VT iDirect, Inc.

TRANSEC Module

Hardware Part Number: E0002268
Firmware Version: Cloak 1.0.2.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 3
Document Version: 0.10

Prepared for:

VT iDirect, Inc.
13861 Sunrise Valley Drive
Suite 300
Herndon, VA 20171
United States of America

Phone: +1 866 345 0983
www.idirect.net

Prepared by:

Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the TRANSEC[1] Module from VT iDirect, Inc. (iDirect). This Security Policy describes how the TRANSEC Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. [2]and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 3 FIPS 140-2 validation of the module. The TRANSEC Module is also referred to in this document as “crypto module” or “module”.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The iDirect website (http://www.idirect.net/) contains information on the full line of products from VT iDirect, Inc.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals responsible for answering technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is organized into two (2) primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional areas of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions, management methods, and usage policies.

[1] TRANSEC – Transmission Security
[2] U.S. – United States

2. TRANSEC Module

2.1 Overview

VT iDirect, Inc.'s satellite-based IP[3] communications technology enables constant connectivity for voice, video, and data applications in any environment. iDirect provides the leading TRANSEC-compliant, bandwidth-efficient satellite platforms for government and military communications. The Secure Satellite Broadband Solutions have uses across a wide range of applications, including maritime connectivity, aeronautical connectivity, military defense, and emergency relief.

iDirect's Secure Satellite Broadband Solutions supports a Time Division Multiple Access (TDMA) upstream carrier and DVB-S2[4] downstream carrier. The iDirect network is optimized for satellite transmissions, obtaining the maximum performance out of satellite bandwidth. The system is fully integrated with iDirect's Network Management System, which provides configuration and monitoring functions. The iDirect network components consist of the Network Management Server, a Protocol Processor, a hub line card, and the Ethernet switch with remote modem. In a star topology, the Protocol Processor acts as the central network controller, the hub line card is responsible for the hub side modulation and demodulation (modem) functions, and the remote modem provides modem functionalities along with the Ethernet switch. A common deployment of the iDirect network components is shown in Figure 1 below.

[3] IP – Internet Protocol

[4] DVB-S2 – Digital Video Broadcast - Satellite - Second Generation

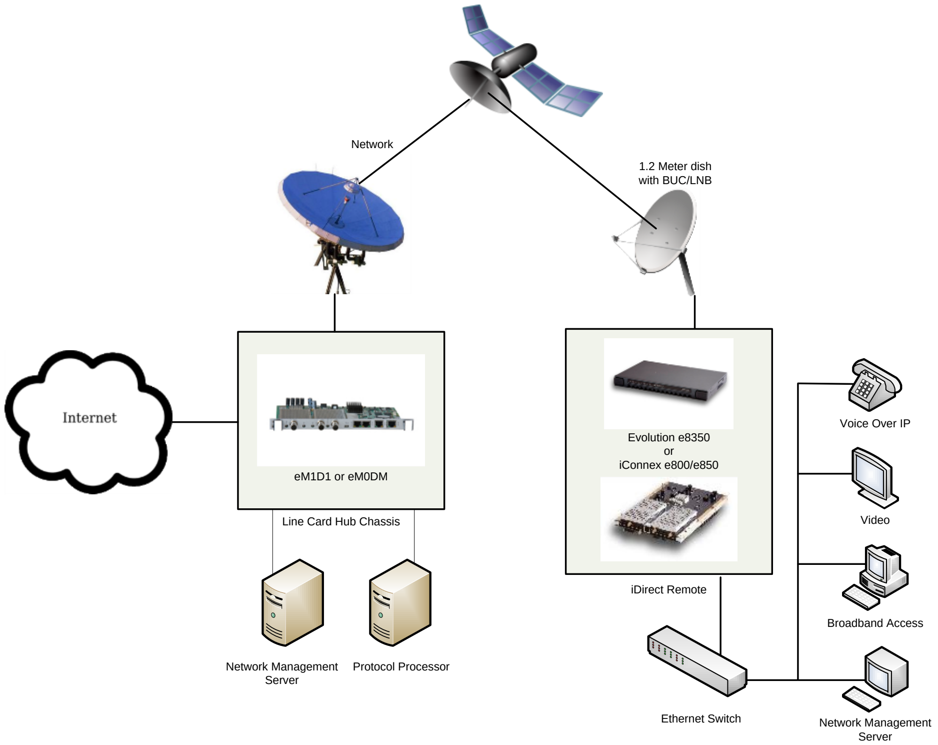

Figure 1 – iDirect Network Deployment

The iDirect TRANSEC Module will provide the cryptographic functionality necessary to secure information going through the network. The TRANSEC Module is a 5.08cm[5] x 5.08cm daughter card (P/N[6]: E0002268) that is installed on the motherboard of a hub line card or a remote modem with unique firmware (version Cloak 1.0.2.0). Each TRANSEC Module can be configured to have a primary and secondary security domain. Each security domain will have its own keys and CSPs[7] to ensure data is sent securely across the network. Packages containing data and control messages are sent across the network between the hub line card and the remote.

The TRANSEC Module is a multi-chip embedded cryptographic module, per FIPS 140-2 terminology. The module is a daughter card with production grade components covered in conformal coating that is opaque within the visible spectrum. Figure 2 and Figure 3 below show the front and back view (respectively) of the TRANSEC Module.

[5] cm – Centimeter
[6] P/N – Part Number
[7] CSP – Critical Security Parameter

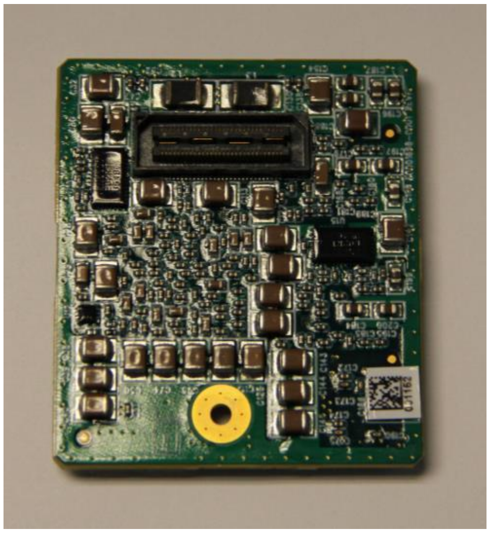

Figure 2 – TRANSEC Module – Front View

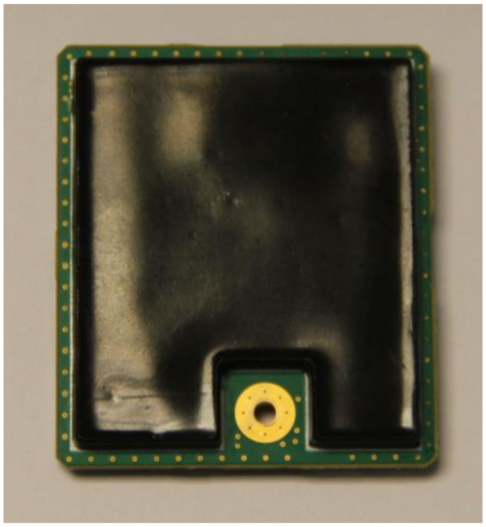

Figure 3 – TRANSEC Module – Back View

Please note that all components visible from the front view of the module are non-security-relevant. These are components such as the module power supply, decoupling capacitors, voltage rails monitoring device, voltage discharge transistors, and the module connector. None of these components actively participate in the performance of cryptographic functions or processing of sensitive data. Additionally, the identifying marks on each component are individually covered with an opaque material under (or as part of) the coating to mitigate identification. Finally, there are no visible/exposed circuit traces. Thus, this view provides nothing that one could ascertain visually that could be exploited to compromise the security of the module.

The TRANSEC Module is validated at the FIPS 140-2 Section levels shown in Table 1 below.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A[8]
7	Cryptographic Key Management	3
8	EMI/EMC[9]	3
9	Self-tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The TRANSEC Module is a hardware module with a multiple-chip embedded embodiment. The overall security level of the module is 3. The cryptographic boundary of the TRANSEC Module is a 5.08cm x 5.08cm daughter card (P/N[10]: E0002268) embedded on the motherboard of a host line card or remote modem. The daughter card contains the following components:

- An Altera Cyclone V FPGA[11] for running the module firmware. This is the primary cryptographic engine of the TRANSEC Module. The LVDS[12] Bus and Local Bus interfaces are integrated into the FPGA.
- 512Mb[13] flash memory for firmware storage. The flash memory is used to store keys, certificates, and passwords as defined in VE07.03.01.
- 4Gb[14] DDR3L[15] RAM[16] for storing keys.
- TPM cryptographic controller for generating entropy for the FIPS-Approved DRBG[17] used in the generation of ECDSA[18] keys.

Figure 4 below shows the functional block diagram of the TRANSEC Module and its interfaces. The cryptographic boundary is indicated by the red dotted line. The following acronyms are in Figure 4 below and have not been previously defined:

[8] N/A – Not Applicable
[9] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[10] P/N – Part Number
[11] FPGA – Field-Programmable Gate Array
[12] LVDS – Low-Voltage Differential Signaling
[13] Mb – Megabits
[14] Gb – Gigabits
[15] DDR3L – Double Data Rate Type Three Low-Voltage
[16] RAM – Random Access Memory
[17] DRBG – Deterministic Random Bit Generator
[18] ECDSA – Elliptic Curve Digital Signature Algorithm

- ATDMA – Adaptive Time Division Multiple Access
- RBG – Random Bit Generator

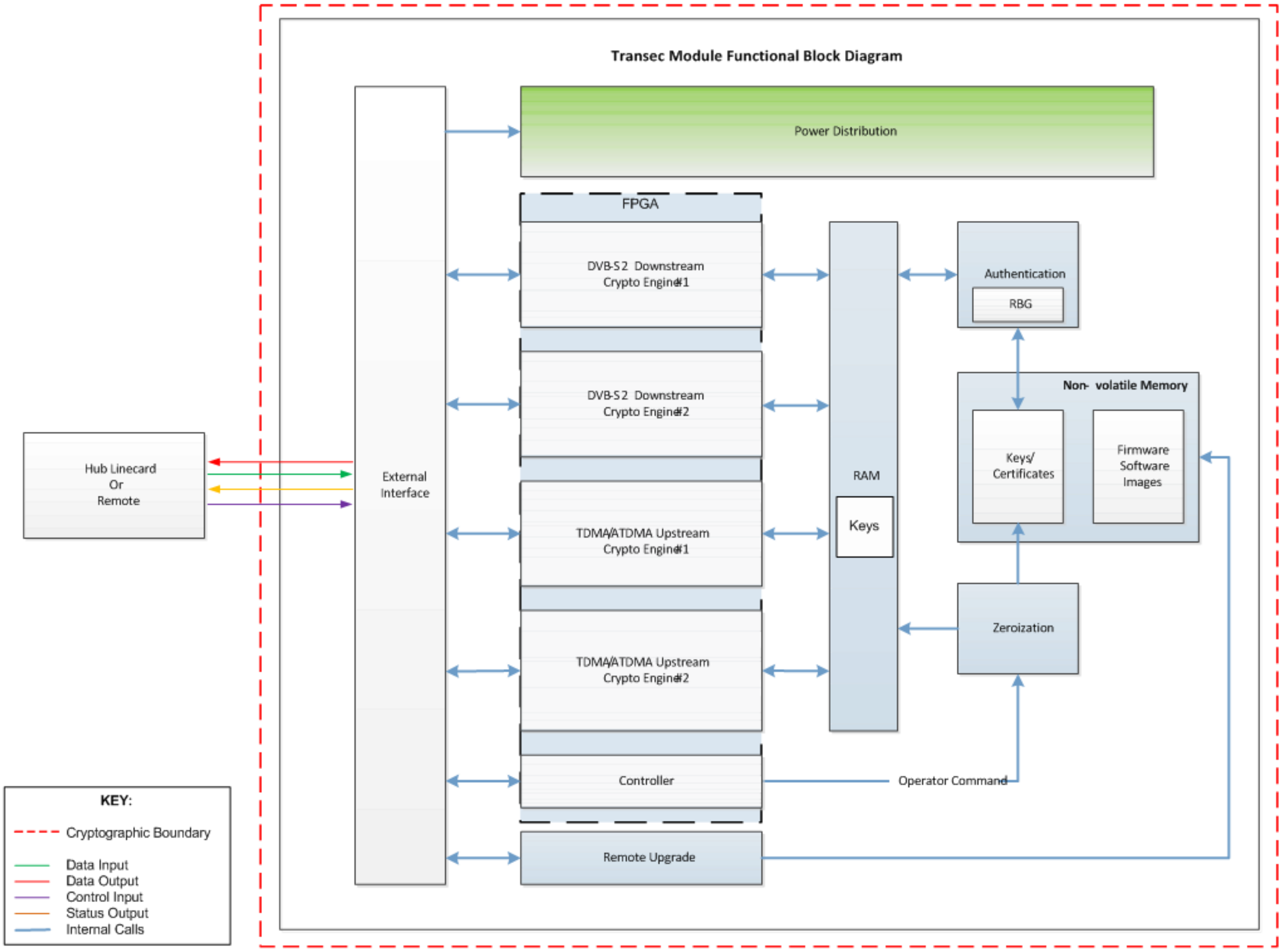

Figure 4 – TRANSEC Module Block Diagram

The module firmware implements the FIPS-Approved algorithms listed in Table 2 below.

Table 2 – FIPS-Approved Firmware Algorithm Implementations

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
#4509	AES[19]	FIPS PUB 197	CBC[20]	256-bit	encryption/decryption

[19] AES – Advance Encryption Standard
[20] CBC – Cipher Block Chaining

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
#121	KAS[21]	NIST SP[22] 800-56A	ECC[23] CDH[24]	NIST-defined curve (P-256)	key agreement
#1096	ECDSA	FIPS PUB 186-4	PKG, Sig Gen, Sig Ver	NIST-defined curve (P-256)	key pair generation, signature generation, signature verification
#3698	SHS[25]	FIPS PUB 180-3	SHA[26] -256, SHA-512	-	message digest
#1473	DRBG	NIST SP 800-90A	Hash-based	-	deterministic random bit generation
#2457	RSA[27]	FIPS PUB 186-4	PKCS[28] #1 v1.5 Signature Verification	2048-bits	digital signature verification

The module FPGA implements the FIPS-Approved algorithms listed in Table 3 below.

Table 3 – FIPS-Approved FPGA Algorithm Implementations

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
#4510	AES	FIPS PUB 197	CBC	256-bit	encryption/decryption

The TRANSEC Module implements the following non-Approved but allowed security functions:

- NDRNG[29] for seeding the DRBG
- AES (Cert. #4509, key unwrapping; key establishment methodology provides 256 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)

[21] KAS – Key Agreement Scheme
[22] SP – Special Publication
[23] ECC – Elliptic Curve Cryptography
[24] CDH – Cofactor Diffie Hellman
[25] SHS – Secure Hash Standard
[26] SHA – Secure Hash Algorithm
[27] RSA – Rivest Shamir and Adleman
[28] PKCS – Public Key Cryptography Standard
[29] NDRNG – Non-Deterministic Random Number Generator

2.3 Module Interfaces

The module's design separates the physical ports into four logically distinct and isolated categories. They are:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

In addition, the module supports a Power Input interface.

The cryptographic boundary of the TRANSEC Module is the daughter card. Figure 4 above is a block diagram of the module that shows the physical interfaces between the TRANSEC Module and the motherboard. The TRANSEC Module plugs directly into the motherboard through the TRANSEC Module Connector. The TRANSEC Module Connector is a 64-pin physical interface that plugs directly into the motherboard of a remote or hub line card. Figure 5 and Figure 6 below show the TRANSEC Module Connector.

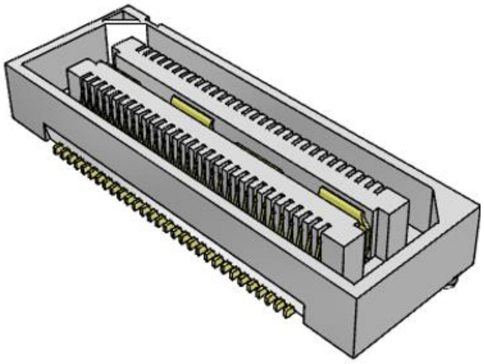

Figure 5 – TRANSEC Module Connector

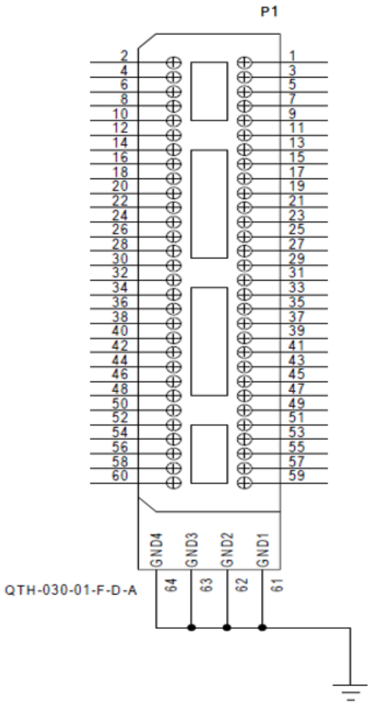

Figure 6 – TRANSEC Module Connector Pin Assignments

Table 4 below provides a mapping of each TRANSEC Module physical interface to the equivalent logical interface.

Table 4 – Physical Interface to Logical Interface Mapping

FIPS 140-2 Logical Interface	Physical Module Interface
Data Input Interface	TRANSEC Module Connector (Pin assignments: 2, 4, 8, 10, 14, 16, 20, 22, 58, 60)
Data Output Interface	TRANSEC Module Connector (Pin assignments: 1, 3, 7, 9, 13, 15, 19, 21, 57, 59)
Control Input Interface	TRANSEC Module Connector (Pin assignments: 5, 29 – 55)
Status Output Interface	TRANSEC Module Connector (Pin assignments: 17)
Power Interface	TRANSEC Module Connector (Pin assignments: 6, 12, 23, 27)

The TRANSEC Module utilizes the I/O pins to perform the following control functions

- Pin 5 (Zeroize) – the signal for the zeroize pin is connected to an external push button. Once the correct pin sequence has been applied, all keys and CSPs are zeroized from the module.
- Pin 53 (RESET) – resets the TRANSEC Module during start-up and for recovery from a critical error state. The RESET will reset all firmware registers and reboot the module.
- Pin 55 (NCONFIG) – causes the FPGA to reload the module.

2.4 Roles, Services, and Authentication

The paragraphs below describe the authorized operator roles and authentication methods supported by the module, as well as the services available to module operators.

2.4.1 Roles and Authenticated Services

The host motherboard is the single operator of the module; however, there are two unique identities (or "roles") that it uses to access module services: CO and User. To perform a given service, the host motherboard sends a message with the username and password for the authorized role being assumed. Using this mechanism, each role is explicitly assumed at each service call.

Table 5 below provides a mapping from each service to the role that is authorized to perform it. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 5 – Mapping of Services to Inputs, Outputs, Roles, CSPs, and Type of Access

Service	Description	Input	Output	Operator		Key/CSP and Type of Access
				CO	User	
Update query	This message returns information about each firmware package on the TRANSEC Module.	Command	Installation information	✓	✓	User Password – X
Update install	This message stores a firmware package in flash memory.	Command	Status	✓		CO Password – X
Update uninstall	This message works like a deletion. The item identified in the command will be deleted from flash memory.	Command	Status	✓		CO Password – X
Update activate	This message marks an item as active. Only one firmware package can be active at a time. The active firmware package is the one that will be loaded by the bootloader.	Command	Status	✓		CO Password – X

Service	Description	Input	Output	Operator		Key/CSP and Type of Access
				CO	User	
Query factory information	This message retrieves factory default information.	Command	Factory default informatio n	✓	✓	User Password – X
Device status	This message returns the status of the device.	Command	Status	✓	✓	User Password – X
Firmware load	This message executes the firmware integrity check when the module is loaded	Command	Status	✓		CO Password – X iDirect Signed Key –- R
Get date and time	This message returns the date and time for the security domain identified.	Command	Date/time	✓	✓	User Password – X
Get channel configuration	This message returns channel configuration data.	Command	Status	✓	✓	User Password – X
Set channel configuration	This message configures a channel for encryption or decryption. Note that the security domain must be specified to allow the TRANSEC Module to select the correct stored ACC[30] key and to properly validate the key roll and other messages.	Command	Status	✓		CO Password – X
Key validity query	This message queries the state of the cryptographic keying information.	Command	Status	✓	✓	User Password –X
Channel statistics	This message requests channel statistics.	Command	Status	✓	✓	User Password – X ACC Key – R DCC[31] Key – R

[30] ACC – Acquisition Ciphertext Channel

[31] DCC – Dynamic Ciphertext Channel

Service	Description	Input	Output	Operator		Key/CSP and Type of Access
				CO	User	
V3[32] keyroll	This message is sent by the PP[33] to the TRANSEC Module containing either ACC or DCC keys.	Command	Status	✓		CO Password – X EC DH shared secret –W, X Key 1 – W, X Key 2 – W, X ECDSA private key – RR RSA public key – RR ACC Key – W DCC Key – W
One way ECC keyroll	This message specifies whether the ACC or DCC key is to be loaded and where the key is to be loaded.	Command	Status	✓		CO Password – X EC DH shared secret –W, X Key 1 – W, X Key 2 – W, X ECDSA private key – R RSA public key – RR ACC Key – W DCC Key - W
Get certificates	This message retrieves an x.509 certificate from the TRANSEC Module.	Command	Status	✓		CO password – X Certificate issued by the iDirect Certificate Authority (CA) Foundry – R
Add certificates	This message adds one or more certificates to storage.	Command	Status	✓		CO password – X Certificate issued by the iDirect CA Foundry – W
Clear certificates	This message clears all certificates of a given type from storage.	Command	Status	✓		CO Password – X Certificate issued by the iDirect CA Foundry– W
Certificate signing request	This message instructs the TRANSEC Module to discard its current ECDSA keypair and to generate a new ECDSA keypair.	Command	Status	✓		CO Password – X ECDSA private key – X, W ECDSA public key – X, W
Certificate query	This message returns the appropriate certificate.	Command	Status	✓	✓	User Password – X Certificate issued by the iDirect CA Foundry – R
Zeroize	This message zeroizes all keys and CSPs in the module.	Command	Status	✓		All CSPs – W

[32] V3 – iDirect's third version of over-the-air messaging
[33] PP – Protocol Processor

2.4.2 Authentication

The module supports identity-based authentication. A unique username and password is sent in with each message from the host motherboard to indicate the entity performing the service. The unique username and password identifies the identity performing the service. Authentication information is not persisted between services. A new username and password is sent each time a service is to be performed.

The password is eight characters in length and is comprised of any combination of U.S.[34]-printable ASCII[35] characters. The password is generated in the factory and hardcoded in flash memory. When a message is received, the password in the message is authenticated with the password stored in flash memory. The probability for guessing an 8-character password that can use 94 different characters is 1 in 94^8 = 1 in 6,095,689,385,410,816. This is less than the required probability.

2.4.3 Unauthenticated Services

The module provides services that do not require authentication (see Table 6 below). These services do not require a host motherboard message with an associated username/password. The available services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the overall security of the module.

Table 6 – Mapping of Unauthenticated Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	Type of Access
Traffic throughput	Secured traffic throughput at the data-link layer	Data Link layer packet	Data Link layer packet	DCC Key – R ACC Key –- R
On-Demand Self-Tests	Zeroizes keys and CSPs via power cycle	Command	Status	All CSPs – W

2.5 Physical Security

The cryptographic module is a multi-chip embedded cryptographic module per FIPS 140-2 terminology. The module is a daughter card with conformal coating covering all components and screws on the card. The conformal coating protects the module from tampering. Any tampering will damage the module and make it inoperable. The conformal coating is opaque within the visible spectrum.

2.6 Operational Environment

The module's firmware, TRANSEC Module version Cloak 1.0.2.0, runs on an Altera Cyclone V FPGA. The FPGA operating system protects memory and process space from unauthorized access. The firmware integrity test protects against unauthorized modification of the module.

[34] U.S. – United States

[35] ASCII – American Standard Code for Information Interchange

2.7 Cryptographic Key Management

The module supports the keys and CSPs listed in Table 7 below.

Table 7 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
ACC Key	AES-256 CBC key	Externally generated, entered electronically in encrypted form	Never exits the module	Plaintext in flash; plaintext in volatile memory	Zeroize control message	Encrypt all traffic and traffic headers required for a remote to acquire the network
Certificates issued by the iDirect CA Foundry	X.509 digital certificates	Externally generated, entered in plaintext form	Exits in plaintext form	Plaintext in flash memory	Zeroize control message	Validate signature verification of keyroll and set date/time
DCC Key	AES-256 CBC key	Externally generated, entered electronically in encrypted form	Never exits the module	Plaintext in volatile memory	Zeroize control message	Encrypt all user traffic and traffic headers
EC DH shared secret	256-bit shared secret	Internally generated	Never exits the module	Plaintext in volatile memory	Zeroized after service completes	Input to EC DH key derivation function
ECDSA private key	256-bit DH private exponent	Internally generated	Never exits the module	Plaintext in flash memory	Zeroize control message	Create the EC DH shared secret
ECDSA public key	256-bit DH public exponent	Internally generated	Exits electronically in plaintext form	Plaintext in volatile memory	Zeroize control message	Create the EC DH shared secret; verify certificates issued by the iDirect CA Foundry
Key 1	AES 256-bit key	Key agreement	Never exits the module	Plaintext in volatile memory	Zeroized after service completes	Decrypt Key 2
Key 2	AES 256-bit key	Externally generated, entered electronically in encrypted form	Never exits the module	Plaintext in volatile memory	Zeroized after service completes	Decrypt ACC and DCC key
iDirect Signed Key	RSA 2048-bit public key	Externally generated, hard coded in flash at the factory	Never exists the module	Plaintext in flash memory	Never zeroized	Validate firmware integrity upon firmware load
RSA public key	RSA 2048-bit public key	Externally generated, entered electronically in plaintext form	Never exists the module	Plaintext in flash memory	Never zeroized	Validate keyroll messages

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG Seed	Random data – 256 bits	Internally generated	Never exits the module	Not persistently stored by the module	Module reset or power-down	Seeding material for SP 800-90A DRBG
DRBG Entropy[36]	Random data – 128 bits	Internally generated	Never exits the module	Plaintext in volatile memory	Module reset or power-down	Entropy material for SP 800-90A DRBG
DRBG 'V' Value	Internal state value	Internally generated	Never exits the module	Plaintext in volatile memory	Module reset or power-down	Used for Hash_DRBG
Crypto-Officer Password	Password	Externally generated, pre-loaded at the factory	Never exits the module	Hardcoded in plaintext in flash memory	Never zeroized	Authenticate the Crypto-Officer role
User Password	Password	Externally generated, pre-loaded at the factory	Never exits the module	Hardcoded in plaintext in flash memory	Never zeroized	Authenticate the User role

[36] The module generates 279 bits of entropy for use in key generation.

2.8 EMI / EMC

The TRANSEC Module was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (home use).

2.9 Self-Tests

Cryptographic self-tests are performed by the module when the module is first powered up and loaded into memory as well as when a random number or asymmetric key pair is created. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

Once the module is loaded from flash memory into the FPGA, the TRANSEC Module performs the following power-up self-tests:

- Firmware integrity test – RSA digital signature verification
- Known Answer Tests (KATs)
    - AES-CBC encrypt KAT (firmware)
    - AES-CBC decrypt KAT (firmware)
    - AES-CBC encrypt KAT (FPGA)
    - AES-CBC decrypt KAT (FPGA)
    - SHA-256 KAT
    - SHA-512 KAT
    - RSA Signature Verification KAT
    - DRBG KAT
    - Primitive "Z" Computation KAT

2.9.2 Conditional Self-Tests

Conditional self-tests are performed from the operational state of the TRANSEC Module. These tests are executed when a specific condition is met. The TRANSEC Module performs the following conditional self-tests:

- Firmware Load Test
- Continuous Random Number Generator Test for SP800-90 DRBG
- Continuous Random Number Generator Test for non-Approved PRNG
- ECDSA pairwise consistency check

2.9.3 Critical Functions Self-Tests

The TRANSEC Module performs the following critical function tests at module power-up:

- DRBG Instantiate
- DRBG Uninstantiate

- DRBG Generate

2.9.4 Error States and Recovery

If the Firmware Load Test fails, the firmware load process is aborted; however, no module halts or restarts are required to clear the error state. This is a transient error state; once the module enters this state and sends a status message of the error, then the error state is automatically cleared and the module returns to its previous operational state. The module will continue to run using the previously-loaded image.

If the module fails any of the other self-tests (power-up, conditional, or critical function), then the module enters a critical error state. In this state, limited services may be performed to install a new firmware image into a non-active partition of the flash memory. Once installed, the non-active partition must be marked "active". On the next reboot, the error state will be cleared, the module will load the newly-loaded firmware image. Upon successful completion of the power-up self-tests, the module will enter a fully operational state. If the condition persists through multiple reboots, the module must be serviced by iDirect.

All cryptographic operations and data output are prohibited in error states.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 3 requirements for this validation.

3. Secure Operation

The sections below describe how to place and keep the module in the FIPS-Approved mode of operation.

3.1 Initial Setup

The TRANSEC Module is installed at the factory on the motherboard of the host. It is delivered to the field with factory-loaded firmware that is used to install and activate the TRANSEC Module firmware (version Cloak 1.0.2.0). The module must be initialized and configured prior to being able to send data between the host and the remote.

3.1.1 Initialization

The following steps are to be followed to install and activate the TRANSEC Module firmware (version Cloak 1.0.2.0):

1. The operator powers on the host and TRANSEC Module. The motherboard of the host and the TRANSEC Module daughter card come up at the same time.
2. The factory image from partition 0 loads.
3. The operator sends the “update install” message indicating that the TRANSEC Module firmware (version Cloak 1.0.2.0) is to be loaded into partition 1.
4. The operator sends the “update activate” message indicating that the firmware installed in partition 1 is to be marked “active”.
5. The operator reboots the host, which will reboot the TRANSEC Module.
6. After reboot, the module automatically loads the firmware activated in Step 4 and performs the firmware integrity check using the iDirect Signed Key for RSA signature verification.
7. Once the firmware is verified and loaded, the power-up self-tests automatically execute.

Upon successful completion of the power-up self-tests, the module automatically enters its FIPS-Approved mode of operation. No data will be sent between the hub line card and remote until all configuration steps have been executed. The module remains in a FIPS-Approved mode until the “zeroize primary” message is sent and executed.

For further instructions on installing and configuring the iDirect TRANSEC Module, please refer to the *iDirect TRANSEC Module Users Guide*.

3.2 Secure Management

Once the module is in FIPS-Approved mode, a “heartbeat” is sent from the TRANSEC Module to the host application indicating that the module is functional. If there is a disruption in the heartbeat, then the TRANSEC Module will reboot.

3.2.1 Monitoring Status

The CO and User manually monitor the status of the TRANSEC Module through various status request messages. See Table 5 above for a list of services used to query the status of the TRANSEC Module.

3.2.2 Zeroization

The module can be zeroized by physically pushing the zeroize I/O pin, which activates the "zeroize primary" service, or sending the "zeroize primary" message from the host to the module. The I/O zeroize pin must be pushed three times to confirm that the zeroize action is to take place. If the sequence of pin pushes is not completed, then the zeroize command is aborted and the module remains in a FIPS-Approved mode of operation.

If the module receives the "zeroize primary" message from the host, then a receipt is immediately sent back to the host to confirm that the command was received. The zeroize sequence will be executed once the configured elapsed time has occurred (0 – 15 seconds). This elapsed time is supported to allow for confirmation of the request to be sent back to the host and for the prior service to be completed.

The "zeroize primary" message zeroizes all keys and CSPs in the primary and secondary security domain.

3.2.3 Loading New Firmware

To load a new firmware image, the "update install" message is first sent from the host to the module with the new firmware image to be installed into partition 1 or 2. If both partitions are full, then the firmware in the non-active partition must be uninstalled by sending the "update uninstall" message to the module. Once uninstalled, the partition will be empty. The "update install" message is then sent to the module to install the new firmware to the non-active partition. The "update activate" message is then sent to mark the non-active partition as "active". Once the new firmware is installed and its partition activated, the module must be rebooted for the new firmware to be loaded into memory for execution.

3.3 User Guidance

No additional guidance for Users is required to maintain the FIPS-Approved mode of operation.

3.4 Non-FIPS-Approved Mode

When placed in its FIPS-Approved mode as described in this Security Policy, the module does not support a non-FIPS-Approved mode of operation.

4. Acronyms

Table 8 below provides definitions for the acronyms used in this document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption System
ASCII	American Standard Code for Information Interchange
ATDMA	Adaptive Time Division Multiple Access
CBC	Cipher Block Chaining
CDH	Cofactor Diffie Hellman
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DCC	Dynamic Ciphertext Channel
DDR3L	Double Data Rate Type Three Low-Voltage
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVB-S2	Digital Video Broadcast - Satellite - Second Generation
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
Gb	Gigabit
KAS	Key Agreement Scheme
KAT	Known Answer Test
LVDS	Low-Voltage Differential Signaling
Mb	Megabit
N/A	Not Applicable

Acronym	Definition
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standard
P/N	Part Number
PP	Protocol Processor
PRNG	Pseudo-Random Number Generator
PSS	Probabilistic Signature Scheme
RAM	Random Access Memory
RBG	Random Bit Generator
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication
TDMA	Time Division Multiple Access
TPM	Trusted Platform Module
TRANSEC	Transmission Security
U.S.	United States

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com