038-F)
LCT	Local Control Terminal
LED	Loop Encryption Device
Mbps	Million Bits per Second
Modem	Modulator/Demodulator

NIST	National Institute of Standards and Technology
PBKDF	Password Based Key Derivation Function
PKI	Public Key Infrastructure
RNG	Random Number Generator
RX	Receiver
SCPC	Single Channel Per Carrier
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SMAT	Shared Message Authentication Token
SNMP	Simple Network Management Protocol
TX	Transmit