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

Document Number 1179470, Rev. 012
October 29, 2018

Prepared by:

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
1179470	007	Updated for Remote Administrator and ESEM Services and PPPoE Enhancements ECP	March 25, 2016	All
1179470	008	Updated in response to CMVP Comments	June 22, 2016	3 - 5
1179470	009	Updated in response to CMVP Comments	June 26, 2016	1, 6
1179470	010	Updated for FW v02.09.06	January 3, 2017	4
1179470	011	Updated for FW v02.11.06 IA Enhancements	June 26, 2018	All
1179470	012	Updated in response to CMVP Comments	October 29, 2018	All

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	02.11.06
	P/N 1010162 with ESEM Version 1 (also referred to as P/N 1091549)	02.11.06
	P/N 1075559 Version 1	02.11.06
	P/N 1075559 with ESEM Version 1 (also referred to as P/N 1091551)	02.11.06
	P/N 1047117: Tamper seal applied over the ESEM	N/A
Tactical	P/N 1010163 Version 1	02.11.06
	P/N 1010163 with ESEM Version 1 (also referred to as P/N 1091550)	02.11.06
	P/N 1075560 Version 1	02.11.06
	P/N 1075560 with ESEM Version 1 (also referred to as P/N 1091552)	02.11.06
	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

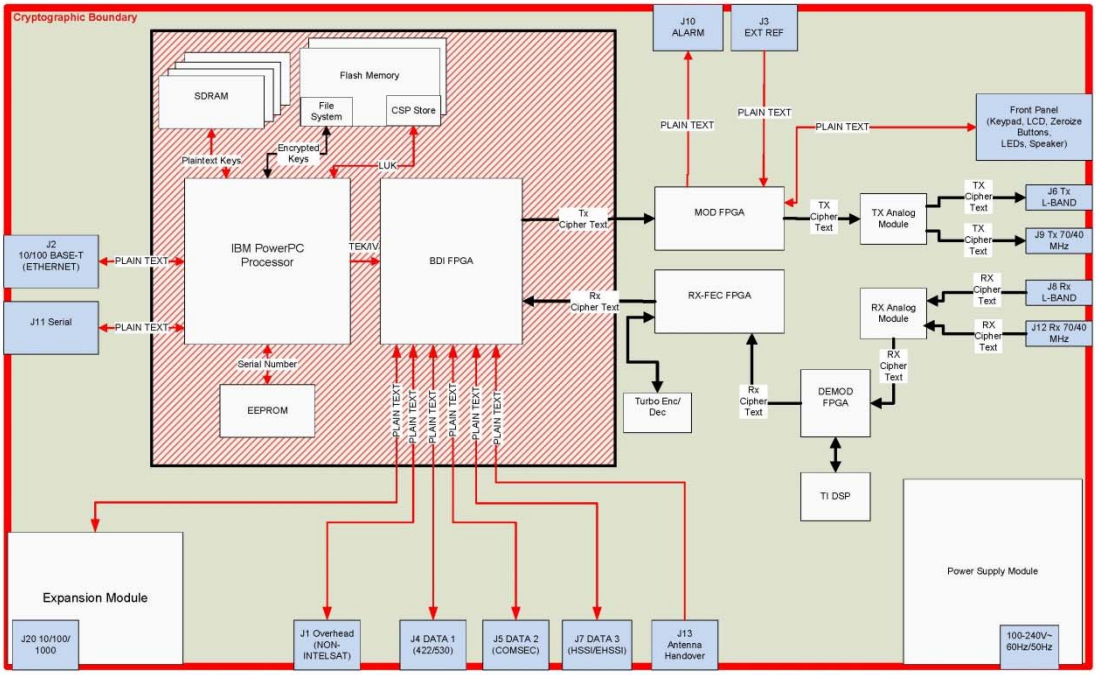

Figure 2: Block Diagram

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

Algorithm Implementation	Algorithm	Description	CAVP 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, KW Key sizes: 256 bits	5475
	CKG	[SP 800-133] Asymmetric Key Generation (§ 6) and Symmetric Key Generation (§ 7) without further post processing (i.e., unmodified output from the DRBG).	Vendor Affirmed
	DRBG	[SP 800-90A] Functions: CTR DRBG Security Strengths: 256 bits	2154
	ECDSA	[FIPS 186-4] Functions: Signature Verification (for firmware images, and feature files) Curves/SHA sizes: P-521 with SHA-512	1466

Algorithm Implementation	**Algorithm**	**Description**	**CAVP Cert. #**
	ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification (for key transport messages) Curves/SHA sizes: P-384 with SHA-384	1466
	KTS	[SP 800-38F] Functions: Wrap, Unwrap (for CSPs) Key sizes: 256 bits Caveat: Key establishment methodology provides 192 bits of encryption strength.	5475
	HMAC	[FIPS 198-1] Functions: Generation, Verification (for SMAT and PBKDF2 authentication) SHA sizes: SHA-384, SHA-512	3630
	KAS	[SP 800-56A] Schema: Ephemeral Unified Parameter sets/Key sizes: EE Supports 256 bits of security.	182
	KAS	[SP 800-56A] Schema: One Pass DH Parameter sets/Key sizes: ED Supports 192 bits of security.	182
	SHA	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-384, and SHA-512	4393
NetSNMP* KDF	KDF	[SP 800-135] Functions: SNMP KDF	1930 (CVL)
OpenSSH* Algorithms	KDF	[SP 800-135] Functions: SSH KDF	1929 (CVL)

* No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

Algorithm Implementation	**Algorithm**	**Description**	**CAVP Cert. #**
	KAS	[SP 800-56A] Schema: Ephemeral Unified Parameter sets/Key sizes: EC, ED, EE Supports 128, 192, and 256 bits of security.	1928 (CVL)
OpenSSL Algorithms	AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, CFB, CTR Key sizes: 128, 192, 256 bits	5476
	CKG	[SP 800-133] Asymmetric Key Generation (§ 6) without further post processing (i.e., unmodified output from the DRBG).	Vendor Affirmed
	ECDSA	[FIPS 186-4] Functions: Asymmetric Key Generation, Signature Generation, Signature Verification Curves: P-256, P-384, and P-521 SHA sizes: SHA-256, SHA-384, and SHA-512	1467
	HMAC	[FIPS 198] Functions: Keyed Hash SHA sizes: SHA1, SHA-256, SHA-512	3631
	SHA	[FIPS 180-4] Functions: Message Digests SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512	4394
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 (1024 bit) blocks and 384 bytes (3072 bits) are generated to seed the Approved DRBG. At 0.174 bits of min-

entropy per bit, the module's DRBG seed contains 3072 * 0.174 > 534 bits of entropy which exceeds the required 384 bits (256 bits of entropy input plus 128 bits of nonce).

- SSH – Uses the following algorithms:
  - Protocol Defined Algorithm Names:
    - Ciphers: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, aes256-cbc
    - Key Exchange Algorithms: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
    - Public Key Algorithms: Ecdsa-sha2-nistp256, Ecdsa-sha2-nistp384, Ecdsa-sha2-nistp521
    - MACs: hmac-sha1, hmac-sha2-256, hmac-sha2-512
  - Corresponding FIPS Algorithms:
    - Ciphers: AES (Cert. # 5476)
    - Key Exchange Algorithms: EC Diffie-Hellman KAS (CVL Certs. #1928 and #1929 with curves P-256, P-384 and P-521; provides 128, 192, or 256 bits of strength), SHA (Cert. # 4394)
    - Public Key Algorithms: ECDSA (Cert. # 1467), SHA (Cert. # 4394)
    - MACs: HMAC (Cert. # 3631), SHA (Cert. # 4394)
- SFTP – Uses the following algorithms:
  - Same as SSH above.
- Telnet –Uses no algorithms.
- SNMPv1 –Uses no algorithms.
- FTP – Uses no algorithms.
- SNMPv3 – Uses the following algorithms:
  - Protocol Defined Algorithm Names: HMAC-SHA, AES
  - Corresponding FIPS Algorithms: HMAC (Cert. # 3631), SHA (Cert. # 4394), AES (Cert. # 5476)

In FIPS mode, the cryptographic module supports the following no security claimed algorithm:

- SP 800-132 PBKDF2 – no security is claimed. Anything imported into the module encrypted using PBKDF2 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 PBKDF2 keys. Corresponding FIPS Algorithm: PBKDF2 (no security claimed).

The EBEM cryptographic module does not contain a non-Approved mode of operation. The FIPS Approved mode of operation is indicated by the banner. When an Operator or Administrator connects to the module using Telnet, SSH, FTP, or SFTP, the banner indicates that the module is in FIPS Approved mode ("Module is in FIPS Approved Mode"). Additionally, if the firmware 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".

Detailed instructions for module installation, initialization, and start-up are provided in Viasat, Inc.'s *EBEM Crypto Officer & User Guide and Software/Firmware Installation Guide*, Viasat document number 1153093.

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, 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 "Crypto Officer" from	Identity-based	User name and Password

Role	Description	Type of Authentication	Authentication Data
	the FIPS 140-2 perspective.		
Peer Modem	The modem at the other end of the RF link, with whom the TEK negotiation occurs.	Role-based Identity-based	HMAC Key, also referred to as SMAT (Shared Modem Authentication Token) 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

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. An administrator is able to configure the modem to allow an unlimited number of login attempts for a given user. One bottleneck that limits the number of login attempts is the 10/100 Ethernet network interface of the module. Ignoring any other limiting factors, this bottleneck can be used to examine the probability of a successful authentication. See the table below for information regarding each authentication method (besides the front panel which is far too slow to be considered), the number of bytes the modem sends over the network to the client during an authentication attempt, and the maximum probability of a successful authentication given that info. Each probability is less than 1/100,000.

Authentication Method	Authentication Attempt Size (Bytes)	Approx. Probability of Authentication
SSH	194	5.353E-09
Telnet	3977	2.611E-10
FTP	1759	5.904E-10
SNMPv1	96	1.082E-08
SNMPv3	307	3.383E-09

Authentication Mechanism	Strength of Mechanism
HMAC Key	The probability that a random attempt will succeed or a false acceptance will occur is the strength of the embedded SHA-384 function 1 / 2^192 which is less than 1/1,000,000. When the HMAC key is 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 / 2^192 which is less than 1/100,000. When the HMAC key is entered (encrypted) over the SSH M&C interface via the LCT, it 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 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.

6. Access Control Policy

Roles and Services

Table 5: Services Authorized for Roles

Service	Description	Operator	Administrator	Peer Modem	Viasat, Inc.	Unauthenticated
Telnet, SSH, SNMPv1, SNMPv3, FTP, or SFTP Access	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	Configure 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		
Change Own Password	One may change one's own password after authentication with the module	X	X			
Set/Change Administrator, Operator User Names & Passwords	Set Administrator and Operator's User Names & Passwords. Unlock accounts and change role type.		X			
Set/Change SNMPv1 Password	Initialize or change the password for authenticating the SNMPv1 user.		X			
Enable/Disable encryption	Configure module exclusive bypass settings		X			
SMAT Entry and Rollover	SMAT Entry (may initiate SMAT rollover if a circuit is established)		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 or feature file.				X	
Zeroize (authenticated)	Actively overwrite all CSPs. Then the module must be powered down. Note: Zeroize not available from Front Panel menu (only unauthenticated zeroize available)	X	X			

Service	Description	Operator	Administrator	Peer Modem	Viasat, Inc.	Unauthenticated
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/Monitor Modem and ESEM configuration, view statistics	Adjust all modem and ESEM parameters. Monitor status of all modem parameters and statistics.	X	X			
View or clear audit log	View or clear audit log, which logs actions of all users and the associated access method. (Only available over remote connection)		X			
Upload/Install Feature File or Firmware Image	Upload a firmware image or a feature file. This will later be validated by the Viasat, Inc. role. (Only available over a remote connection)		X			
Issue/Fill/Delete Simplex PKI Key Material	Issue/Fill/Delete key material needed for authentication and key establishment for PKI circuits. This includes: Trust Anchor, Certificate Authority certificates, CRLs, IA /KE certificates, and IA/KE private keys.		X			
View Filled PKI Information	View IDs and type of key material that is filled in the modem.	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	X			X
Display Status	Show non-security relevant status of the cryptographic module via the front panel.					X

Service	Description	Operator	Administrator	Peer Modem	Viasat, Inc.	Unauthenticated
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
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).

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 uses the SMAT as input, so only EBEMs 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 512-bit value.
- 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.'
- 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 Administrator) 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 Administrator) 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.
- SSH Ephemeral Private Key: A 256-bit ECDSA ephemeral key (configurable up to 384-bit and 512-bit) used by the SSH protocol to generate shared secret between the server and client.
- SSH Static Private Key: A 256-bit ECDSA static key used by the SSH protocol to authenticate the host server to the client.

- SSH Shared Secret: Derived as the shared secret 'k' value (as specified in RFC4253) during the key agreement phase (as specified in NIST SP 800-56A) of the SSH (SecSH) protocol.
- SSH Exchange Hash: Derived as the exchange hash 'H' value (as specified in RFC4253) during the key agreement phase of the SSH (SecSH) protocol.
- SSH Encryption Key: Derived as the encryption key value (as specified in RFC4253) during the key agreement phase of the SSH (SecSH) protocol. Used by OpenSSL AES CBC and CTR with a key size of 128, 192, or 256 bits.
- SSH Authentication Key: Derived as the authentication key value (as specified in RFC4253) during the key agreement phase of the SSH (SecSH) protocol. Used by OpenSSL HMAC with a size of 160 bits for SHA-1, 256 bits for SHA-256, or 512 bits for SHA-512.
- SNMP Ephemeral Private Authentication Key: 160-bit key generated from a user supplied passphrase per RFC 3414. This key is used in an HMAC to provide user authentication for SNMPv3 messages per RFC 3414.
- SNMP Ephemeral Private Encryption Key: A 160-bit key generated from a user-supplied passphrase per RFC 3414. This key is used to encrypt and decrypt SNMPv3 messages using CFB128-AES-128 per RFC 3826.

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
- 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 or SMAT 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 or SMAT into the modem (per NIST SP 800-56A C (2e, 0s, ECC CDH). Received over an authenticated connection from the LCT.
- SSH Ephemeral Public Key: A 256-bit ECDSA ephemeral key (configurable up to 384-bit and 512-bit) used by the SSH protocol to generate a shared secret between the server and client.
- SSH Static Public Key: A 256-bit ECDSA static key used by the SSH protocol to allow the client to uniquely identify the host server.
- SSH Remote Client Ephemeral Public Key: A 256-bit ECDSA ephemeral key (configurable up to 384-bit and 512-bit) used by the SSH protocol to generate a shared secret between the server and client.

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	CSPs																	
	SMAT (HMAC Key)	**DRBG Seed and DRBG Internal State**	**SMATCircuit 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**	**Administrator Password**	**Operator Password**	**Local Unique Key**
Telnet, SSH, SNMPv1, SNMPv3, FTP, or SFTP Access																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	I, U	I, U	
Change Own Password																I,U,S	I,U,S	U
Set/Change Admin, Operator User Names & Passwords																I, S	I, S	U
Set/Change SNMPv1 Password																	I,S	U
Enable/Disable encryption															I,S	I, U		
SMAT Entry and Rollover	I, S	G, U										G, U	E,U	E, U		I,U		U
Encryption			U	U	U	U												
Cryptographically Validate image																		
Zeroize (Authenticated)	Z		Z	Z	Z	Z		Z		Z					Z	Z	Z	Z
Configure System Time																I,U		
Configure Access to Unsecure Protocols																I,U		
Configure password policy																I,U		
Change/Monitor Modem and ESEM configuration, view statistics																I,U	I,U	
View or clear audit log																I,U		
Upload/Install Feature File or Firmware Image																I,U		
Issue/Fill/Delete Simplex PKI Key Material		G, U						I,U, S		I,U, S		G, U	E,U	E, U		I,U		U
View Filled PKI Information																I,U	I,U	
User Login																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																		
Display status															O			

Service	CSPs																	
	SMAT (HMAC Key)	**DRBG Seed and DRBG Internal State**	**SMATCircuit 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**	**Administrator Password**	**Operator Password**	**Local Unique Key**
Zeroize (Unauthenticated)	Z		Z	Z	Z	Z		Z		Z					Z	Z	Z	Z
Self-tests		G, U												G				
Antenna Handover Service																		
Local/Remote																		
Alarm Mute																		

Service	CSPs							
	SSH Ephemeral Private Key	**SSH Static Private Key**	**SSH Shared Secret**	**SSH Exchange Hash**	**SSH Encryption Key**	**SSH Authentication Key**	**Net-SNMP Ephemeral Private Authentication Key**	**Net-SNMP Ephemeral Private Encryption Key**
Telnet, SNMPv1, or FTP Access								
SSH, SFTP	G, U, Z	G, U, S	E, U, Z	E, U, Z	E, U, Z	E, U, Z		
SNMPv3							G, U	G, U
Circuit Establishment								
Encryption Establishment and Authentication								
Change Own Password								
Set/Change Admin, Operator User Names & Passwords								

Service	CSPs							
	SSH Ephemeral Private Key	**SSH Static Private Key**	**SSH Shared Secret**	**SSH Exchange Hash**	**SSH Encryption Key**	**SSH Authentication Key**	**Net-SNMP Ephemeral Private Authentication Key**	**Net-SNMP Ephemeral Private Encryption Key**
Set/Change SNMPv1 Password								
Enable/Disable encryption								
SMAT Entry and Rollover								
Encryption								
Cryptographically Validate image								
Zeroize (Authenticated)	Z	Z	Z	Z	Z	Z	Z	Z
Configure System Time								
Configure Access to Unsecure Protocols								
Configure password policy								
Change/Monitor Modem and ESEM configuration, view statistics								
View or clear audit log								
Upload/Install Feature File or Firmware Image								
Issue/Fill/Delete Simplex PKI Key Material								
View Filled PKI Information								
User Login								
Power On								
Power Off	Z		Z	Z	Z	Z	Z	Z
Reset								
Display status								
Zeroize (Unauthenticated)	Z	Z	Z	Z	Z	Z	Z	Z
Self-tests			G	G	G	G		
Antenna Handover Service								
Local/Remote								
Alarm Mute								

Table 7: Public Key Access Rights within Services

Service	Public Keys														
	Firmware/ Feature 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**	**Remote Ephemeral KE Public Key**	**Key Fill Ephemeral Public Key**	**LCT Key Fill Remote Ephemeral KE Public Key**	**SSH Ephemeral Public Key**	**SSH Static Public Key**	**SSH Remote Client Ephemeral Public Key**
Telnet, SSH, SNMPv1, SNMPv3, FTP, or SFTP Access															
SSH, SFTP													G, U, O, Z	G, U, S, O	I, U, Z
Circuit Establishment															
Encryption Establishment and Authentication		G, U, O	I,U	U	U	U,O	G,U, O	U	I,U	I, U					
Change Own Password															
Set/Change Admin, Operator User Names & Passwords															
Set/Change SNMPv1 Password															
Enable/Disable encryption															
SMAT Entry and Rollover															
Encryption															
Cryptographically Validate image	I,S														
Zeroize (Authenticated)														Z	
Configure System Time															
Configure Access to Unsecure Protocols															
Configure password policy															
Change/Monitor Modem and ESEM configuration, view statistics															
View or clear audit log															
Upload/Install Feature File or Firmware Image	U														
Issue/Fill/Delete Simplex PKI Key Material				I,S	I,S	I,S		I,S			G,U,O	I,U			
View Filled PKI Information															
User login															
Power On															
Power Off		Z	Z				Z		Z	Z	Z	Z	Z		
Reset															
Display status															
Zeroize (Unauthenticated)														Z	
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 supports defined roles with a defined set of corresponding services. The defined roles shall be:
    - Operator (FIPS 140-2 "User")
    - Administrator (FIPS 140-2 "Crypto Officer")
    - Peer Modem
    - Viasat, Inc.
- Separation of roles: The cryptographic module requires distinct authentication for each role. Simultaneous service is permitted, but authentication is always required when switching between roles
- The cryptographic module does not support a maintenance role or maintenance interface.
- The purpose, function, service inputs, and service outputs performed by each role are defined and appropriately restricted.
- The cryptographic module does not support the output of plaintext CSPs.
- The cryptographic module design ensures 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 supports exclusive bypass capabilities. The cryptographic module requires 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 Administrator password that shall be changed before any services are allowed.
- Re-authentication is required upon power cycling the module.
- The cryptographic module supports role-based or identity-based authentication for all security relevant services; re-authentication is 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 will 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 disallows the ability to simultaneously occupy more than one state at a time.
- The cryptographic module's physically contiguous cryptographic boundary is defined including all module components and connections (ports), information flows, processing,

and input/output data. All vendor-defined non-security relevant circuitry are argued for exclusion from the cryptographic boundary.

- All cryptographic module data output is inhibited when the module is in an error state during any self-test.
- Data output is 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 distinguishes between data and control for input and data and status for output. In addition, the cryptographic module supports a power interface.
- All of the implemented integrated circuits are standard quality, production-grade components.
- The cryptographic module contains an opaque tamper evident enclosure.
- CSPs are protected against unauthorized disclosure, modification, and substitution. Public keys and critical settings are protected against unauthorized modification and substitution.
- The cryptographic module supports key generation using an Approved RNG listed in FIPS PUB 140-2 Annex C.
- The cryptographic module enforces an entity association for all keys that are input to/output from the cryptographic module; an entity association is 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 provides 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 provides an indicator upon successful self-test completion as follows:
    - Fault LED off
- The cryptographic module enters an error state upon failure of any self-test and provides an indicator upon failure as follows:
    - Fault LED on
- Upon entering an error state, the cryptographic module inhibits all data outputs, inhibits cryptographic operations, and provides error status. The status output does 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 an Administrator, or Operator is logged into the Front Panel, SSH, SNMPv1, SNMPv3, FTP, and SFTP protocols users cannot configure the EBEM.

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
EbemCrypto AES	KATs: EbemCrypto, separate encryption and decryption tests Modes: ECB Key sizes: 256 bits
OpenSSL AES	KATs: OpenSSL, separate encryption and decryption tests Modes: CBC, CFB, CTR Key sizes: 256 bits, 128 bits, 256 bits (respectively)
EbemCrypto KTS	KATs: Separate wrap and unwrap tests. Key sizes: 256 bits
EbemCrypto DRBG	KATs: CTR DRBG Security Strengths: 256 bits
EbemCrypto ECDSA	KAT: FIPS 186-4 Signature Verification Curves/Key sizes: P-521 with SHA-512
EbemCrypto ECDSA	PCT: FIPS 186-4 Signature Generation, Signature Verification Curves/Key sizes: P-384 with SHA-384
OpenSSL ECDSA	PCT: FIPS 186-4 Signature Generation, Signature Verification Curves/Key Sizes: P-384 with SHA-384
EbemCrypto HMAC	KATs: Generation, Verification SHA sizes: SHA-384, SHA-512
OpenSSL HMAC	KATs: Generation, Verification SHA sizes: SHA-1, SHA-256, SHA-512
EbemCrypto KAS	KATs: Ephemeral Unified, per IG 9.6 – ECCCDH Primitive Computation and KDF using P-521 curve. Parameter Sets/Key sizes: EE
EbemCrypto KAS	KATs: One Pass DH, per IG 9.6 – ECCCDH Primitive Computation and KDF using P-384 curve. Parameter Sets/Key sizes: ED
OpenSSH KAS	KATs: Ephemeral Unified, per IG 9.6 – ECCCDH Primitive Computation using P-384 curve. Parameter Sets/Key sizes: ED
NetSNMP KDF	KATs: SNMP KDF
OpenSSH KDF	KATs: SSH KDF

EbemCrypto SHA	KATs: EbemCrypto SHA-384, SHA-512
OpenSSL SHA	KATs: OpenSSL SHA SHA-1, SHA-256, SHA-512 Note: SHA-1, SHA-256, and SHA-512 are also tested in OpenSSL HMAC self-tests. SHA-384 omitted (per IG 9.4)
uClibc 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.
EbemCrypto DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
EbemCrypto ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation (static and ephemeral per IG 9.9).
OpenSSL ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation (per IG 9.9 and FIPS PUB 140-2 Section 4.9.2).
Firmware Load	FIPS 186-4 ECDSA P-521 with SHA-512 signature verification performed when firmware is loaded.
EbemCrypto 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) for EbemCrypto Ephemeral Unified KAS and EbemCrypto One Pass DH KAS. Partial validation of OpenSSH Ephemeral Unified KAS.
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 Administrator (FIPS 140-2 “Crypto Officer”) 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):

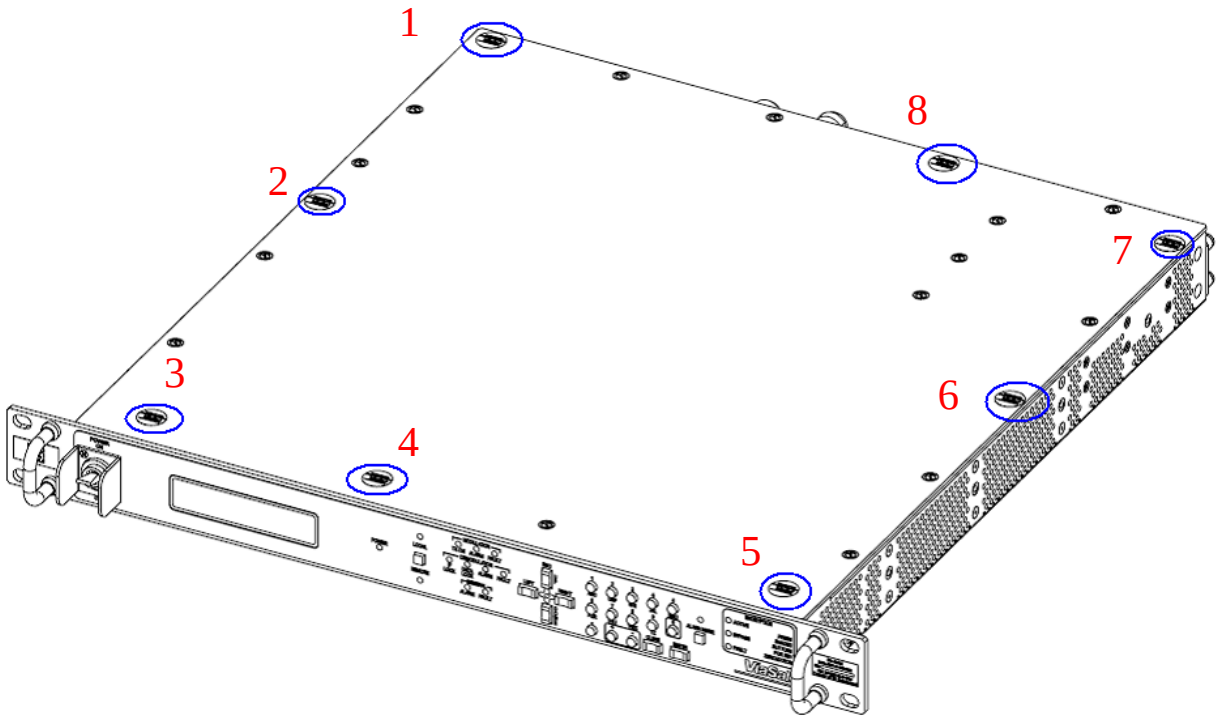

Figure 3: Tamper Seal locations on the Strategic EBEM (Eight Seals)

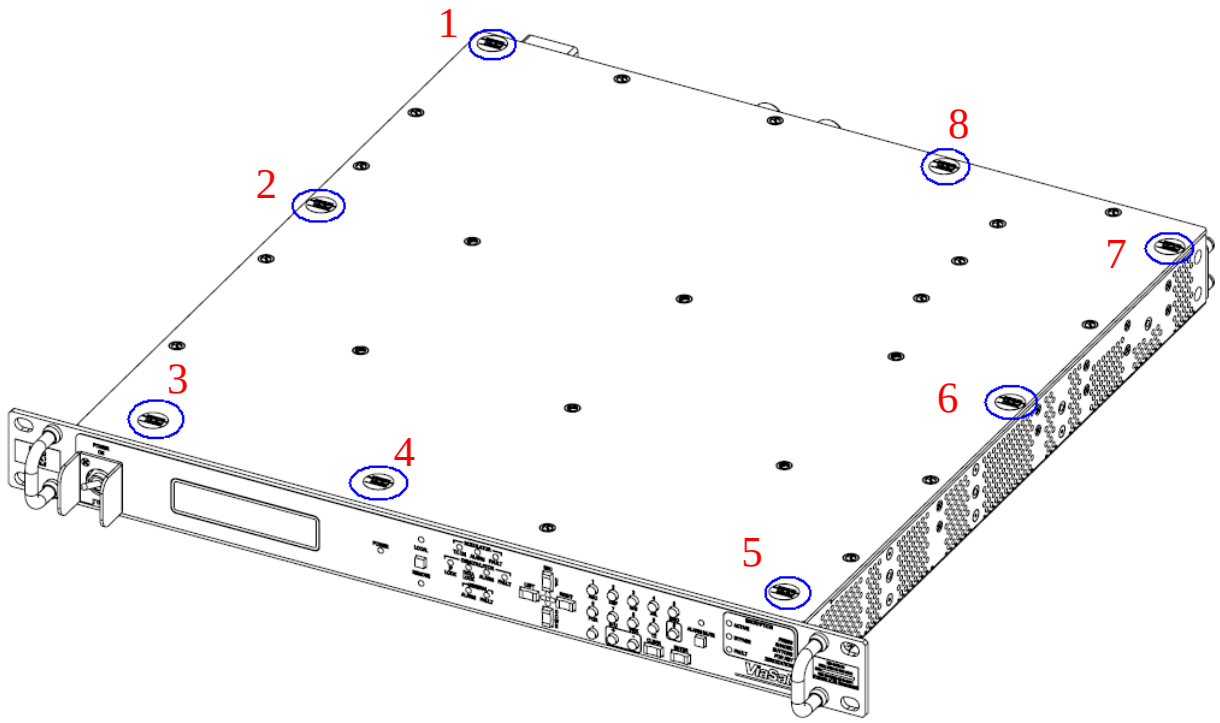

Figure 4: Tamper Seal locations on the Tactical EBEM (Eight Seals)

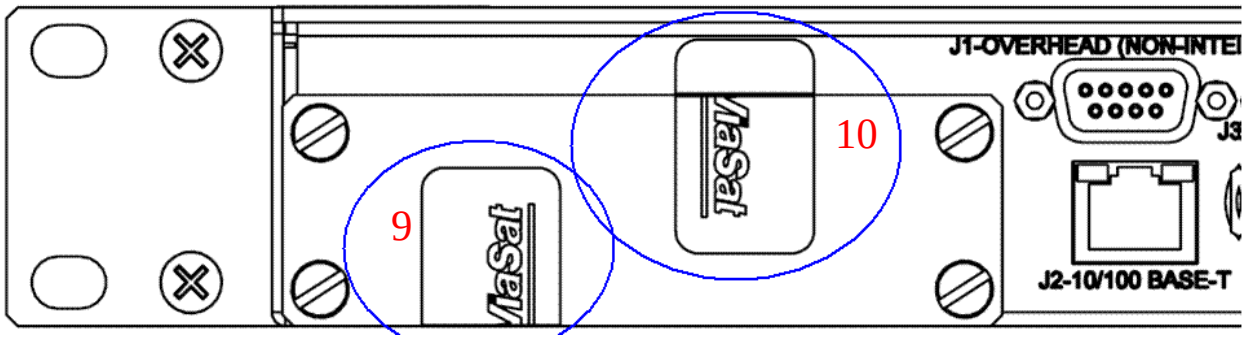

Figure 5: Tamper Seal Location of Expansion Port with Blank Plate Installed (Two Seals)

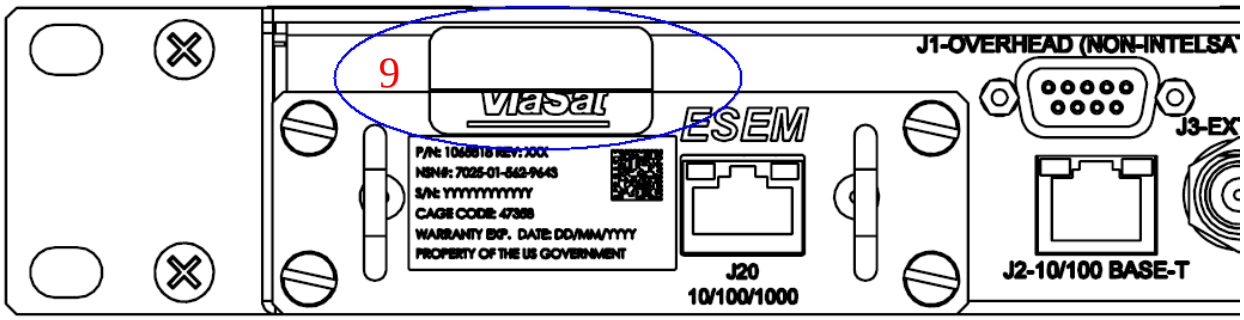

Figure 6: Tamper Seal Location on Expansion Port with ESEM Installed (One Seal)

All tamper seals are installed at the factory except the one shown in Figure 6 for the ESEM. In the case of an EBEM that contains an ESEM (i.e., as in Figure 6, the one (1) tamper seal must be installed by the Administrator (FIPS 140-2 "Crypto Officer"). Prior to installation, the Administrator (FIPS 140-2 "Crypto Officer") 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 Administrator (FIPS 140-2 "Crypto Officer") 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
- NIST SP 800-56A
- NIST SP 800-90A
- NIST SP 800-132
- NIST SP 800-38F

13. Definitions and Acronyms

Acronym	DEFINITION
AES	Advanced Encryption Standard
BIT	Built-in Test
CAVS	Cryptographic Algorithm Validation System
CSP	Critical Security Parameter (as defined per FIPS 140-2)
CTR	Counter (i.e. AES Counter mode)
DRBG	Deterministic Random Bit Generator
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