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

Document Number 1057314, Rev. 011
July 7, 2010

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	May 4, 2007	All
002	Updated for EBEM SW Release 01.01.08	July 24, 2007	All
003	Revised per InfoGard comments for SW Release 01.01.08	August 6, 2007	All
004	Updated for EBEM SW Release 01.03.05	May 19, 2008	All
005	Updated per InfoGard comments for SW Release 01.03.05	June 24, 2008	All
006	Updated to include commercial HW part numbers for both EBEM variants	July 10, 2009	All
007	Updated for EBEM Release 02.01.04 and ESEM module	October 28, 2009	All
008	Updated “DRNG” to “RNG” per InfoGard comments	November 13, 2009	All
009	Updated to clarify references to SP800-56A per comments	November 18, 2009	All
010	Updated to address CMVP comments	June 3, 2010	All
011	Updated to address 2nd set of CMVP comments	July 7, 2010	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	01.03.05 and 02.01.04
	P/N 1010162 with ESEM, Version 1	02.01.04 only
	P/N 1075559, Version 1	01.03.05 and 02.01.04
	P/N 1075559 with ESEM, Version 1	02.01.04 only
Tactical	P/N 1010163, Version 1	01.03.05 and 02.01.04
	P/N 1010163 with ESEM, Version 1	02.01.04 only
	P/N 1075560, Version 1	01.03.05 and 02.01.04
	P/N 1075560 with ESEM, Version 1	02.01.04 only

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:

- AES – ECB and CTR modes with 256-bit keys for data encryption/decryption
- SHA-1 for hashing
- SHA-512 for hashing
- HMAC-SHA-1 for authentication (SMAT)
- HMAC-SHA-512 for authentication (SMAT)
- Elliptic Curve DSA with 521-bit keys for digital signature verification of externally loaded firmware images
- FIPS Approved ANSI X9.31 RNG with 128-bit AES core for random number generation

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

- Elliptic Curve Diffie-Hellman (ECDH) (key agreement; key establishment methodology provides 256 bits of encryption strength).

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 example 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 shall support four distinct operator roles (User, 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	Type of Authentication	Authentication Data
User	Role-based operator authentication	Password

Role	Type of Authentication	Authentication Data
Cryptographic-Officer	Role-based operator authentication	Password
Peer Modem	Modem communities sharing a common SMAT (Shared Message Authentication Token) input to the HMAC	HMAC Key
ViaSat, Inc. Role	Identity-based authentication through ECDSA digital signature	ECDSA Signature Key

Table 3: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
User Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/1,000,000. The probability of successfully authenticating to the module within one minute is 3/1,000,000 which is less than 1/100,000.
Crypto Officer Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/1,000,000. The probability of successfully authenticating to the module within one minute is 3/1,000,000, which is less than 1/100,000.
HMAC Verification	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 probability of successfully authenticating to the module within one minute is number of possible HMAC attempts in a 1 minute period is 1 / 2^160 which is less than 1/100,000.
ECDSA Signature	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 due to maximum of one attempt per minute.

6. Access Control Policy

Roles and Services

Table 4: Services Authorized for Roles

Role	Authorized Services
User	• Circuit Establishment: Set up an encryption circuit • Encryption establishment: use HMAC (with SMAT) to authenticate the AES encrypted the pipeline. • Telnet or SNMPv1 Service: Connect to the EBEM using Telnet or SNMPv1 • Disconnect circuit: tear down the link (by command or power cycle).
Cryptographic-Officer	• RNG Seed Entry and Acceptance • Set User Password • Change CO & User Passwords • Enable/disable encryption: configure module exclusive bypass settings • SMAT Entry via front Panel • Set encryption compatibility mode
Peer modem role	• Encryption: Perform encryption on an established encrypted circuit with a peer modem. • Authenticate Encrypted circuit (far end modem): use HMAC (with SMAT) to authenticate the AES encrypted the pipeline. • Disconnect encrypted circuit (tear down the link)
ViaSat, Inc. Role	• Cryptographically validate and load an uploaded firmware image • Cryptographically validate and load an uploaded feature file • Cryptographically validate and load an uploaded ESEM configuration file

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- User & CO login
- Power On
- Power Off
- Reset
- SNMPv1: set/get non-security relevant parameters.

- Establish unencrypted circuit: establish a circuit to an external modem using a plaintext link via Telnet, SNMPv1, or the front panel (note: this requires the Cryptographic Officer to first set the 'bypass' flag in the 'Enable/disable' encryption service).
- Display status: show non-security relevant status of the cryptographic module via Telnet, SNMPv1, or the front panel.
- Zeroize: actively overwrite all Critical Security Parameters (CSPs) through the Telnet, SNMPv1, or the front panel.
- Self-tests: Perform a suite of power-up self tests
  - All power-up self tests are initiated automatically without operator intervention
  - Send a command via Telnet, SNMPv1, or front panel.
- Antenna Handover Service (command sent from ship to modem to switch antennas).
- Upload File
- Manage configuration files
- Enable/disable trial period for access to additional configuration items
- System log
- View log
- Clear log
- Export log
- Manage features: install feature (configuration) file
- View ESEM hardware information
- View Ethernet and link statistics
- Clear Ethernet and link statistics

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.
- CO password: 6-digit minimum 20 maximum, chosen from 10 digits; used to authenticate CO, will lockout after 3 failed attempts.
- User password: 6- digit minimum 20 maximum passwords, used to authenticate the User; will lockout after 3 failed attempts.
- Seed: ANSI X9.31 compliant RNG with AES for Random number generation.
- Seed Key: ANSI X9.31 compliant RNG with AES for Random number generation.
- RNG Internal State: Used for generating random numbers via ANSI X9.31 RNG.
- TxTEK (Transmit Traffic Encryption Key): A 256-bit AES CTR mode traffic encryption key; used to protect the circuit between modems.
- RxTEK (Receive Traffic Encryption Key): A 256-bit AES CTR mode traffic decryption key; used to protect the circuit between modems.
- 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: Circuit establishment with peer modem, per FIPS SP800-56A Section 5.8.1.2 Elliptic Curve Diffie-Hellman.
- ECDH Shared Secret (Z=xp): Per FIPS SP800-56A Section 5.8.1.2 Elliptic Curve Diffie-Hellman. Concatenation KDF state: per FIPS SP800-56A.
- 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.

Definition of Public Keys:

The following are the public keys contained in the module.

- Trust Anchor - ECDSA Public Key: verify authenticity of new firmware images
- ECDH Public Key: circuit establishment with peer modem, 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

As specified per end user policy

Table 5: CSP Access Rights within Roles & Services

Role					Service	CSPs											
ViaSat, Inc.	**Unauthenticated**	**C.O.**	**User**	**Peer Modem**		**SMAT**	**CO Password**	**User Password**	**Seed&Seed Key**	**RNG State**	**TxTEK**	**RxTEK**	**AES Counter**	**AES Nonce**	**ECDH Private**	**ECDH Shared Secret**	**Bypass Flag**	**Crypto Compatibility Mode**
	X				User&CO login		I, U	I, U										
		X			Enable/disable encryption	U		I, U		U	E,U	E,U	G,U	G,U	G,U	E,U	U	U
			X		Circuit Establishment			I, U									U	
			X		Encryption Establishment	U		I, U		U	E	E	G	G	G	E		U
				X	Encryption	U				U	E,U	E,U	G,U	G,U	G,U	E,U		
				X	Authenticate Encrypted circuit	U												
			X	X	Disconnect Encrypted circuit			I, U										
		X			Set User Password			I, S										
		X			Change CO and User passwords		I, S	I, S										
X					Cryptographically Validate Firmware image													
			X		Telnet or SNMPv1			I,U										
	X	X	X		Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
	X	X	X	X	Self-tests	U	U, I	U, I	U	U	U	U	U	U	U	U		
		X			SMAT Entry	I	U,I											
		X			RNG Seed Entry and Acceptance		U,I		I									
		X			Set Crypto Compatibility Mode													I, S

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.

- Separation of roles: The cryptographic module shall disallow a User and Cryptographic Officer from obtaining services at the same time. If a User is logged into the modem, and a Cryptographic Officer then logs in, the module shall automatically log out the User role. This shall be accomplished through a forced power cycle.
- The cryptographic module shall support defined roles with a defined set of corresponding services. The defined roles shall be:
    - User
    - Cryptographic Officer
    - Peer Modem
    - ViaSat, Inc. Role
- 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
  - ECDSA KAT (verify)
  - AES KAT (encrypt/decrypt)
  - ANSI X9.31 RNG KAT
  - HMAC-SHA-1 KAT (includes test for underlying SHA-1 implementation)
  - HMAC-SHA-512 KAT (includes test for underlying SHA-512 implementation)
  - ECDH power up self tests
- Critical functions tests
  - Integrity test on persistent storage (32 bit EDC)
  - ECDH Pair-wise Consistency Test
  - Verification of FPGA loading (BIT)
- Firmware/software 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 checking a flag value, which is stored 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 labels 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 depicts the tamper label locations (circled in blue):

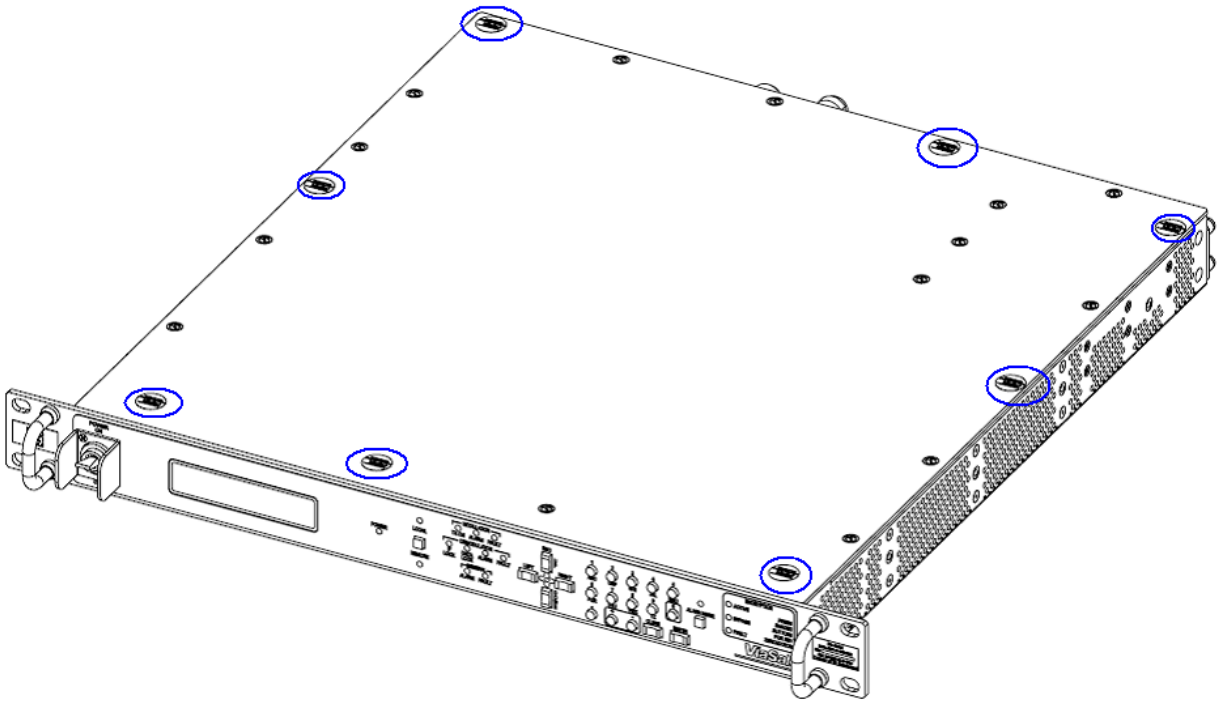

Figure 2: Tamper Label locations on the Strategic EBEM (8 labels)

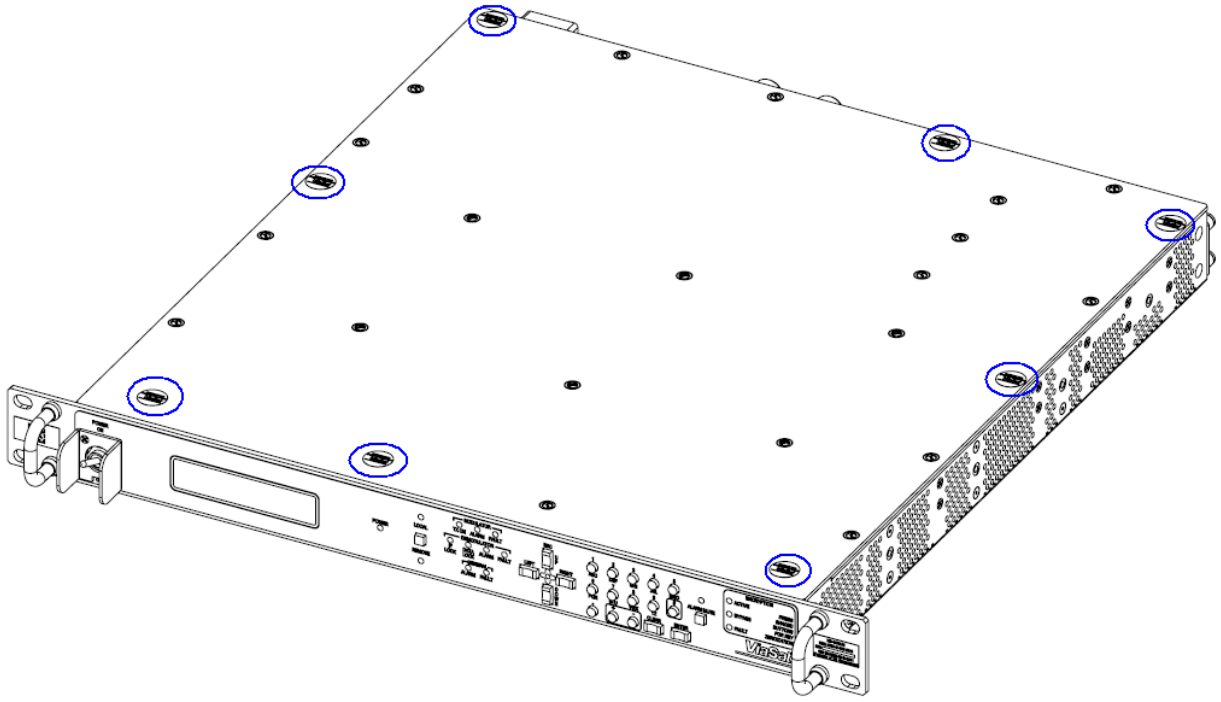

Figure 3 Tamper Label locations on the Tactical EBEM (8 labels)

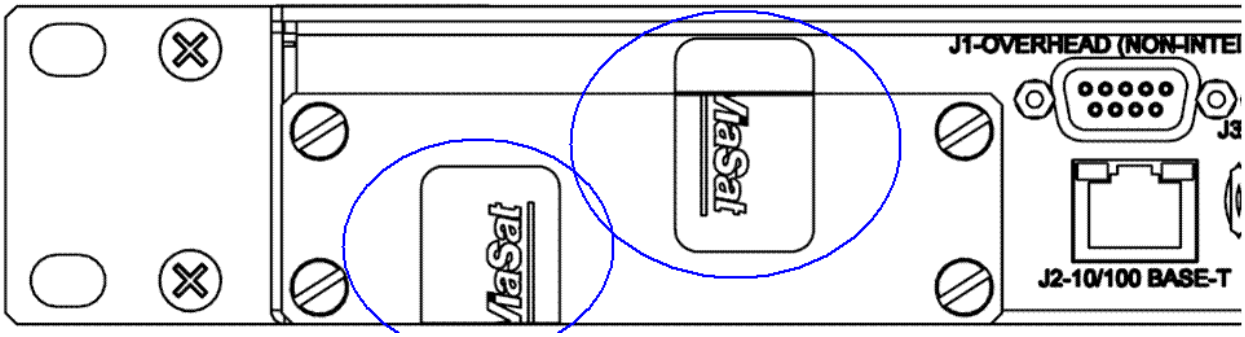

Figure 4: Tamper Label Location of Expansion Port with Blank Plate Installed (2 labels)

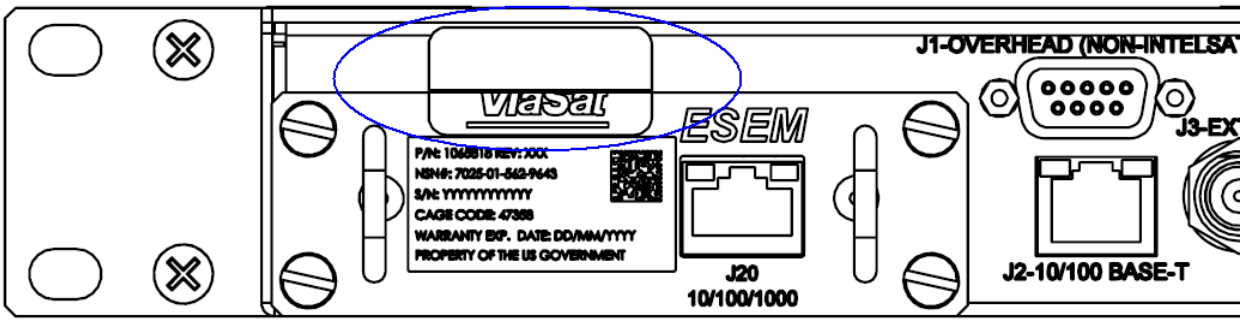

Figure 5 Tamper Label Location on Expansion Port with ESEM Installed (1 label)

All tamper labels 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 label 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 label installation are provided in ViaSat, Inc.'s *EBEM Password Administrator User Guide and Software/Firmware Installation Guide*, ViaSat document number 1052586, Section 11.

10. Mitigation of Other Attacks Policy

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

Table 7: Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

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