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

Non-Proprietary Security Policy

Document 1216806 Version 002

October 10, 2022

TABLE OF CONTENTS

1 MODULE OVERVIEW 3

2 SECURITY LEVEL 5

3 MODES OF OPERATION 6

4 **PORTS AND INTERFACES 9**

5 IDENTIFICATION AND AUTHENTICATION POLICY 9

6 ACCESS CONTROL POLICY 10

6.1 ROLES AND SERVICES 10
6.2 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 11
6.3 DEFINITION OF PUBLIC KEYS 12
6.4 DEFINITION OF CSPS MODES OF ACCESS 12

7 OPERATIONAL ENVIRONMENT 13

8 SECURITY RULES 14

9 PHYSICAL SECURITY POLICY 16

9.1 PHYSICAL SECURITY MECHANISMS 16
9.2 OPERATOR REQUIRED ACTIONS 17

10 MITIGATION OF OTHER ATTACKS POLICY 18

11 REFERENCES 19

12 DEFINITIONS AND ACRONYMS 19

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 1.4.2. 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.

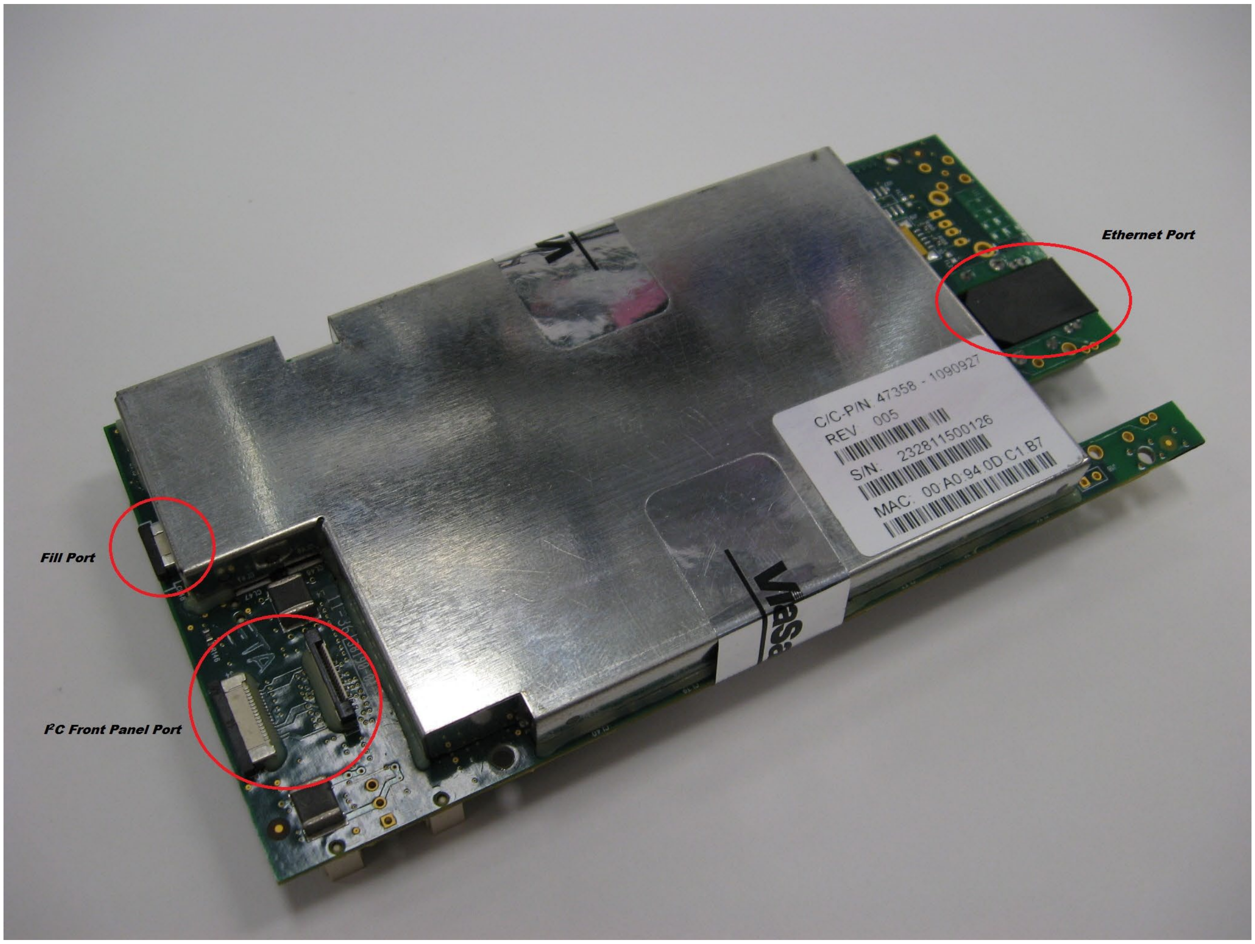

Figure 1-1 Top Side of the 1090927 Cryptographic Module

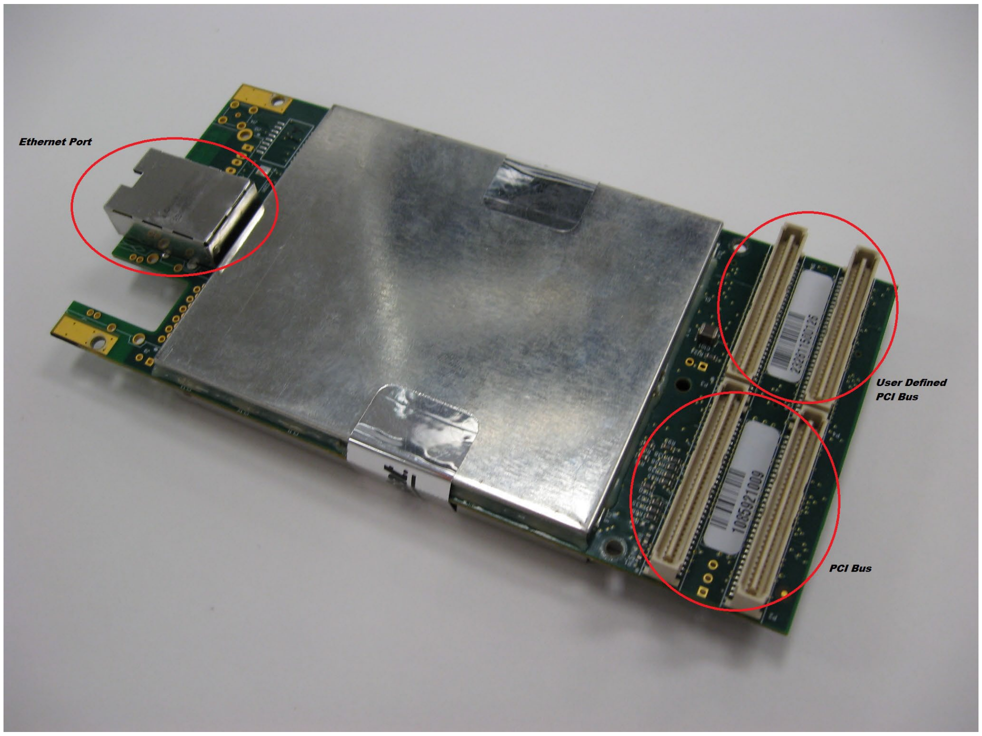

Figure 1-2 Bottom Side of the 1090927 Cryptographic Module

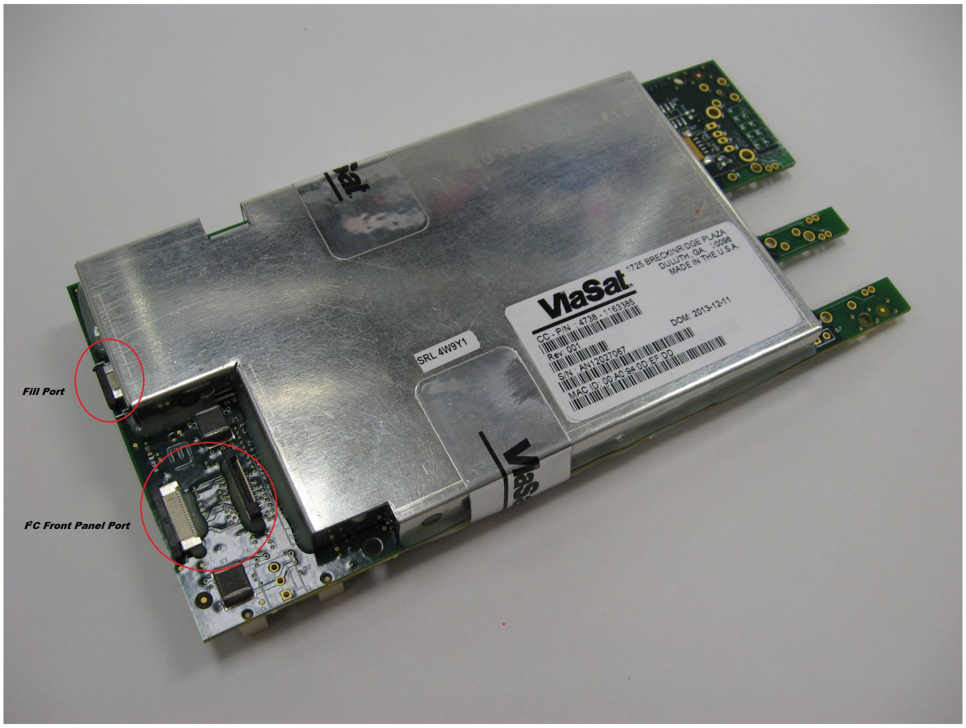

Figure 1-3 Top Side of the 1163385 Cryptographic Module

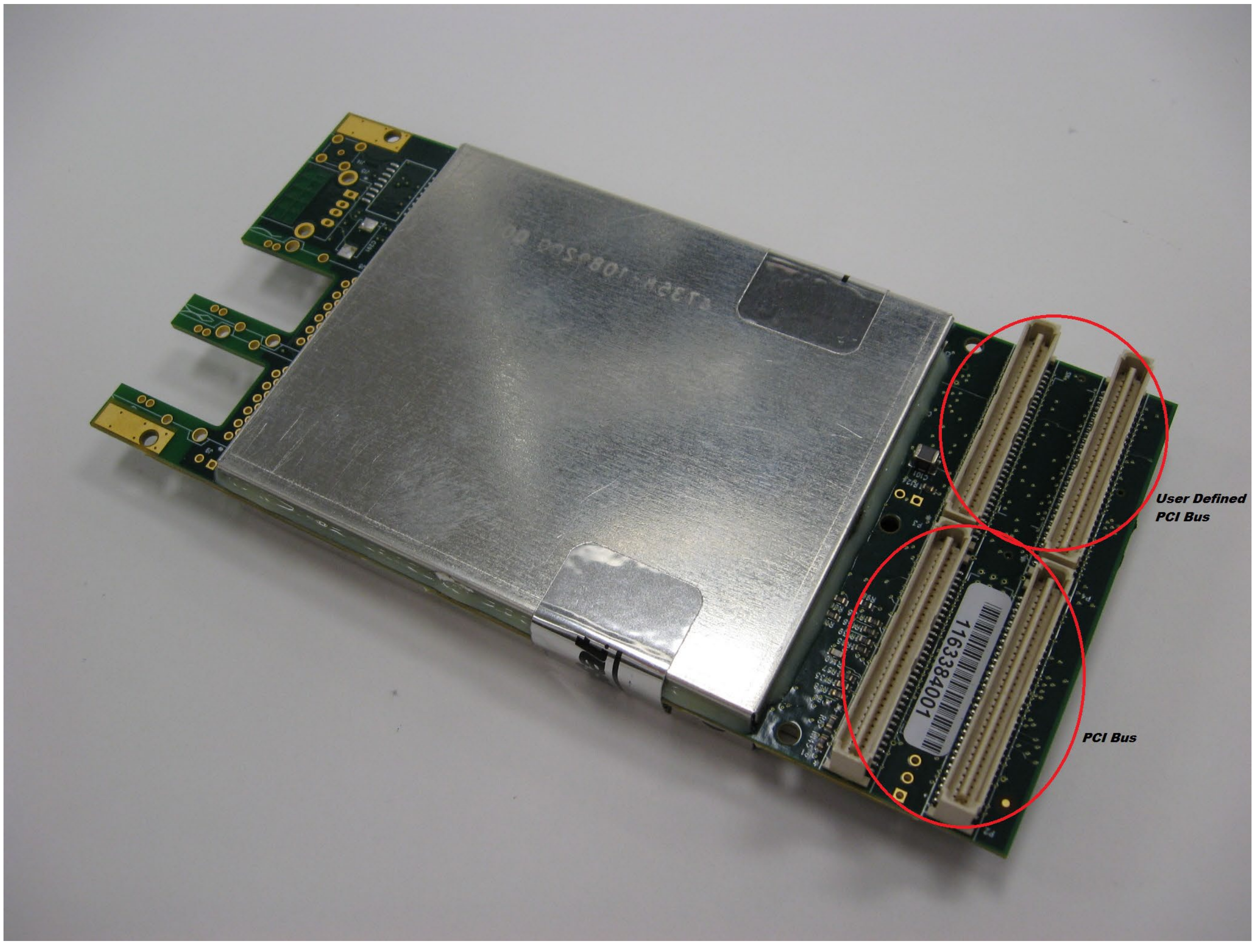

Figure 1-4 Bottom Side of the 1163385 Cryptographic Module

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

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 mode of operation provides the cryptographic capabilities required for the Viasat LinkWay waveform operating on Viasat S2 hardware.
- LinkWay on CBM Hardware
  - This mode of operation provides the cryptographic capabilities required for the Viasat LinkWay waveform operating on Viasat CBM hardware.
- Generic Interface on CBM Hardware
  - This mode of operation provides a waveform-agnostic interface to the V3K-102 cryptographic module operating on Viasat CBM hardware.
  - The “Generic Interface on CBM Hardware” mode does not use AES ECB and CTR modes for encryption within the FPGA, only bypass operation is permitted. In this mode, the V3K-102 is used to validate image integrity and provide red-black separation within the modem.

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_LWS2-1.4.0	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 sizes: 256 bits	A2235
AES_CTR_LWCBM-1.4.0	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 sizes: 256 bits	A2236
AESUtils-1.4.0	AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption (in Processor for CSPs) Modes: ECB Key sizes: 256 bits	A2230
	Key Wrap	[SP 800-38F] Functions: Wrap, Unwrap Key sizes: 256 bits	A2230
EcDSAUtils-1.4.0	ECDSA	[FIPS 186-4] Functions: Signature Verification (for firmware images, and feature files) Curves/SHA sizes: P-384 with SHA-384 or SHA-512	A2231
FIPS198-1.4.0	HMAC	[FIPS 198-1] Functions: Generation, Verification Minimum key length: 112 bits SHA sizes: SHA-384	A2232

Algorithm Implementation	**Algorithm**	**Description**	**CAVP Cert. #**
SP800_108-1.4.0	KBKDF	[SP800-108] Functions: Key Derivation Function in Counter Mode HMAC: HMAC-SHA384	A2234
KTS	AES-KW	Key establishment methodology provides 256-bits of encryption strength	A2230
SHAUtils-1.4.0	SHS	[FIPS 180-4] Functions: Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-384, and SHA-512	A2233

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^{2}C 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 2 lists the supported operator roles along with their required identification and authentication techniques. Table 3 outlines each authentication mechanism and the associated strengths.

Table 3 - Roles and Required Identification and Authentication

Role	**Type of Authentication**	**Authentication Data**
User	Role-based operator authentication	Password
Crypto-Officer (Admin)	Role-based operator authentication	Password
Vendor	Role-based operator authentication	ECDSA authentication

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.
ECDSA authentication	Using the V3K-102's ECDSA implementation, the probability that a random attempt will succeed is the strength of the embedded SHA-384 function: $1/2^{192}$, which is less than 1/1,000,000. 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 4 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)	Vendor	
X			**Encrypted Circuits**: Runs the encryption/decryption operation.

X	X		**Set Passphrase:** Sets the Passphrase for use with the SP800-108 KDF (used when creating TEKs).
X			**Over-The-Air Re-key:** Receives/decrypts or encrypts/sends a new Seed Key using a KEK with AES-KW**.**
X			**Over-The-Air Zeroize:** Zeroizes all non-volatile passwords and CSPs, resets the Crypto-Officer password back to default, and resets the hardware.
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		**Load Keys via Message API**: Loads between one and four Seed Keys for use with the SP800-108 KDF (used when creating TEKs).
		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:

- **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.

- **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 (SP800-108 Context) 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 (SP800-108 Key Derivation 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-CTR keys. 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-KW key. The KEK is derived from the TSK and Passphrase using SP800-108 KBKDF. Prior to sending/receiving a Seed Key via AES key wrap with the KEK, the Crypto-Officer must load the initial Seed Key.

6.3 Definition of Public Keys

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

- **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.
- **Vendor 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 5 defines the relationship between access to CSPs and the different module services. The types of access used in the table are Generate (G), Read (R), Write (W), and Zeroize (Z).

Table 6 - CSP and Public Key Access Rights within Services

	Crypto-Officer Password	User Password	Passphrase	Traffic Seed Key	Traffic Encryption Key (TEK)	Key Encryption Key (KEK)	Operator Organization Trust Anchor Public Key	Subordinate Operator Organization Public Key	Vendor Trust Anchor Public Key
Encrypted Circuits			R	R	R				
Set Passphrase			W						
Over-The-Air Re-key				W		R, W	R	R	
Over-The-Air Zeroize	Z	Z	Z	Z	Z	Z	R, Z	R, Z	
Enable/Disable Bypass									
Change Passwords	W	W							
Load Keys via Message API				W					
Install Firmware Image							W	W	R, W
Install Feature File									R
Show Status									
Self-Tests									
Zeroize	Z, W	Z	Z	Z	Z	Z	Z	Z	
Load Signed Files									
Power On/Off									
Non-Encrypted Circuits									

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. The Vendor role is distinct from the others in that it requires the Vendor Trust anchor Private Key, which is not available to any other roles; no other roles have access to Vendor role services.
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 following self-tests:
    a. <u>Power Up Self-Tests:</u>
        i. Cryptographic Algorithm Tests:
            (1) AES-256 ECB Encrypt/Decrypt KATs (Known Answer Test) (Cert. #**A2230**)

(2) AES-256 CTR Encrypt KAT (Cert. #**A2235**, **#A2236**)

(3) AES-256 KW Wrap/Unwrap KAT (Cert #**A2230**)

(4) ECDSA P-384 SHA-384 Verify KAT (Cert #**A2231**)

(5) ECDSA P-384 SHA-512 Verify KAT (Cert #**A2231**)

(6) HMAC-SHA-384 KAT (Cert #**A2232**)

(7) SP800-108 KBKDF KAT (Cert #**A2234**)

(8) SHA-384 KAT (Cert #**A2233**)

(9) SHA-512 KAT (Cert #**A2233**)

ii. Firmware Integrity Test: Performed on all executable code using a 32-bit Error Detection Code (EDC)

b. <u>Conditional Self-Tests:</u>

i. Firmware Load Test: ECDSA signature verification (Cert #**A2231**)

ii. Manual Key Entry Tests: 32-bit EDCs

iii. Exclusive Bypass Test: Verifies which mode (Bypass or Encryption) the module is in by checking flag values which are stored in non-volatile memory and whose integrity is verified by a 32-bit EDC (CRC).

iv. Critical Functions Tests:

(1) CSP I/O Continuous Test: Verifies the CSP storage access

(2) AES Counter Value Continuous Test: Verifies that the current counter value in the FPGA AES implementation is greater than the previous counter value.

27. If a non FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.

9 Physical Security Policy

9.1 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.

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).

9.2 Operator Required Actions

The operator is required to periodically inspect tamper evident seals. Table 6 outlines the recommendations for inspecting/testing physical security mechanisms of the module.

Table 7 - 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.

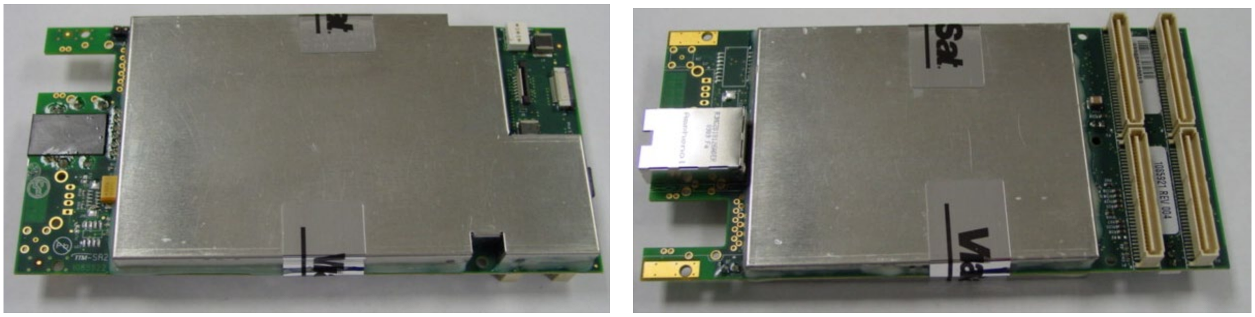

Figure 2– Tamper Seal Placement

10 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.

11 References

FIPS PUB 180-4; National Institute of Standards and Technology, *Secure Hash Standard, Federal Information Processing Standards Publication 180-4, Secure Hash Standard*, March, 2012

FIPS PUB 186-2; National Institute of Standards and Technology, *Federal Information Processing Standards Publication 186, Digital Signature Standard,* October 5, 2001

FIPS PUB 197; National Institute of Standards and Technology, *Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES)*, March 6, 2002

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

ANSI X9.31 – 1998; American National Standard for Financial Services, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA,)* September 9, 1998

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

12 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.