Viasat, Inc.
Type 3 Data Encryption Device
(V3K-102)

Non-Proprietary Security Policy

Document 1216806 Version 002

March 23, 2022

TABLE OF CONTENTS

1 Module Overview

The Viasat Type 3 Data Encryption Device (V3K-102) is a multi-chip embedded cryptographic module. The V3K-102 is implemented as two nearly-identical hardware variants: the commercial-temperature hardware variant which includes a disabled ethernet port (P/N 1090927, revisions 002, 003, 004, and 005[i]) and the industrial-temperature hardware variant without an ethernet port (P/N 1163385, revisions 001 and 002); both the commercial and industrial temperature variants use firmware version 1.5.3. The V3K-102 provides encryption and decryption services, key management and can provide filtering for domain separation. The V3K-102 uses a PMC interface, allowing it to be used internal to communications equipment. The V3K-102 is intended for use in environments where "Type 3" cryptographic products are required. Typical applications are military Type 3 Transmission Security (TRANSEC), Type 3 Communications Security (COMSEC). The cryptographic boundary of the module is the boundary of the V3K-102 board.

Figures 1-1 and 1 2 show the V3K-102 (1090927) and its cryptographic boundary along with all of the interface ports. Figures 1-3 and 1-4 show the V3K-102 (1163385) and its cryptographic boundary along with all of the interface ports.

Figure 1-1 Top Side of the 1090927 Cryptographic Module

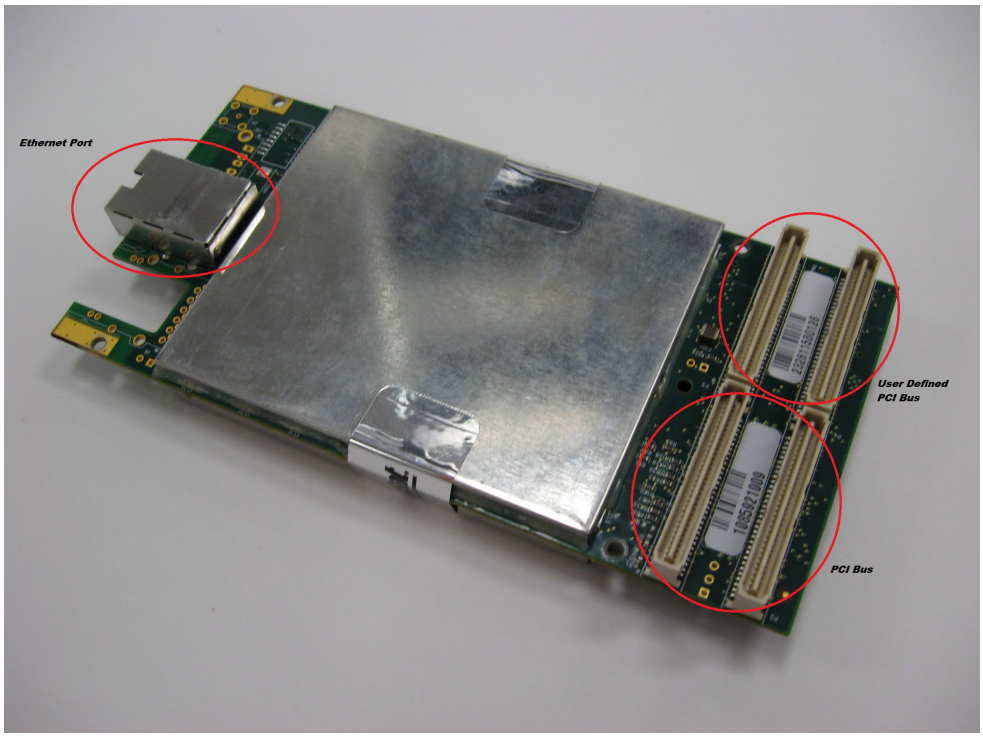

Figure 1-2 Bottom Side of the 1090927 Cryptographic Module

Figure 1-3 Top Side of the 1163385 Cryptographic Module

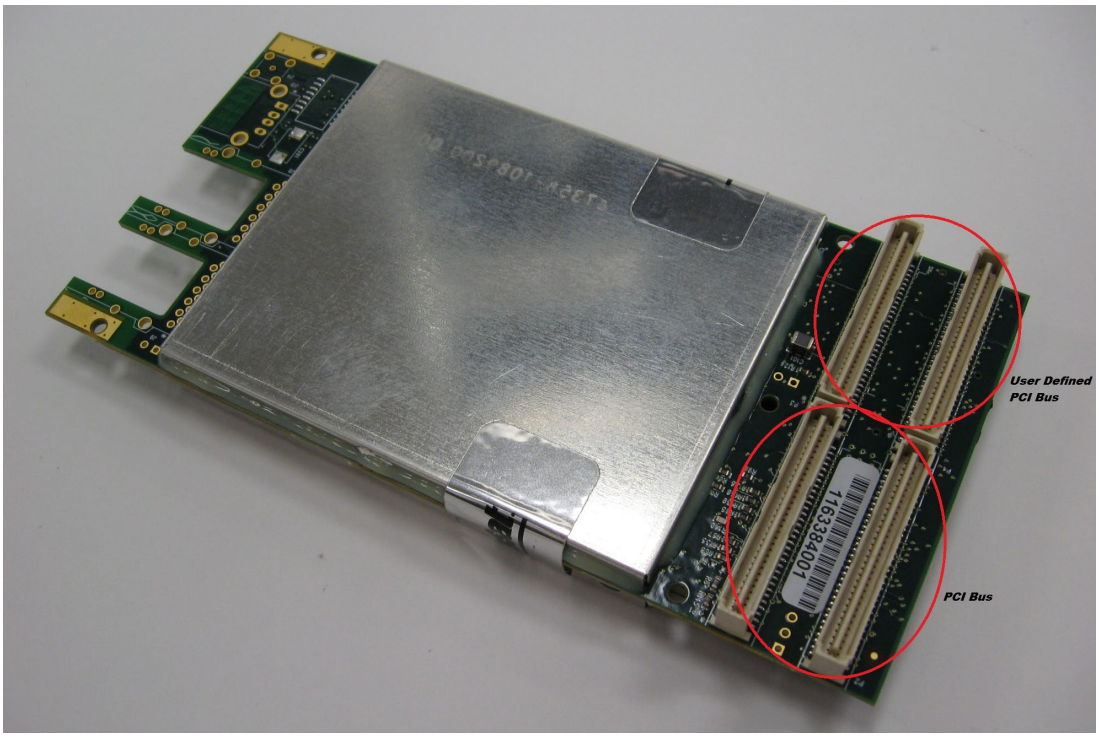

Figure 1-4 Bottom Side of the 1163385 Cryptographic Module

2 Security Level

The V3K-102 meets the overall requirements applicable to Level 2 security of FIPS 140-2. Table 1 specifies the levels met for specific FIPS 140-2 areas.

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

The V3K-102 runs in a single FIPS-Approved mode of operation that supports 3 different logical configurations defined below. The logical configuration that the module executes in is dependent on the Modem hardware into which it is installed.

- LinkWay on S2 Hardware
    - This configuration provides the cryptographic capabilities required for the Viasat LinkWay waveform operating on Viasat S2 hardware.
- LinkWay on CBM Hardware
    - This configuration provides the cryptographic capabilities required for the Viasat LinkWay waveform operating on Viasat CBM hardware.
- Generic Interface on CBM Hardware
    - This configuration provides a waveform-agnostic interface to the V3K-102 cryptographic module operating on Viasat CBM hardware.

The cryptographic module supports the following FIPS Approved algorithms:

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

Algorithm Implementation	Algorithm	Description	CAVP Cert. #
AES_CTR_LWS2-1.5.0	AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption (in FPGA for data) Modes: ECB (Encryption only), CTR (Encryption and Decryption) Instances: 2 data paths Key size: 256 bits	A2331
AES_CTR_LWCBM-1.5.0	AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption (in FPGA for data) Modes: ECB (Encryption only), CTR (Encryption and Decryption) Instances: 4 data paths Key size: 256 bits	A2332

Algorithm Implementation	Algorithm	Description	CAVP Cert. #
AES_CTR_G-1.5.0	AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption (in FPGA for data) Modes: ECB (Encryption only), CTR (Encryption and Decryption) Instances: 4 data paths Key size: 256 bits	A2330
AESUtils-1.5.0	AES	[FIPS 197, SP 800-38A, SP800-38F] Functions: Encryption, Decryption (in Processor for CSPs) Modes: ECB, KW Key size: 256 bits	A2329
	KTS	AES-KW using 256 bit keys	A2329
NistCtrDrbg-1.5.0	DRBG	[SP 800-90A] Functions: CTR DRBG Security Strengths: 256 bits	A2336
	CKG	[SP 800-133] Asymmetric Key Generation (§ 5) and Symmetric Key Generation (§ 6) without further post processing	Vendor Affirmed
EcDSAUtils-1.5.0	ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, and Signature Verification Curves/SHA sizes: Signature Generation: P384 with SHA-384 Signature Verification: P-521 with SHA-512, P-384 with SHA-384 or SHA-512	A2333

Algorithm Implementation	Algorithm	Description	CAVP Cert. #
	KAS	[SP 800-56A] Schema: Ephemeral Unified Key sizes: P-521 One Step Concatenation KDF with SHA-512 Schema: One Pass DH Key sizes: P-384 One Step Concatenation KDF with SHA-384 Key establishment methodology provides 192 or 256 bits of encryption strength	A2333
ENT (NP)	SP800-90B	[SP 800-90B] Provides 0.798 bits of entropy per bit sampled. Used to instantiate the DRBG to a security strength of 256 bits.	N/A
FIPS198-1.5.0	HMAC	[FIPS 198-1] Functions: Generation, Verification (for SMAT and PBKDF2 authentication) SHA sizes: SHA-384, SHA-512 Key length: Minimum of 112 bits	A2334
SP800_108-1.5.0	KBKDF	[SP 800-108] Functions: Key Derivation Function in Counter Mode HMAC: HMAC-SHA384	A2339
PBKDF2-1.5.0	PBKDF2	[SP 800-132] Functions: HMAC-SHA384 Iterations: 1-1000	A2337

Algorithm Implementation	Algorithm	Description	CAVP Cert. #
SHAUtils-1.5.0	SHA	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-384, and SHA-512	A2338
JENT	SHA-3	Functions: SP800-90B Conditioning Function. SHA size: SHA3-256	A2335

The V3K-102 leaves the factory in a FIPS Approved mode of operation and does not contain a Non-FIPS Approved mode of operation. The operator invokes the FIPS Approved mode of operation simply by powering on the V3K-102.

The FIPS Approved mode of operation is indicated by a Status Output to the I^2C Front Panel LCD. The Status Output indicating FIPS Approved mode of operation is a non-blank character in the first character position of the first row of the display. The non-blank character is one of 'A', 'U' or '-'.

The Status Output Bypass LED bit on the I^2C Front Panel is indicated as "off" when the module is running normally without bypass and "on" if encryption is being exclusively bypassed (Note: Bypass is set via the Enable/Disable Bypass service).

Additionally, the Message API provides a mechanism for querying the status of FIPS Approved mode of operation.

4 Ports and Interfaces

The V3K-102 provides the following physical ports and logical interfaces:

- PCI Bus (qty. 2) - control input, status output
- User Defined PCI Bus (qty. 2) - data input, data output, control input, status output (control input & status output support the "Message API")
- I^2C Front Panel Port – data input, data output, control input, status output
- Power Port
- Ethernet Port – disabled (not present on P/N 1163385)

5 Identification and Authentication Policy

The V3K-102 supports three distinct operator roles. The module enforces the separation of roles using role-based operator authentication. Table 3 lists the supported operator roles along with their required identification and authentication techniques. Table 4 outlines each authentication mechanism and the associated strengths.

Table 3 - Roles and Required Identification and Authentication

Role	Description	Type of Authentication	Authentication Data
User	A "User" from the FIPS 140-2 perspective.	Role-based	User name and Password
Crypto Officer (Admin)	A "Crypto Officer" from the FIPS 140-2 perspective.	Role-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 Role-based	HMAC Key, also referred to as SMAT (Shared Modem Authentication Token) Identity and Authentication (IA) FIPS 186-4 ECDSA Signature Key Pair
Vendor (Viasat, Inc.)	Signer of firmware image files and feature files. A Viasat trust anchor used to validate authenticity when loading these files on modem.	Role-based	FIPS 186-4 ECDSA Signature Key

Table 4 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	A password entered via the Front Panel interface consists of between 8 and 20 numeric characters. The probability that a random attempt will succeed or a false acceptance will occur is $1/10^8$ which is less than 1/1,000,000. A password entered via the Message API consists of between 8 and 20 octets. The probability that a random attempt will succeed or a false acceptance will occur is $1/255^8$ which is less than $1/1.7x10^{19}$. Entering an incorrect password 9 consecutive times will lock the module. The probability of successfully authenticating to the module within one minute is $9/10^8$ which is less than 1/100,000.
HMAC Key	The probability that a random attempt will succeed or a false acceptance will occur is the strength of the embedded SHA-384 function $1 / 2^{192}$ which is less than 1/1,000,000. When the HMAC key is entered (encrypted) over the Message API interface, it takes approximately 0.01 seconds to fill so no more than 6000 attempts can occur in any one minute period. The probability of successfully authenticating to the module within a one minute period is $6000 / 2^{192}$ (which is < 1/100,000) due to a maximum of six thousand attempts per minute.
FIPS 186-4 ECDSA IA/Firmware/Feature Signature Key (P-384/SHA-384)	Using the V3K-102'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. For Firmware/Feature Signatures, there is a maximum of three attempts per minute. The probability of successfully authenticating to the module within a one minute period is $3/2^{192}$ which is less than 1/100,000.

6 Access Control Policy

6.1 Roles and Services

Table 5 lists each operator role and the services authorized for each role. Following Table 4, all unauthorized services are listed.

Table 5 - Services Authorized for Roles

Roles				Authorized Services
User	**Crypto-Officer (Admin)**	**Peer Modem**	**Vendor**	
X	X			**Circuit Establishment:** Configure an encrypted or unencrypted circuit. Applicable only to the Generic mode of operation.
		X		**Encryption:** Perform encryption on an established encrypted circuit with a peer modem. Applicable only to the Generic mode of operation.
X				**Encrypted Circuits**: Runs the encryption/decryption operation. Applicable only to Linkway modes of operation.
		X		**Encrypted Circuits and Authentication:** Use HMAC (with SMAT) or ECDSA signature verification (with IA PKC) to authenticate the AES encrypted pipeline. Applicable only to the Generic mode of operation.
X	X			**Set Passphrase:** Sets the Passphrase for use with the SP800-108 KDF (used when creating TEKs). Applicable only to the Linkway modes of operation.
	X			**SMAT Entry & Rollover:** SMAT Entry (may initiate SMAT rollover if a circuit is established). Applicable only to the Generic mode of operation.
X				**Over-The-Air Re-key:** Receives/decrypts or encrypts/sends a new Seed Key**.** Applicable only to Linkway modes of operation.
X				**Over-The-Air Zeroize:** Zeroizes all non-volatile passwords and CSPs, resets the Crypto-Officer password back to default, and resets the hardware. Applicable only to Linkway modes of operation.
X	X			**Message API Zeroize:** Zeroizes all non-volatile passwords and CSPs, resets the Crypto-Officer password back to default, and resets the hardware.
	X			**Enable/Disable Bypass:** Activates/deactivates bypass on Encrypted Circuits service.
X	X			**Change Passwords:** Changes User password and/or Crypto-Officer password. Note that on initialization of the module, the Crypto-Officer must run this service to set up the initial User Password and the User may only change the User password.
X	X			**Load/Manage Cryptographic Material via Message API**: Loads TSKs, Simple PKI Key Material (CA Certificates, CRLs, IA / KE Certificates, and Private Keys).
			X	**Install Firmware Image:** Installs the new firmware image. Note that signature verification of the loaded firmware also authenticates the Vendor role.
			X	**Install Feature File:** Installs the new feature file. Note that signature verification of the loaded feature file also authenticates the Vendor role.

Unauthenticated Services:

The V3K-102 supports the following unauthenticated services:

- **Query Status**: Obtain version number, model information, etc.
- **Self-Tests**: Runs the required FIPS 140-2 self-tests at power-up.
- **Zeroize**: Zeroizes all non-volatile passwords and CSPs, then resets the Crypto-Officer password back to default and resets the hardware. Only available via local physical access.
- **Load Signed Files**: Loads firmware images and/or feature files, for use later by authenticated users (the Vendor role).
- **Power On/Off**: Physically activate the on/off switch.
- **Non-Encrypted Circuits:** If the Crypto Officer has enabled bypass via the Enable/Disable Bypass service, the module can process plaintext data without authentication.

6.2 Definition of Critical Security Parameters (CSPs)

The following Critical Security Parameters (CSPs) are used in the module:

- **Local Unique Key (LUK)**: 256 bit AES key using KW mode. A key used only within the V3K-10x to protect CSPs.
- **Crypto-Officer Password**: Between 8 and 20 numeric characters if entered via the Front Panel or 8 and 20 octets if entered via the Message API used to authenticate the Crypto-Officer role. A default Crypto-Officer password is shipped with the module and reinitialized after the Zeroize, Message API Zeroize or Over-The-Air Zeroize service.
- **User Password**: Between 8 and 20 numeric characters if entered via the Front Panel or 8 and 20 octets if entered via the Message API used to authenticate the User role.
- **PBKDF2 Password**: Used to derive the PBKDF2 KEK. The PBKDF2 Password is between 14 and 128 bytes and is entered alongside PBKDF2 protected Static IA and KE keys.
- **PBKDF2 KEK**: 256 bit AES keys using KW mode. Used to decrypt the PBKDF2 protected keys, which may include the Static IA and KE keys.
- **Passphrase**: 10-32 alpha-numeric characters if entered via the Front Panel or 10-32 octets if entered via the Message API then converted to a 256 bit (via padding, etc.) seed. Used as the XSEED input for the Context input for the SP800-108 KDF. This is used with the input Seed Key to generate TEKs.
- **Traffic Seed Key**: 256 bit seed key. Comes in via the Message API or AES key wrap. Crypto-Officer must be logged in first if the Message API (Load Keys via Message API service) is used. The User role must be logged in first if AES key wrap is used (Over-The-Air Rey-key service). Used as the XKEY input for the K_0 input for the SP800-108 KDF. This is used with the Passphrase input to generate TEKs.

- **Traffic Encryption Keys (TEKs)**: 256 bit AES keys using CTR mode. 32 keys derived using the Passphrase and Seed Key. Each is used for a week at a time and then destroyed.
- **Key Encryption Key (KEK)**: 256 bit AES key using KW mode. Prior to sending/receiving a Seed Key via AES key wrap with the KEK, the Crypto-Officer must load the initial Seed Key.
- **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 Entropy Input**: 41 bytes of random data from the entropy source used as the seed input and another 21 bytes of random data from the entropy source used as the nonce to initialize the Deterministic Random Bit Generator (per NIST SP 800-90A). The entropy source is based on memory-read times and conditioning times. The conditioned data has been evaluated as containing at least 204.551302568 bits of min entropy per 256-bit output block
- **DRBG Internal State**: The internal state of the NIST SP 800-90A CTR DRBG. These are values 128 bit "V" and 256 bit "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:** 256-bit AES key using KW mode. 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:** ECDH 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:** ECDH 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:** 256-bit AES key using KW mode. Used to encrypt private keys filled into the modem. Generated outside of the security boundary.

6.3 Definition of Public Keys

The following public keys and critical settings are used in the module:

- **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).
- **Remote 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.
- **Operator Organization Trust Anchor Public Key**: ECDSA key used to validate the AES key wrapped messages (Over-The-Air Re-key service) and the Over-The-Air

Zeroize service request.

- **Subordinate Operator Organization Public Key:** ECDSA key used to validate the AES key wrapped messages (Over-The-Air Re-key service) and the Over-The-Air Zeroize service request. These are the collection of public keys (contained in X.509v3 certificates) in the path between the Operator Organization Trust Anchor Public Key and the private key (the private key of the "signing certificate") used to sign the message.
- **Viasat Trust Anchor Public Keys**: ECDSA keys used to validate downloaded firmware images and/or feature files.

6.4 Definition of CSPs 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

	CSPs																					
Service	**Crypto Officer Password**	**User Password**	**Passphrase**	**Traffic Seed Key**	**Traffic Encryption Key (TEK)**	**Key Encryption Key (KEK)**	**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**	**PBKDF2 Password**	**PBKDF2 KEK**	**Local Unique Key**
Circuit Establishment	I,U	I,U																				
Encryption									U	U	U	U										
Encrypted Circuits			U	U	U																	
Encrypted Circuits and Authentication	I,U	I,U					U	G,U	E	E	G,O		E,U	U	G,U	U	G,U					
Set Passphrase			I																			
SMAT Entry & Rollover							I,O	G,U										G,U	EU			U
Over-The-Air-Re-key				I,S		I,S																
Over-The-Air-Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Message API Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Enable / Disable Bypass	I,U																					
Change Passwords	I,U,S	I,U,S																				
Load / Manage Cryptographic Material via Message API	U	U	I,S	I,S	I,O,S	I,O,S	I,S	G,U				I		I,U,S		I,U,S		G,U	E,U	I, U	E, U	U
Install Firmware Image																						
Install Feature File																						

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the V3K-102 does not contain a modifiable operational environment.

8 Security Rules

The V3K-102's design corresponds to the following security rules. The security rules are enforced by the module in order to comply with the requirements for FIPS 140-2 Level 2.

1. The cryptographic module shall enforce separation of roles by disallowing a User and a Crypto-Officer from obtaining services at the same time. If a User is logged into the module, and a Crypto-Officer then logs in, the module shall automatically log out the User role. This shall be accomplished through a forced power cycle.
2. The cryptographic module shall support defined roles with a defined set of corresponding services. The defined roles shall be: User, Crypto-Officer, and Vendor.
3. The cryptographic module shall not support a maintenance role or maintenance interface.
4. The purpose, function, service inputs, and service outputs performed by each role shall be defined and appropriately restricted.
5. The cryptographic module shall not support the output of plaintext CSPs.
6. The cryptographic module design shall ensure that unauthenticated services do not provide the ability to modify, disclose, or substitute any module CSPs, use Approved security functions, or otherwise affect module security.
7. The cryptographic module shall support exclusive bypass capabilities. The cryptographic module requires two independent internal actions to enter into the bypass state. Enabling the exclusive bypass mode requires the operator to execute two independent internal actions; both selecting the exclusive bypass mode and then confirming the selection. Any operator shall be able to determine when bypass capability is selected as follows: Bypass status LED indicated on the I^2C Front Panel as well as via the Message API.
8. 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 Crypto-Officer password that shall be changed before any services are allowed.
9. Re-authentication shall be required upon power cycling the module.
10. The cryptographic module shall support role-based authentication for all security relevant services; re-authentication shall be required to change roles.
11. 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.

12. 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.
13. 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. Visible vendor-defined non-security relevant circuitry are excluded from the cryptographic boundary.
14. All cryptographic module data output shall be inhibited when the module is in an error state or during self-tests.
15. Data output shall be logically disconnected from the processes performing key generation, manual key entry, and zeroization. Note that "during key entry, the manually entered values may be temporarily displayed to allow visual verification and to improve accuracy" (FIPS 140-2, page 32).
16. 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.
17. All of the implemented integrated circuits shall be standard quality, production-grade components.
18. The cryptographic module shall contain an opaque tamper evident enclosure.
19. CSPs shall be protected against unauthorized disclosure, modification, and substitution. Public keys and critical settings shall be protected against unauthorized modification and substitution.
20. The cryptographic module shall enforce entity association for all keys that are input to/output from the cryptographic module; entity association shall be enforced for all keys stored within the cryptographic boundary.
21. Key establishment techniques supported by the cryptographic module shall be commercially available as allowed under the requirements of FIPS PUB 140-2 Annex D.
22. The cryptographic module shall provide the ability to zeroize all plaintext CSPs.
23. Power-up self-tests shall not require operator actions. The cryptographic module shall provide an indicator upon successful self-test completion as follows:
    a. Fault Status Output off
24. The cryptographic module shall enter an error state upon failure of any self-test and shall provide an indicator upon failure as follows:
    a. Fault Status Output on
25. 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.
26. The cryptographic module shall perform the self-tests outlined in section 9, Table 7 and Table 8.
27. If a non FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.

9 Self-Tests

The cryptographic module shall support the following self-tests:

Table 7 - Power Up Self-tests

Test Target	Description
AES-256 ECB Encrypt/Decrypt	KATs: separate encryption and decryption tests Modes: ECB Key sizes: 256 bits Cert #**A2329**
AES-256 CTR Encrypt	KATs: EBEM AES CTR Encryption only (because CTR mode utilizes ECB encrypt for both encryption and decryption) Modes: ECB Key sizes: 256 bits Cert #**A2330, #A2331, #A2332**
AES KW	KAT: SP800-38F AES KW, 256-bit Cert #**A2329**
DRBG KAT	KAT: SP800-90A CTR_DRB Cert. #A2336
ECDSA P-384 SHA-384 Signature Generation	KAT: Signature Generation Curves/Key Sizes: P-384 with SHA-384 Cert #**A2333**
ECDSA P-384 SHA-384 Verify	PCT: FIPS 186-4 Signature Verification Curves/Key sizes: P-384 with SHA-384 Cert #**A2333**
ECDSA P-384 SHA-512 Verify	KAT: FIPS 186-4 Signature Verification Curves/Key sizes: P-384 with SHA-512 Cert #**A2333**
FIPS 198-1 HMAC	KATs: FIPS 198-1 Generation, Verification SHA sizes: SHA-384, SHA-512 Cert #**A2334**
SP800-108 KDF	KATs: Key Derivation. Key sizes: 256 bits Cert #**A2339**
ECDH P-384 Shared Secret	KAT: Shared Secret computation Cert #**A2333**
ECDH P-521 Shared Secret	KAT: Shared Secret computation Cert #**A2333**
Concat KDF P-384 SHA-384	KAT: Concatenation KDF Curves/Key Sizes: P-384 with SHA-384 Cert #**A2333**
Concat KDF P-521 SHA-512	KAT: Concatenation KDF Curves/Key Sizes: P-521 with SHA-512 Cert #**A2333**
PBKDF2	KAT: SP800-132 PBKDF2 Cert #**A2337**

SHA-384	KAT: SHA-384 hash verification Cert #**A2338**
SHA-512	KAT: SHA-512 hash verification Cert #**A2338**
SHA3	KAT: SHA3-256 hash verification Cert #**A2335**
Firmware Integrity Test	32-bit EDC performed over all executable code

Table 8 - Conditional Self-tests

Test Target	Description
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation (ephemeral per IG 9.9). Cert #**A2333**
Firmware Load	FIPS 186-4 ECDSA P-521 with SHA-512 signature verification performed when firmware is loaded. Cert #**A2333**
Manual Key Entry	32-bit EDC tests on every manually-entered key.
SP 800-56A Assurances	Pairwise key validation (per IG 9.6) for Ephemeral Unified KAS and One Pass DH KAS. Cert #**A2333**
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).
Entropy Source Health Tests	APT and RCT per SP800-90B (implemented in JEnt).
DRBG Health Tests	SP800-90A Health Tests

10 Physical Security Policy

10.1 Physical Security Mechanisms

The V3K-102 multi-chip embedded cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Production-grade opaque enclosure sealed using epoxy and with tamper evident seals

Two tamper seals are used on both hardware variants of the module and are applied during manufacturing.

10.2 Operator Required Actions

The operator is required to periodically inspect tamper evident seals. Table 9 outlines the recommendations for inspecting/testing physical security mechanisms of the module.

Table 9 - 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.

Figure 2 depicts the tamper seal locations on the V3K-102 with both seals adhering to top of bottom of module at approximately the half-way point on each side.

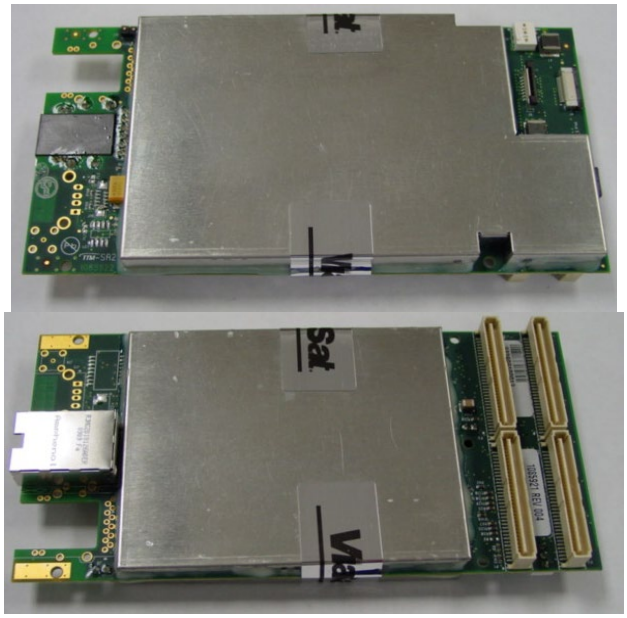

Figure 2– Tamper Seal Placement

10.3 EMI/EMC

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

11 Mitigation of Other Attacks Policy

The V3K-102 has not been designed to mitigate any other attacks outside of the scope of FIPS 140-2.

12 References

FIPS PUB 180-4; National Institute of Standards and Technology, *Secure Hash Standard, Federal Information Processing Standards Publication 180-4, Secure Hash Standard*, August 2015

FIPS PUB 186-4; National Institute of Standards and Technology, *Federal Information Processing Standards Publication 186, Digital Signature Standard,* July 2013

FIPS PUB 197; National Institute of Standards and Technology, *Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES)*, November 6, 2001

FIPS PUB 198-1; National Institute of Standards and Technology, *Federal Information Processing Standards Publication 198-1, The Keyed-Hash Message Authentication Code (HMAC),* July, 2008

NIST SP800-108; National Institute of Standards and Technology, *NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions,* October, 2009

ITU-T Recommendation X.509 (1997 E); *Information Technology - Open Systems Interconnection - The Directory: Authentication Framework,* June 1997

13 Definitions and Acronyms

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CSP	Critical Security Parameter
COMSEC	Communications Security
CRC	Cyclic Redundancy Check
CTR	Counter
DoD	Department of Defense
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EMI	Electro-Magnetic Interference
EMC	Electro-Magnetic Compatibility
FIPS	Federal Information Processing Standard
I^2C	Inter-Integrated Circuit
KAT	Known Answer Test
KEK	Key Encryption Key
LCD	Liquid Crystal Display
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
PCI	Peripheral Component Interconnect
PMC	PCI Mezzanine Card
SHA	Secure Hash Algorithm
TEK	Traffic Encryption Key
TRANSEC	Transmission Security

[i] Hardware revisions occur when items in the Bill Of Materials (BOM) for a product change. This usually occurs because of changes to production test firmware or when components become End-Of-Life (EOL) by the manufacturer and are replaced with manufacturer recommended form, fit and function compatible components.