iDirect Government, LLC

TRANSEC Module

Hardware Part Number: E0002268
Firmware Version: Cloak 1.0.3.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 3
Document Version: 0.7

Prepared for:

iDirect Government, LLC
13921 Park Center Road, Suite 600
Herndon, VA 20171
United States of America

Phone: +1 703 648 8118
www.idirectgov.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
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 iDirect Government, LLC (iDirectGov). This Security Policy describes how the TRANSEC Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2.

FIPS 140-2 details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by National Institute of Standards and Technology (NIST) and Communication Security Establishment (CSE).

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 iDirectGov website (https://idirectgov.com/) contains information on the full line of products from iDirect Government, LLC
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about 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 area 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. TRANSEC Module

2.1 Overview

iDirect Government, LLC's satellite-based IP[2] communications technology enables constant connectivity for voice, video, and data applications in any environment. iDirectGov 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.

iDirectGov's Secure Satellite Broadband Solutions supports a Time Division Multiple Access (TDMA) upstream carrier and DVB-S2[3] downstream carrier. The iDirectGov network is optimized for satellite transmissions, obtaining the maximum performance out of satellite bandwidth. The system is fully integrated with iDirectGov's Network Management System, which provides configuration and monitoring functions. The iDirectGov 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 iDirectGov network components is shown in Figure 1 below.

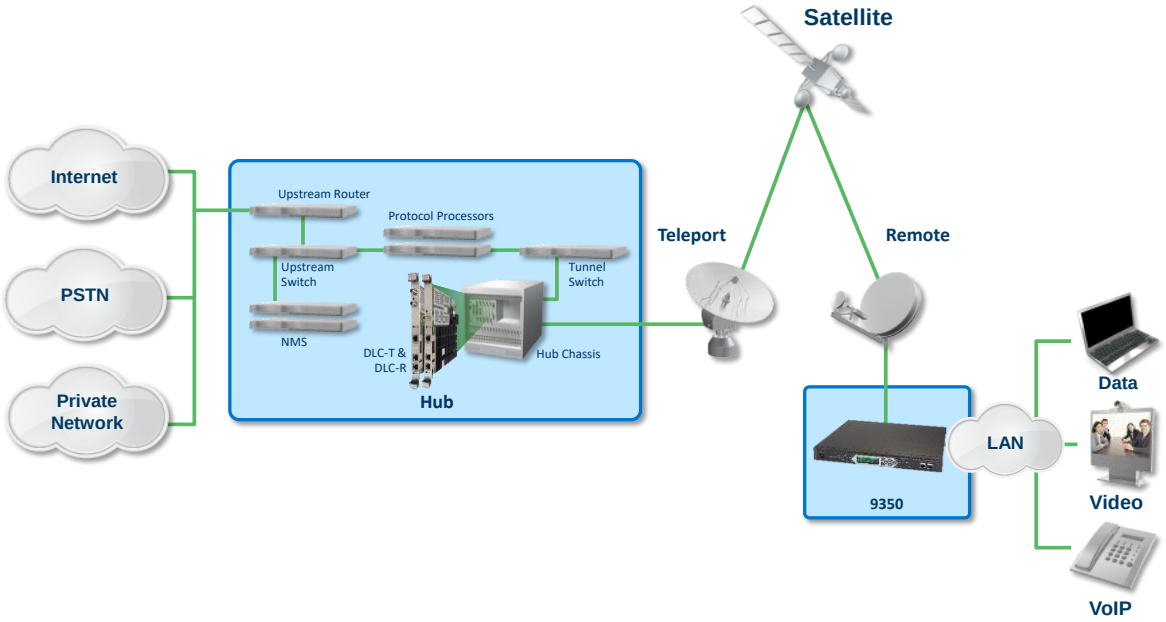

Figure 1 – iDirectGov Network Deployment

[2] IP – Internet Protocol
[3] DVB-S2 – Digital Video Broadcast - Satellite - Second Generation

The iDirectGov TRANSEC Module provides the cryptographic functionality necessary to secure information going through the network.

The TRANSEC Module is a 5.08cm[4] x 5.08cm daughter card (P/N[5]: E0002268) that is installed on the motherboard of devices such as hub line cards and remote modems. Packages containing data and control messages are sent across the network between the hub and the remote. Further, each TRANSEC Module can be configured to have a primary and secondary security domain, where each security domain will have its own set of keys and CSPs[6] to ensure data is sent securely across the network.

Figure 2 and Figure 3 below show the front and back side (respectively) of the TRANSEC Module with epoxy applied.

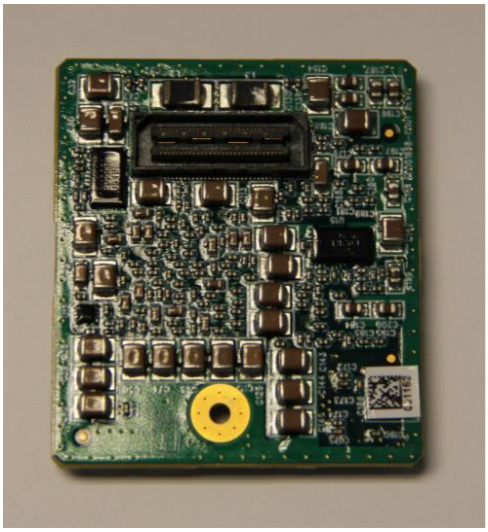

Figure 2 – TRANSEC Module (Front Side)

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

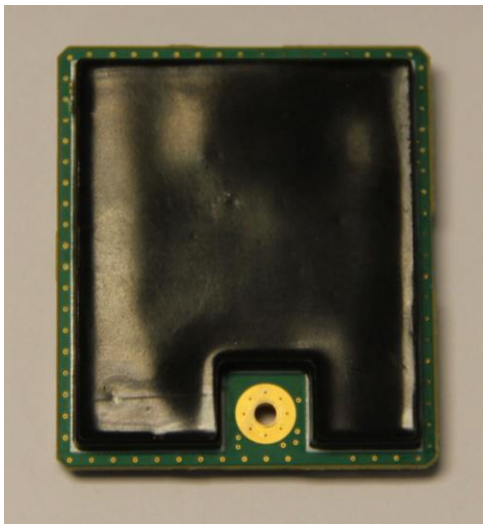

Figure 3 – TRANSEC Module (Back Side)

The epoxy is opaque within the visible spectrum on the module's back side. While the epoxy on the front side of the module is clear, please note that there are no security-relevant components visible from the front side. These are components such as the module power supply, decoupling capacitors, voltage rails monitoring device, voltage discharge transistors, and the TRANSEC 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[7]
7	Cryptographic Key Management	3
8	EMI/EMC[8]	3
9	Self-tests	3

[7] N/A – Not Applicable
[8] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Section	Section Title	Level
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[9]: 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[10] for running the module firmware. This is the primary cryptographic engine of the TRANSEC Module. The LVDS[11] Bus and Local Bus interfaces are integrated into the FPGA.
- 512Mb[12] flash memory for firmware storage. The flash memory is used for persistent storage of keys, certificates, and passwords.
- 4Gb[13] DDR3L[14] RAM[15] for temporary storage of keys during operation.

2.2.1 Cryptographic Boundary

Figure 4 below shows the functional block diagram of the TRANSEC Module and its interfaces.

[9] P/N – Part Number
[10] FPGA – Field-Programmable Gate Array
[11] LVDS – Low-Voltage Differential Signaling
[12] Mb – Megabits
[13] Gb – Gigabits
[14] DDR3L – Double Data Rate Type Three Low-Voltage
[15] RAM – Random Access Memory

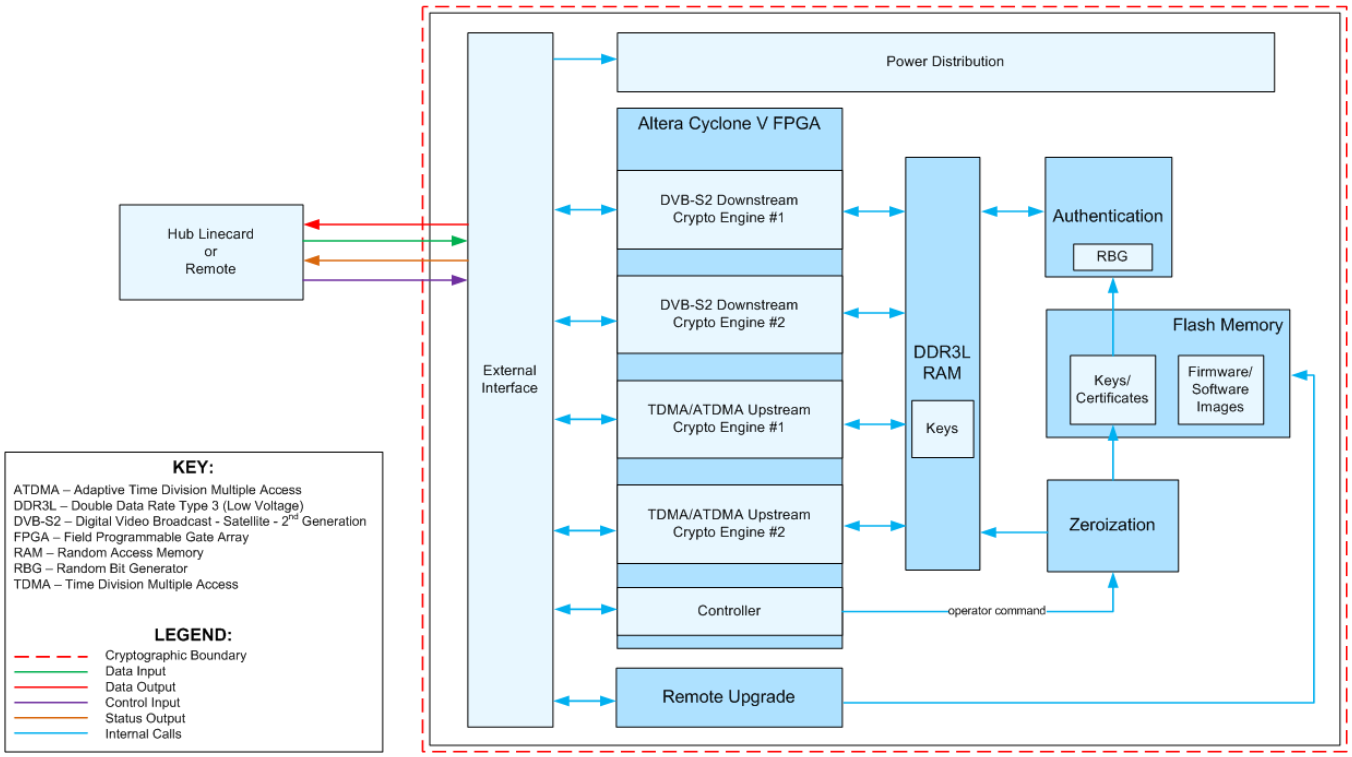

Figure 4 – TRANSEC Module Block Diagram

2.2.2 Algorithm Implementations

The TRANSEC Module utilizes the FIPS-Approved algorithm implementation sources listed in Table 2 below.

Table 2 – Algorithm Implementations

Implementation Name	Certificate Number
iDirectGov TRANSEC Cryptographic Library	A2105
iDirectGov TRANSEC SHA-3 Implementation	A2102
iDirectGov TRANSEC ECDH Implementation	A2053
iDirectGov TRANSEC Hardware AES Implementation	A2103

Table 3 below lists the certificate numbers awarded to each Approved algorithm.

Table 3 – Algorithm Certificate Numbers

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
A2103	AES[16]	FIPS PUB 197	CBC[17]	256	Encryption/decryption
A2105	AES	FIPS PUB 197	CBC	128, 192, 256	Encryption/decryption *The module does not use 128-bit or 192-bit key sizes operationally.*
Vendor Affirmed	CKG[18]	NIST SP[19] 800-133r2	-	-	Seed generation for asymmetric keys
A2105	DRBG[20]	NIST SP 800-90Ar1	Hash-based	SHA2-256	Deterministic random bit generation
A2105	ECDSA[21]	FIPS PUB 186-4	-	P-256	Key pair generation
			-	P-256	Public key validation
			-	P-256 (SHA-256, SHA2-512)	Digital signature generation
			-	P-256 (SHA-256, SHA2-512)	Digital signature verification
N/A	ENT (NP)[22]	NIST SP 800-90B	-	-	Entropy
A2053	KAS[23]	NIST SP 800-56Ar3 NIST SP 800-56Cr2	(ECC CDH[24] primitive) Scheme: OnePassDh KAS Role: Responder Methods: Full Validation, Key Pair Generation, Partial Validation KDF methods: One-step no-counter KDF (SHA2-256)	P-256	Key agreement[25] *Key establishment methodology provides 128 bits of encryption strength.*
A2105	RSA[26]	FIPS PUB 186-4	PKCS[27] #1 v1.5	2048 (SHA-256, SHA2-512)	Digital signature verification
A2102	SHA	FIPS PUB 202	SHA3-256	-	Message digest
A2105	SHS[28]	FIPS PUB 180-4	SHA2 -256, SHA2-512	-	Message digest

The vendor affirms the following cryptographic security methods:

[16] AES – Advance Encryption Standard
[17] CBC – Cipher Block Chaining
[18] CKG – Cryptographic key generation
[19] SP – Special Publication
[20] DRBG – Deterministic Random Bit Generator
[21] ECDSA – Elliptic Curve Digital Signature Algorithm
[22] ENT (NP) – Entropy (Non-Physical)
[23] Uses ECC – Key Agreement Scheme - Elliptic Curve Cryptography
[24] CDH – Cofactor Diffie-Hellman
[25] This complies with Scenario X1(2) in FIPS 140-2 Implementation Guidance D.8.
[26] RSA – Rivest Shamir Adleman
[27] PKCS – Public Key Cryptography Standard
[28] SHS – Secure Hash Standard

- Cryptographic key generation – Per *NIST SP 800-133rev2*, the module uses the FIPS-Approved hash-based DRBG specified in *NIST SP 800-90Arev1* for generation of seeds for asymmetric key generation. The generated seed is an unmodified output from the DRBG.

The module implements the non-Approved but allowed algorithms shown in Table 4 below.

Table 4 – Allowed Algorithms

Algorithm	Caveat	Use
AES (Cert. A2105, key unwrap)	Key establishment methodology provides 256 bits of encryption strength	Key unwrap[29] using 256-bit AES-CBC

2.2.3 Modes of Operation

When initialized per the guidance in section 3.1 of this Security Policy, the module only operates in the Approved mode of operation.

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.

[29] Per *FIPS 140-2 IG* D.9, any Approved mode of AES is allowed as a key unwrapping technique.

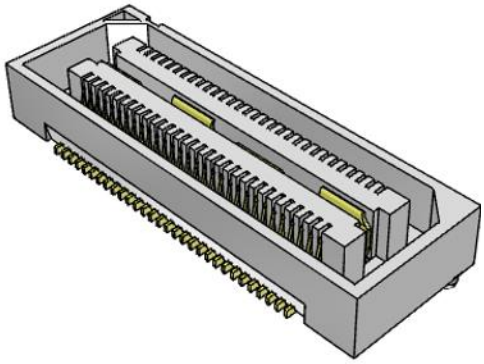

Figure 5 – TRANSEC Module Connector

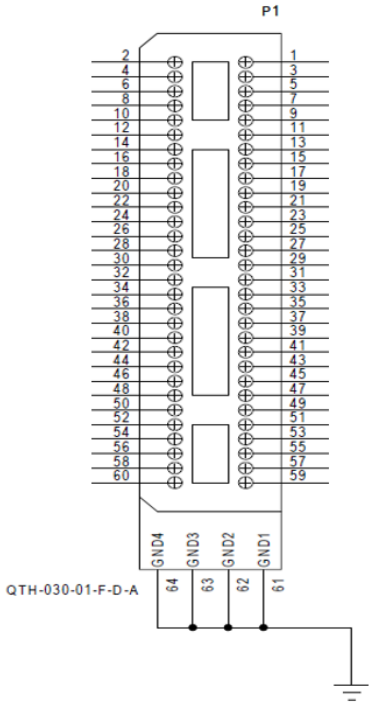

Figure 6 – TRANSEC Module Connector Pin Assignments

Table 5 below provides a mapping of each TRANSEC Module physical interface to the equivalent logical interface.

Table 5 – 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)

FIPS 140-2 Logical Interface	Physical Module Interface
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)
Ground Interface	TRANSEC Module Connector (Pin assignments: 61 – 64)

The TRANSEC Module utilizes specific pins to perform control functions as follows:

- 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

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. The CO role is responsible for installing, configuring, and zeroizing the module. The User role is used to perform status and system monitoring services.

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.

2.4.2 Services

Table 6 below provides a mapping from each module 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 6 – Mapping of Services to Inputs, Outputs, Roles, CSPs, and Type of Access

Service	Operator		Description	Input	Output	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	CO Password – X 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
Query factory information	✓	✓	This message retrieves factory default information.	Command	Factory default information	CO Password – X User Password – X
Device status	✓	✓	This message returns the status of the device.	Command	Status	CO Password – X User Password – X
Firmware load	✓		This message executes the firmware integrity check when the module is loaded	Command	Status	CO Password – X Firmware Signature Key – R
Get date and time	✓	✓	This message returns the date and time for the security domain identified.	Command	Date/time	CO Password – X User Password – X
Get channel configuration	✓	✓	This message returns channel configuration data.	Command	Status	CO Password – X User Password – X

Service	Operator		Description	Input	Output	Key/CSP and Type of Access
	CO	User				
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	CO Password – X User Password –X
Session ID request	✓		This message will be used by the host to instruct the TRANSEC Module to generate a unique session id for the specified session.	Command	Status	CO Password – X
Channel statistics	✓	✓	This message requests channel statistics.	Command	Status	CO Password – X User Password – X ACC Key – R DCC[31] Key – R
Reset statistics	✓		This message instructs the TRANSEC Module to reset different statistics counters.	Command	Status	CO Password – X
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 RSA public key – R, X ECDSA public key – R, X ECDSA private key – R, X ECDH shared secret – W, X Key 1 – W, X 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 RSA public key – R, X ECDSA public key – R, X ECDSA private key – R, X ECDH shared secret – W, X Key 1 – W, X Key 2 – W, X ACC Key – W DCC Key – W

[30] ACC – Acquisition Ciphertext Channel
[31] DCC – Dynamic Ciphertext Channel
[32] V3 – iDirectGov's third version of over-the-air messaging
[33] PP – Protocol Processor

Service	Operator		Description	Input	Output	Key/CSP and Type of Access
	CO	User				
Get certificates	✓		This message checks the validity and returns a list of all the certificates stored.	Command	Status	CO password – X Certificate issued by the iDirectGov 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 iDirectGov 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 iDirectGov 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 – W ECDSA public key – W
Certificate query	✓	✓	This message returns the appropriate certificate from the specified security domain.	Command	Status	CO Password – X User Password – X Certificate issued by the iDirectGov CA Foundry – R
Get PKI hash	✓	✓	This message gets the global/local PKI hash from the specified security domain.	Command	Status	CO Password – X User Password – X
Set PKI hash	✓		This message sets the global/local PKI hash in the specified security domain.	Command	Status	CO Password – X
Zeroize	✓		This message zeroizes all keys and CSPs in the module.	Command	Status	All CSPs – W

The module also provides services that do not require authentication (see Table 7 below). These services do not require a host motherboard message with an associated username/password. These services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the overall security of the module.

Table 7 – 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
Zeroize primary	Zeroizes keys and CSPs via zeroize I/O pin	Command	Status	All CSPs – W

2.4.3 Authentication

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

The fastest network connection supported by the module is 100 Mbps[36] . At most ($100x10^6$ bits/second × 60 seconds) = $6x10^9$ = 6,000,000,000 bits of data can be transmitted in one minute. Each password is 64 bits (8 bits per character x 8 characters), meaning $9.375x10^7$ passwords can be passed to the module (assuming there is no overhead). This equates to a 1:65,020,686 chance of a random attempt will succeed, or a false acceptance will occur in a one-minute period, which is less than the required probability.

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 epoxy covering all components on the card. The epoxy protects the module from tampering. Any tampering will damage the module and render it inoperable. Further, the epoxy is opaque within the visible spectrum on the module's back side, protecting all security-relevant module components from direct visual access.

2.6 Operational Environment

The module's firmware, TRANSEC Module version Cloak 1.0.3.0, 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.

2.7 Cryptographic Key Management

The module supports the keys and CSPs listed in Table 8 below.

[34] U.S. – United States
[35] ASCII – American Standard Code for Information Interchange
[36] Mbps – Megabits per second

Table 8 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
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	Validates signature verification of keyroll and set date/time
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	Encrypts all traffic and traffic headers required for a remote to acquire the network
DCC Key	AES-256 CBC key	Externally generated, entered electronically in encrypted form	Never exits the module	Plaintext in volatile memory	Zeroize control message	Encrypts all user traffic and traffic headers
ECDH shared secret	256-bit shared secret	Internally established via ECC CDH primitive	Never exits the module	Plaintext in volatile memory	Zeroized after service completes	Used as input to ECDH KAS KDF for generating Key 1
ECDSA private key	256-bit ECDH private exponent	Internally generated via DRBG	Never exits the module	Plaintext in flash memory	Zeroize control message	Creates the ECDH shared secret
ECDSA public key	256-bit ECDH public exponent	Internally generated via DRBG	Exits electronically in plaintext form	Plaintext in volatile memory	Zeroize control message	Creates the ECDH shared secret; verify certificates issued by the iDirect CA Foundry
Key 1	AES 256-bit key	Internally established via key agreement	Never exits the module	Plaintext in volatile memory	Zeroized after service completes	Decrypts 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	Decrypts ACC and DCC key
Firmware Signature Key	RSA 2048-bit key	Externally generated, hard coded in flash at the factory	Never exits the module	Plaintext in flash memory	Never zeroized	Validates firmware integrity
RSA public key	RSA 2048-bit public key	Externally generated, entered electronically in plaintext form	Never exits the module	Plaintext in flash memory	Never zeroized	Validates keyroll messages
DRBG Entropy	Random data – 128 bits	Internally generated	Never exits the module	Plaintext in volatile memory	Module reset or power-down	Entropy material for Hash_DRBG

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 Hash_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	Authenticates 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	Authenticates the User role

The module uses a software-based CPU jitter entropy scheme internal to the module for seeding the DRBG used in the generation of ECDSA keys. This entropy scheme was validated for compliance with *NIST SP 800-90B*. Based on noise source testing and analysis, the estimated minimum entropy is 1.851477 per 4 bits of data. The overall amount of generated entropy meets the required security strength of 256 bits based on the amount of entropy requested by the module.

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 using 2048-bit RSA digital signature verification
- Known Answer Tests (KATs) in FPGA
    - AES-CBC encrypt and decrypt KATs (256-bit)
- Known Answer Tests (KATs) in firmware
    - AES-CBC encrypt and decrypt KATs (256-bit)
    - SHA2-256 KAT
    - SHA2-512 KAT
    - SHA3-256 KAT
    - ECDSA sign/verify PCT[37] (curve P-256)
    - RSA verify KAT (2048-bit)
    - DRBG KAT
    - ECC CDH Primitive “Z” Computation KAT
    - KAS One-Step KDF KAT (SHA2-256)
- Health Tests in Entropy (performed over 1024 consecutive samples)
    - Entropy “Stuck” Test
    - Entropy Repetition Count Test
    - Entropy Adaptive Proportion Test
    - Entropy Lag Predictor Test

[37] PCT – Pairwise Consistency Test

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
- DRBG Continuous Random Number Generator Test
- Entropy "Stuck" Test
- Entropy Repetition Count Test
- Entropy Adaptive Proportion Test (performed over 512 samples during runtime)
- Entropy Lag Predictor Test
- ECDSA sign/verify PCT

2.9.3 Critical Functions Self-Tests

The module performs health checks for the DRBG's Generate, Instantiate, and Uninstantiate functions as specified in section 11.3 of *NIST SP 800-90Arev1*. These tests are performed at power-up. The module also performs all applicable key assurances for its ECDH implementation as specified in section 9 of *NIST SP 800-56Arev3*. These tests are performed as conditional tests.

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 iDirectGov.

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. **Operating the module without following all required initialization and configuration steps below is prohibited; any such operation is outside the scope of this Security Policy.**

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 1.0.3.0). 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 1.0.3.0):

1. The CO 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 CO sends the “update install” message indicating that the TRANSEC Module firmware (version Cloak 1.0.3.0) is to be loaded into partition 1.
4. The CO sends the “update activate” message indicating that the firmware installed in partition 1 is to be marked “active”.
5. The CO 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 Firmware Signature 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 initialization steps have been executed. The module remains in a FIPS-Approved mode until the “zeroize primary” message is sent and executed.

For general instructions on initializing and configuring the module, please refer to the *iDirectGov TRANSEC Module Users Guide*. For operation in the Approved mode, the CO shall follow the initialization steps below.

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 6 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. Once this occurs, the module will no longer be in an operational state. The CO must reinitialize and configure the module per the guidance in section 3.1 of this document to return to an operational state.

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.

4. Acronyms and Abbreviations

Table 9 below provides definitions for the acronyms and abbreviations used in this document.

Table 9 – Acronyms

Acronym	Definition
AES	Advanced Encryption System
ASCII	American Standard Code for Information Interchange
ATDMA	Adaptive Time Division Multiple Access
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSP	Critical Security Parameter
DCC	Dynamic Ciphertext Channel
DDR3L	Double Data Rate Type 3 (Low Voltage)
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVB-S2	Digital Video Broadcast - Satellite - 2nd Generation
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ENT (NP)	Entropy (Non-Physical)
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
Gb	Gigabit
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDA	Key Derivation Algorithm
KTS	Key Transport Scheme
LVDS	Low-Voltage Differential Signaling
Mb	Megabit
N/A	Not Applicable

Acronym	Definition
NIST	National Institute of Standards and Technology
PCT	Pairwise Consistency Test
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
TRANSEC	Transmission Security
U.S.	United States

Prepared by:

Corsec Security, Inc.

12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

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