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

Document Number 1148155, Rev. 001
October 31, 2012

Prepared by:

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

Record of Review and History

VERSION	RATIONALE	RELEASE	AFFECTED PAGES
001	Initial Release in Agile	October 31, 2012	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	02.03.02
	P/N 1010162 with ESEM, Version 1 (also referred to as P/N 1091549, Version 1)	02.03.02
	P/N 1075559, Version 1	02.03.02
	P/N 1075559 with ESEM, Version 1 (also referred to as P/N 1091551, Version 1)	02.03.02
Tactical	P/N 1010163, Version 1	02.03.02
	P/N 1010163 with ESEM, Version 1 (also referred to as P/N 1091550, Version 1)	02.03.02
	P/N 1075560, Version 1	02.03.02
	P/N 1075560 with ESEM, Version 1 (also referred to as P/N 1091552, Version 1)	02.03.02

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

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:

- 2 FPGA AES – ECB and CTR modes with 256-bit keys for data encryption/decryption (Cert. #1203 and 1204)
- FW AES – ECB mode with 256-bit key for encryption/decryption of CSP store (Cert. #2242)
- SHA-1 for hashing (Cert. #1931)
- SHA-256 for hashing (Cert. #1932)
- SHA-512 for hashing (Cert. #1931)
- HMAC-SHA-1 for authentication (SMAT) (Cert. #1372)
- HMAC-SHA-512 for authentication (SMAT) (Cert. #1372)
- FIPS 186-2 Elliptic Curve DSA with 521-bit keys for digital signature verification of externally loaded firmware images (Cert. #351)
- FIPS Approved ANSI X9.31 RNG with 128-bit AES core for random number generation (Cert. #1121)

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

- Elliptic Curve Diffie-Hellman (ECDH) (key agreement; key establishment methodology

provides 128 or 256 bits of encryption strength).

- Telnet – no security is claimed. Non-compliant algorithms used.
- SSH – no security is claimed. Non-compliant algorithms used.
- SNMPv1/SNMPv3 – no security is claimed. Non-compliant algorithms used.
- FTP/SFTP – no security is claimed. Non-compliant algorithms used.

For random value generation the EBEM cryptographic module relies on the implemented deterministic random number generator (RNG) that is compliant with ANSI X9.31 using an AES engine.

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: 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
- Expansion slots: 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 2: 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
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)
ViaSat, Inc.	Signer of ESEM configuration files and software images. A ViaSat trust anchor used to validate authenticity when loading these files on modem.	Identity-based	ECDSA Signature Key

Table 3: 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. A reboot is required to change the HMAC key, so only one unique HMAC authentication attempt will occur in any one minute period. The probability of successfully authenticating to the module within one minute is 1 / 2^160 which is less than 1/100,000.
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. The probability of successfully authenticating to the module within a one minute period is also 1 / 2^80 (which is < 1/100,000) due to a maximum of one attempt per minute.

6. Access Control Policy

Roles and Services

Table 4: Services Authorized for Roles

Service	Description	Operator	Administrator	Cryptographic Officer	Peer Modem	ViaSat, Inc.
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) 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 Admin, Operator User Names & Passwords		X	X		
Change Admin and Operator Passwords	Change Admin and Operator Passwords		X	X		
Enable/disable encryption	Configure module exclusive bypass settings			X		
Set Admin, Operator, and CO User Names & Passwords	Set Admin, Operator, and CO User Names & Passwords			X		
Change Admin, Operator, and CO Passwords	Change Admin, Operator, and CO Passwords			X		
SMAT Entry	SMAT Entry via front panel			X		

Service	Description	Operator	Administrator	Cryptographic Officer	Peer Modem	ViaSat, Inc.
RNG Seed Entry and Acceptance	RNG Seed Entry and acceptance.			X		
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	Actively overwrite all CSPs.	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			

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.

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Operator, Administrator, or Crypto Officer login
- Power On
- Power Off
- Reset

- Display status: Show non-security relevant status of the cryptographic module via the front panel.
- Zeroize: Actively overwrite all Critical Security Parameters (CSPs) through SNMPv1, or the front panel.
- Self-tests: Perform a suite of Power On Self Tests (POSTs). All POSTs are initiated automatically without operator intervention
- Antenna Handover Service (command sent from ship to modem to switch antennas).
- 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).
- Alarm Mute: Mute the audible alarm.

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.
- Seed: A 128-bit initialization vector to the FIPS-Approved ANSI X9.31 RNG
- Seed Key: A 128-bit AES Key that is input to the FIPS-Approved ANSI X9.31 RNG.
- RNG Internal State: The internal state of the FIPS-Approved ANSI X9.31 RNG, used as an input to the next RNG state.
- TxTEK (Transmit Traffic Encryption Key): A 256-bit AES CTR mode traffic encryption key. This key is used to protect data sent over RF circuits from modems to peer modems.
- RxTEK (Receive Traffic Encryption Key): A 256-bit AES CTR mode traffic decryption key. This key is used to decrypt protected data sent over RF circuits from peer modems. This key is an exact match of a peer modem's TxTEK for symmetric AES cryptographic communication.
- AES Counter: The lower 64 bits of a 128 bit counter used for CTR mode encryption; incremented every AES block. This is generated by a tick count which is an authenticated service. Only authenticated roles have access to the AES Counter.
- AES Nonce: The upper 64 bits of a 128-bit counter used for CTR mode encryption; regenerated every circuit establishment.
- ECDH Private Key: Module's private key used for circuit establishment with peer modem, per FIPS SP800-56A Section 5.8.1.2 Elliptic Curve Diffie-Hellman.
- ECDH Shared Secret (Z=xp): Generated per FIPS SP800-56A and used with Section 5.8.1.2 Concatenation KDF to establish the TEKs and IVs.
- 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.
- 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.
- Password Encryption Key: A 256-bit AES key used to encrypt centralized user database of user names and passwords.

Definition of Public Keys:

The following are the public keys contained in the module.

- Trust Anchor - ECDSA Public Key: Used to validate the authenticity of signed code images and/or feature files
- ECDH Public Key: Module's public key used for circuit establishment with peer modem, per FIPS SP800-56A Section 5.8.1.2 Elliptic Curve Diffie-Hellman.
- Peer Modem's Public Key: Peer Modem's public key used for circuit establishment, per FIPS SP800-56A Section 5.8.1.2 Elliptic Curve Diffie-Hellman.

Definition of CSPs Modes of Access

Table 5 defines the relationship between CSPs and only those module services that access CSPs. The modes of access shown in the Table 5 are defined as follows.

- Input (I): the data item is entered into the cryptographic module
- 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 5: CSP and Public Key Access Rights within Services

Service	CSPs and Public Keys																
	SMAT (HMAC Key)	**Seed & Seed Key**	**RNG Internal State**	**TxTEK**	**RxTEK**	**AES Counter**	**AES Nonce**	**ECDH Private**	**ECDH Shared Secret**	**Bypass Flag**	**Crypto Compatibility Mode**	**CO Password**	**Administrator Password**	**Operator Password**	**Password Encryption Key**	**Trust Anchor**	**ECDH Public Key**	**Peer Modem's Public Key**
Telnet, SSH, SNMPv1, SNMPv3, FTP, or SFTP													I,U	I,U				
Circuit Establishment										U			I, U	I, U				
Encryption Establishment and Authentication	U		U	E	E	G	G	G	E		U		I, U	I, U			U	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				
Change Admin and Operator Passwords													I, S	I, S				
Enable/disable encryption	U		U	E,U	E,U	G,U	G,U	G,U	E,U	U	U	I, U						
Set Admin, Operator, and CO User Names & Passwords												I, S						
Change Admin, Operator, and CO Passwords												I, S						
SMAT Entry	I,U, S											I, S						
RNG Seed Entry and Acceptance		I,U, S										I, U						
Set Crypto Compatibility Mode											I, S	I, U						
Encryption	U		U	E,U	E,U	G,U	G,U	G,U	E,U								G,U	U

Service	CSPs and Public Keys																	
	SMAT (HMAC Key)	**Seed & Seed Key**	**RNG Internal State**	**TxTEK**	**RxTEK**	**AES Counter**	**AES Nonce**	**ECDH Private**	**ECDH Shared Secret**	**Bypass Flag**	**Crypto Compatibility Mode**	**CO Password**	**Administrator Password**	**Operator Password**	**Password Encryption Key**	**Trust Anchor**	**ECDH Public Key**	**Peer Modem's Public Key**
Cryptographically Validate image																I, U		
Zeroize (Authenticated)	Z	Z	Z	Z	Z	Z	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 configuration or monitor modem													I,U	I,U				
View or clear audit log													I,U					
Upload Image													I,U					
Operator, Admin, & CO login												I, U	I, U	I, U	U			
Power On																		
Power Off																		
Reset																		
Display status																		
Zeroize (Unauthenticated)	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z		Z	Z
Self-tests	U	U	U	U	U	U	U	U	U			U, I	U, I	U, I			U	
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:
    - Operator
    - Administrator
    - Cryptographic-Officer
    - Peer Modem
    - 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.
- The cryptographic module shall ensure that the seed and seed key inputs to the approved RNG are not equal.
- 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.
- 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 9 shall be installed for the module to operate in a FIPS Approved mode of operation.
- The cryptographic module shall support the following self-tests:

Power up Self Tests

- Cryptographic algorithm tests
  - 2 FPGA AES KATs (ECB encrypt only KAT required because CTR mode utilizes ECB encrypt for both encryption and decryption)
  - FW AES KAT (ECB encrypt and decrypt)
  - HMAC-SHA-1 KAT (includes test for underlying SHA-1 implementation)
  - SHA-256 KAT
  - HMAC-SHA-512 KAT (includes test for underlying SHA-512 implementation)
  - ECDSA KAT (verify)
  - ANSI X9.31 RNG KAT
  - ECDH power up self tests
- Critical functions tests
  - Integrity test on persistent storage (32-bit EDC)
  - Verification of FPGA loading (BIT)
- Firmware integrity test on all executable code (32-bit EDC)

Conditional Self Tests

- Continuous RNG Test
- Firmware Load Test via ECDSA signature verification
- Manual Key entry test performed via Error Detection Code
- ECDH conditional self tests
- Bypass Tests:
  Exclusive 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).

9. 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 tamper evident seals
- Protected vents

Operator Required Actions

The CO is required to periodically inspect the tamper evident seals, enclosure, and vents as shown in Table 6. 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 6: 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):

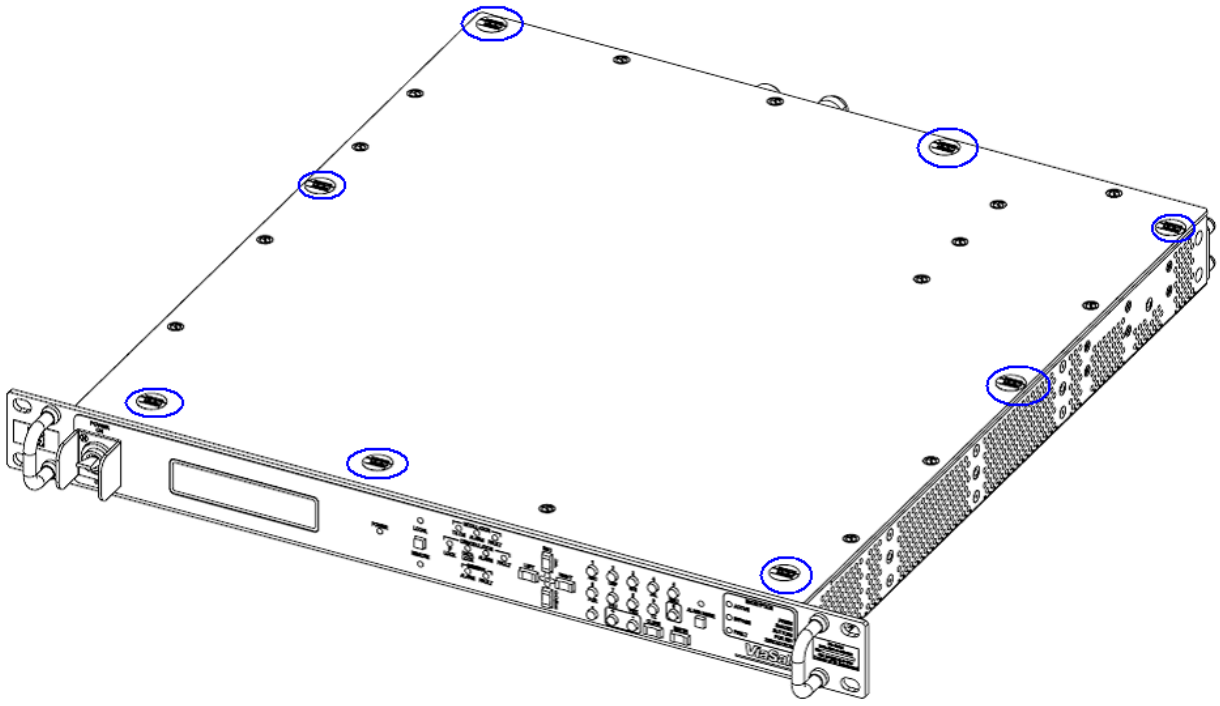

Figure 2: Tamper Seal locations on the Strategic EBEM (8 seals)

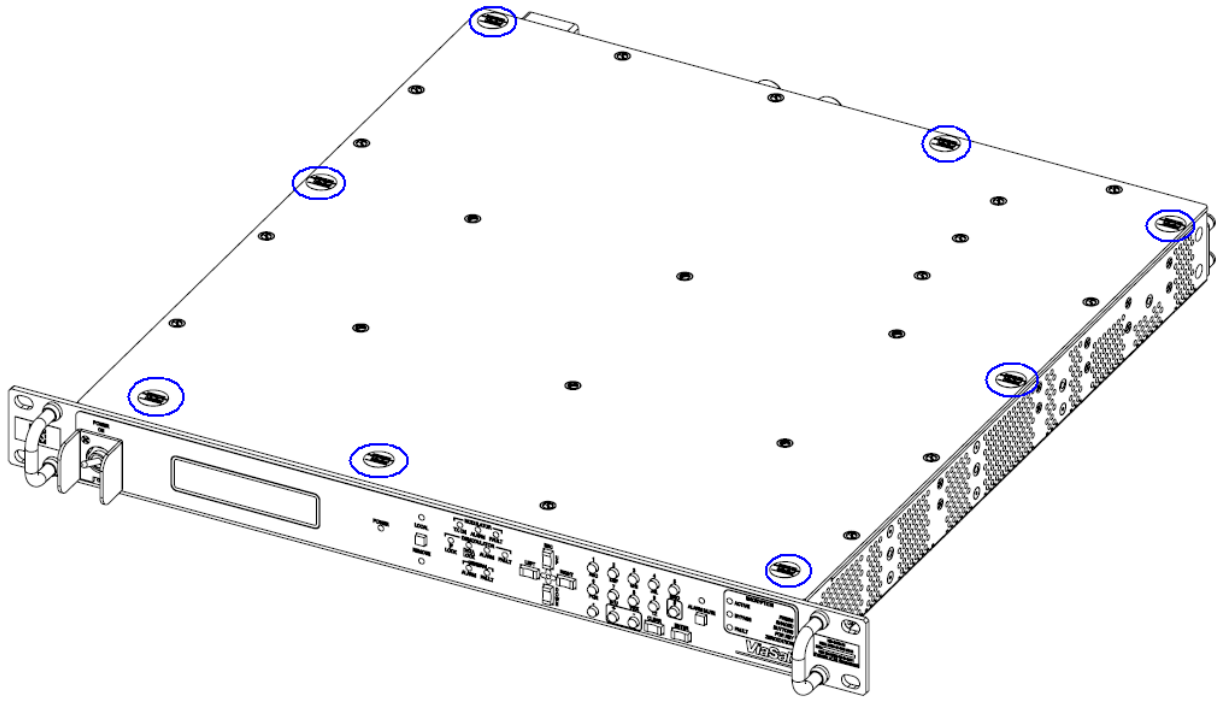

Figure 3 Tamper Seal locations on the Tactical EBEM (8 seals)

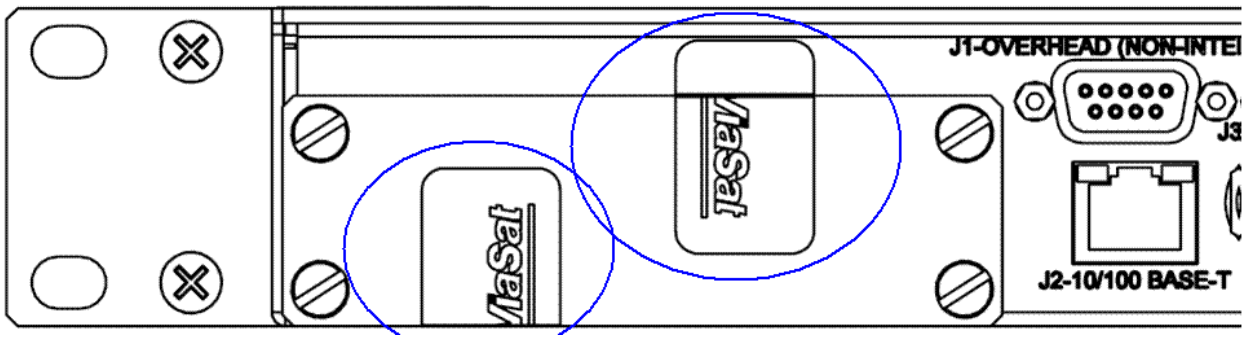

Figure 4: Tamper Seal Location of Expansion Port with Blank Plate Installed (2 seals)

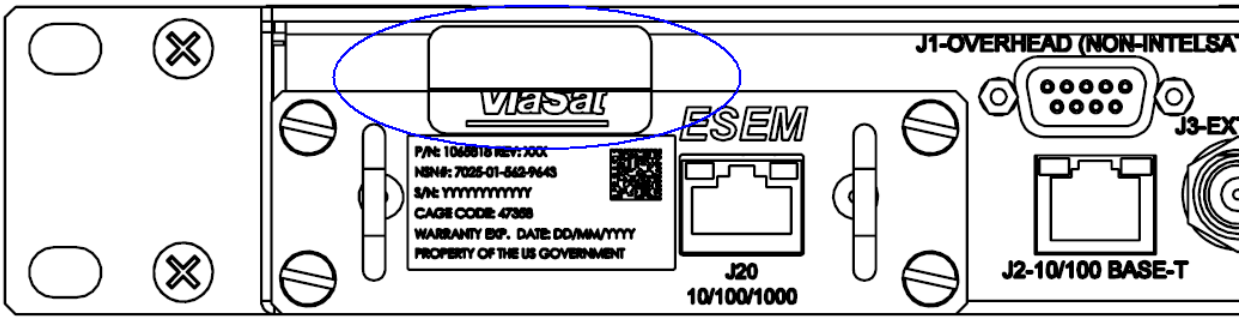

Figure 5: Tamper Seal Location on Expansion Port with ESEM Installed (1 seal)

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.

10. Mitigation of Other Attacks Policy

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

11. References

- FIPS PUB 140-2
- FIPS PUB 180-1
- FIPS PUB 180-2
- FIPS 186-2
- FIPS PUB 198
- FIPS PUB 46-3
- FIPS PUB 186-2
- FIPS SP800-56A

12. 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)
DSA	Digital Signature Algorithm
ECB	Ethernet Client Bridge
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
FW	Firewall
KDF	Key Derivation Function
LCT	Local Control Terminal
LED	Loop Encryption Device
Mbps	Million Bits per Second
Modem	Modulator/Demodulator
RNG	Random Number Generator
RX	Receiver
SCPC	Single Channel Per Carrier
SHA	Secure Hash Algorithm
SMAT	Shared Message Authentication Token
SNMP	Simple Network Management Protocol
TX	Transmit