M3-SE-RTR2 and TXC3

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 6.0

March 3, 2014

Table of Contents

1 INTRODUCTION.......... 3

1.1 PURPOSE.......... 3
1.2 MODULE VALIDATION LEVEL 3
1.3 REFERENCES.......... 3
1.4 TERMINOLOGY 4
1.5 DOCUMENT ORGANIZATION 4

2 M3-SE-RTR2 AND TXC3.......... 5

2.1 M3-SE-RTR2 AND TXC3 CRYPTOGRAPHIC MODULE (CISCO 5915 ESR BASED) PHYSICAL CHARACTERISTICS.......... 5
2.2 MODULE INTERFACES.......... 6
2.3 ROLES AND SERVICES.......... 8
2.3.1 Crypto Officer Services.......... 9
2.3.2 User Services 10
2.3.3 Unauthenticated Services.......... 10
2.3.4 Strength of Authentication 10
2.4 PHYSICAL SECURITY 11
2.5 CRYPTOGRAPHIC ALGORITHMS 13
2.5.1 Approved Cryptographic Algorithms.......... 13
2.5.2 Non-Approved Cryptographic Algorithms 13
2.6 CRYPTOGRAPHIC KEY MANAGEMENT.......... 14
2.7 SELF-TESTS 18
2.7.1 Self-tests performed by the IOS and Hardware.......... 19

3 SECURE OPERATION OF THE M3-SE-RTR2 AND TXC3.......... 19

3.1 PHYSICAL SECURITY 20
3.2 INITIAL SETUP 20
3.3 SYSTEM INITIALIZATION AND CONFIGURATION.......... 20
3.4 IPSEC REQUIREMENTS AND CRYPTOGRAPHIC ALGORITHMS 21
3.5 PROTOCOLS 21
3.6 REMOTE ACCESS 21
3.7 HTTPS/TLS MANAGEMENT IS NOT ALLOWED IN FIPS MODE.......... 22
3.8 IDENTIFYING OPERATION IN AN APPROVED MODE.......... 22
3.9 NOTES ON SERVICES.......... 22

1 Introduction

1.1 *Purpose*

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco 5915 Embedded Services Router (ESR) as integrated in the DTECH LABS' M3-SE-RTR2 and TXC3 products. This security policy describes how the M3-SE-RTR2 and TXC3 enclosures along with the embedded Cisco 5915 Embedded Services Routers (ESR) meet the security requirements of FIPS 140-2, and how to operate the router with on-board crypto enabled in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the M3-SE-RTR2 and TXC3 products manufactured by DTECH LABS, Inc.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

1.2 *Module Validation Level*

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**2**

Table 1 Module Validation Level

1.3 *References*

This document deals only with operations and capabilities of the M3-SE-RTR2 and the TXC3 (Packaged Cisco 5915 Embedded Services routers) in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

- The DTECH LABS website contains information on the full line of M3-SE and TXC products. Please refer to the following website: www.dtechlabs.com
- The Cisco Systems website contains information on the full line of Cisco Systems routers. Please refer to the following website: http://www.cisco.com/en/US/products/hw/routers/index.html
- The Cisco 5915 Embedded Services Routers is part of the family of Mobile Internet Routers: http://www.cisco.com/en/US/products/hw/routers/products.html#N390A6E
- For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the M3-SE-RTR2 and the TXC3 are referred to as the 5915 ESR based product, router, the module, or the system.

1.5 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the M3-SE-RTR2, TXC3 and the Cisco 5915 Embedded Services Router, and explains the secure configuration and operation of the module(s). This introduction section is followed by Section 2, which details the general features and functionality of the router(s). Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is DTECH-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact DTECH LABS.

2 M3-SE-RTR2 and TXC3

The M3-SE-RTR2 and TXC3 are high-performance, ruggedized routers utilizing the Cisco 5915 ESR. With onboard hardware encryption, the Cisco 5915 offloads encryption processing from the router to provide highly secure yet scalable video, voice, and data services for mobile and embedded outdoor networks. The M3-SE-RTR2 and TXC3 provide a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements. This section describes the general features and functionality provided by the routers. The M3-SE-RTR2 and TXC3 use industrial-grade components and is optimized for harsh environments that require Cisco IOS Software routing technology. The following subsections describe the physical characteristics of the routers.

2.1 M3-SE-RTR2 and TXC3 Cryptographic Module (Cisco 5915 ESR based) Physical Characteristics

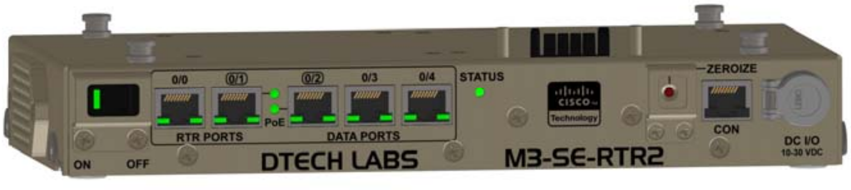

Figure 1 M3-SE-RTR2

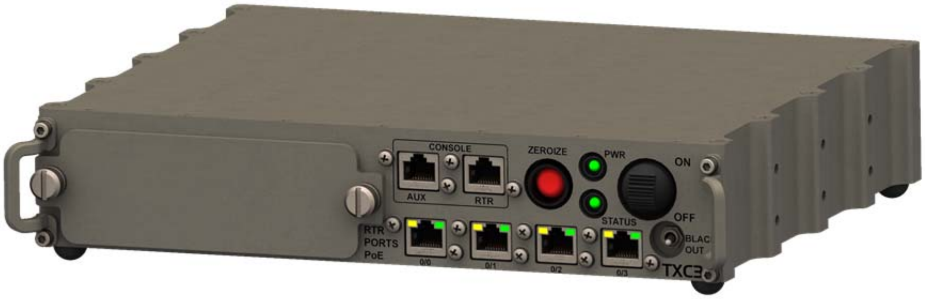

Figure 2 TXC3

The M3-SE-RTR2 and the TXC3 is a router and switch module that is available in both air and conduction-cooled models respectively, which contain a multiple-chip standalone cryptographic module embedded on the internal circuit boards. The ruggedized enclosures of the M3-SE-RTR2 and the TXC3 (providing a cryptographic boundary at FIPS 140-2 Level 2) also protect the module against the elements.

The module features the following interfaces:

1. One RS-232 serial console port (via edge fingers)
2. 2 Routed Fast Ethernet and 3 Switched Fast Ethernet interfaces (via edge fingers)
3. Power (via PCI stacking connector)
4. JTAG interface (via edge fingers)
5. LED signals (via edge fingers)

The LED signals are located on the edge fingers. The card, itself, does not contain any LEDs. A system integrator is responsible for connecting the LED signals to actual LEDs:

Each 5915 ESR provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power.

The physical boundary of the ruggedized enclosures of the M3-SE-RTR2 and the TXC3 are discussed as they provide the protection to meet FIPS 140-2 Level 2.

2.2 Module Interfaces

The M3-SE-RTR2 features the following interfaces:

1. One serial console port
2. One routed 10/100 ETH WAN port
3. One routed 10/100 ETH Data port
4. Three switched 10/100 ETH Data ports
5. LEDs
6. One DC power interconnect
7. One 2 pin DC power I/O (Wide range 10-30 VDC)
8. One power On/Off Switch
9. One “Zeroize” push button
10. Four mechanical interconnect bushings
11. Four mechanical interconnect slide locks

The TXC3 features the following interfaces:

1. Two serial console ports
2. One routed 10/100 ETH WAN port
3. One routed 10/100 ETH Data port
4. Three switched 10/100 ETH Data ports
5. LEDs
6. One DC power interconnect
7. One 2 pin DC power I/O (Wide range 10-30 VDC)

8. One power On/Off Switch
9. One “Zeroize” push button
10. One “Black-out” toggle switch
11. One auxiliary module bay with 10/100 ETH and Power interconnect to router.

These interfaces are depicted in the figures below:

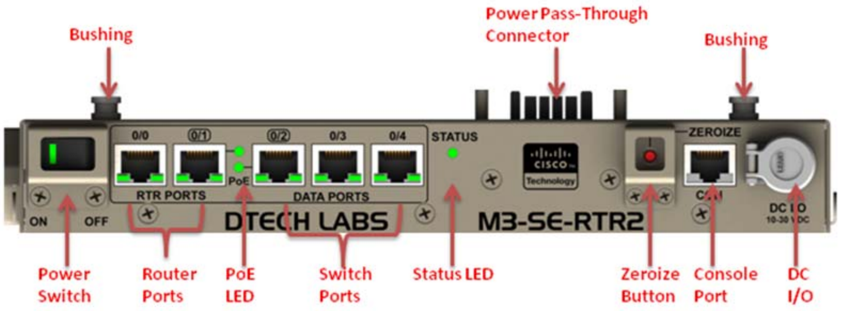

Figure 3: M3-SE-RTR2 Interfaces

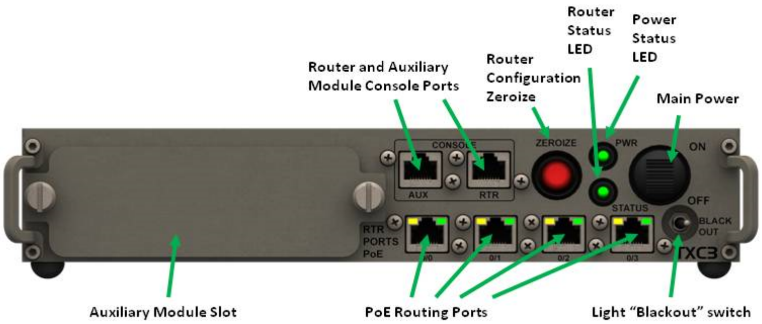

Figure 4: TXC3 Front Interfaces

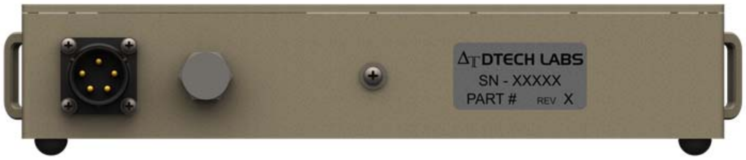

Figure 5: TXC3 Rear Interface

The following tables provide more detailed information regarding the interfaces and their functions:

Main Power Switch	Main power to the module with a green LED.
Router Ports	Two (0/0, 0/1) Layer 3 router ports.
PoE	PoE indicates that power is being applied to the port. (802.3at)
Switch Ports	Three (0/2, 0/3, 0/4) Layer 2 switch ports. (802.3at)
Status	Green Status LED to show WAN activity.
Ethernet LEDs	Used to show link and activity on Ethernet ports
Power Pass-Through Connector	Used to pass power to other directly connected M3-SE series modules.
Zeroize Button	Used to erase router configuration and/or Cisco IOS
Console Port	Used to configure the router. The default user ID and password are “cisco/cisco”. Default baud 9600 8N1. (use standard Cisco rollover console cable)
Bushings	Used to attach the M3-SE-RTR2 to other M3-SE series modules.
DC I/O Port	10 - 30 VDC input / output to power to charge batteries or to power encryption device.

Table 2 – M3-SE-RTR2 Interface Descriptions

RTR Ports - PoE	LAN/WAN 10/100 (L2/L3) multilayer Power over Ethernet ports (802.3at Compliant).
Console	Router console port provides a connection into the Wolverine Lite for configuration of router. Auxiliary console port provides a connection to any module in the AUX slot.
Zeroize	Zeroize Feature (quickly and easily erases saved router configuration and/or Cisco IOS). NOTE: There is a software configuration on the router required to enable this function.
Status	Provides router status indication.
PWR	Turns unit power on and off.
Power Indicator	Indicates there is power to the unit.
Black Out	Extinguishes all external lights for blackout operations.
AUX Module Slot	Space for an auxiliary module. Cover plate secures the slot when auxiliary modules are not used.

Table 3 – TXC3 Interface Descriptions

2.3 Roles and Services

Authentication in the M3-SE-RTR2 and TXC3 is role-based. There are two main roles in the router that operators can assume: the Crypto Officer role and the User role. There is also a maintenance role available through the JTAG connector of the internal Cisco 5915 board;

however it is inaccessible as described in the Physical security section of this document. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. The configuration of the encryption and decryption functionality is performed only by the Crypto Officer after authentication to the Crypto Officer role by providing a valid Crypto Officer username and password. Once the Crypto Officer configured the encryption and decryption functionality, the User can use this functionality after authentication to the User role by providing a valid User username and password. The Crypto Officer can also use the encryption and decryption functionality after authentication to the Crypto Officer role. The module supports RADIUS and TACACS+ for authentication. The RSA digital signature authentication mechanism is used to authenticate the User role via IPSec/IKE protocol implementation.

2.3.1 Crypto Officer Services

A Crypto Officer enters the system by accessing the console/auxiliary port with a terminal program or SSHv2 session to a LAN port or the 10/100 management Ethernet port. The Crypto Officer authenticates as a User and then authenticates as the Crypto Officer role. During initial configuration of the router, the Crypto Officer password (the “enable” password) is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router.

The Crypto Officer services consist of the following:

Configure the router	Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
Define Rules and Filters	Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
View Status Functions	View the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.
Manage the router	Log off users, shutdown or reload the router, erase the flash memory, manually back up router configurations, zeroize all cryptographic keys or CSPs, view complete configurations, manager user rights, and restore router configurations. In addition, Crypto Officer also has access to all User services.
Set Encryption/Bypass	Set up the configuration tables for IP tunneling. Set preshared keys

	and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address. The router implements alternating bypass capability.
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand

2.3.2 User Services

Users can access the system in two ways:

1. By accessing the console port with a terminal program or via IPSec protected telnet or SSH session to an Ethernet port. Please note that the PC used for the console connection is a non-networked PC. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program.

2. Via an IPSec session. This session is authenticated either using a shared secret or RSA digital signature authentication mechanism.

The services available to the User role consist of the following:

Status Functions	View state of interfaces and protocols, version of IOS currently running.
Network Functions	Connect to other network devices and initiate diagnostic network services (i.e., ping, mtrace).
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).
Directory Services	Display directory of files kept in flash memory.
GetVPN	Negotiation and encrypted data transport via Get VPN
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand
Zeroization Services	Zeroize cryptographic keys stored in Dynamic Random Access Memory (DRAM) via power cycling

2.3.3 Unauthenticated Services

The services available to unauthenticated users are:

- Viewing the status output from the module’s LEDs
- Perform bypass services
- Powering the module on and off using the power switch on the third-party chassis

2.3.4 Strength of Authentication

The security policy stipulates that all user passwords and shared secrets must be 8 alphanumeric characters, so the password space is 218 trillion possible passwords. The possibility of randomly guessing a password is thus far less than one in one million. To exceed a one in 100,000 probability of a successful random password guess in one minute, an attacker would have to be capable of 28 million password attempts per minute, which far exceeds the operational capabilities of the module to support.

When using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength. An attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 5.19×10^{28} attempts per minute, which far exceeds the operational capabilities of the modules to support.

2.4 Physical Security

The M3-SE-RTR2 and TXC3 rugged enclosures serving as a physical embodiment of the Cisco 5915 ESR are being validated at physical security level 2. As such, along with using production grade material, the module does implement physical security mechanisms in the form of tamper evident seals. Below illustrations identify the four locations on the M3-SE-RTR2 and six locations on the TXC3 of these seals to comply with FIPS 140-2 Level 2 requirements. To ensure proper evidence of possible tampering, clean surfaces with rubbing alcohol, let dry and then apply the FIPS tamper evident labels supplied (DTECH Orderable P/N: DT-FIPS-TEL) to the chassis of the unit as shown in Figure 6 or Figure 7 for your respective product.

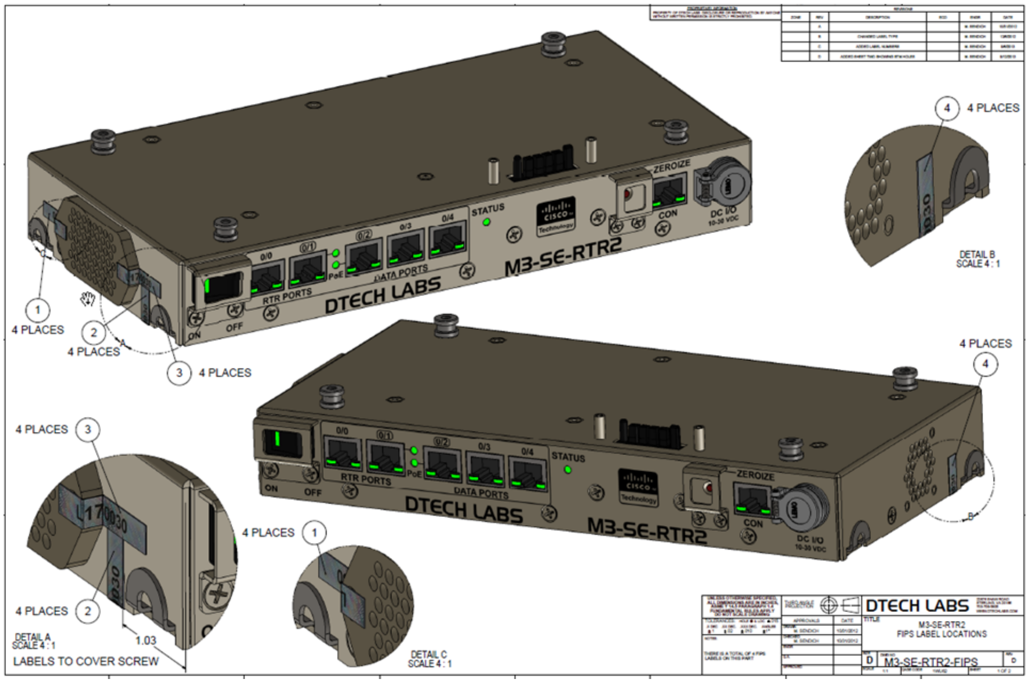

Figure 6: M3-SE-RTR2-FIPS Tamper Evidence

The M3-SE-RTR2 (Hardware version “-FIPS”) encloses the Cisco 5915 ESR in opaque material in the form of aluminum sheet metal (.060 wall thickness). The crypto module on the Cisco

5915 is not accessible or visible from the exterior of the enclosure as all interfaces are made available on the external face of the product through a custom interface board. Although the Cisco 5915 Module supports a maintenance role in FIPS mode via its JTAG interface of the boards edge finger connectors, that connector and those signals are encapsulated by the interface board and terminated so there is no access to this interface, therefore no maintenance role is available in this product without the complete disassembly which would be evident due to the use of the warranty/tamper seals shown in the figure above. The physical specifications of the M3-SE-RTR2 are as follows: 10.25" x 5.06" 1.5", 1.6 pounds.

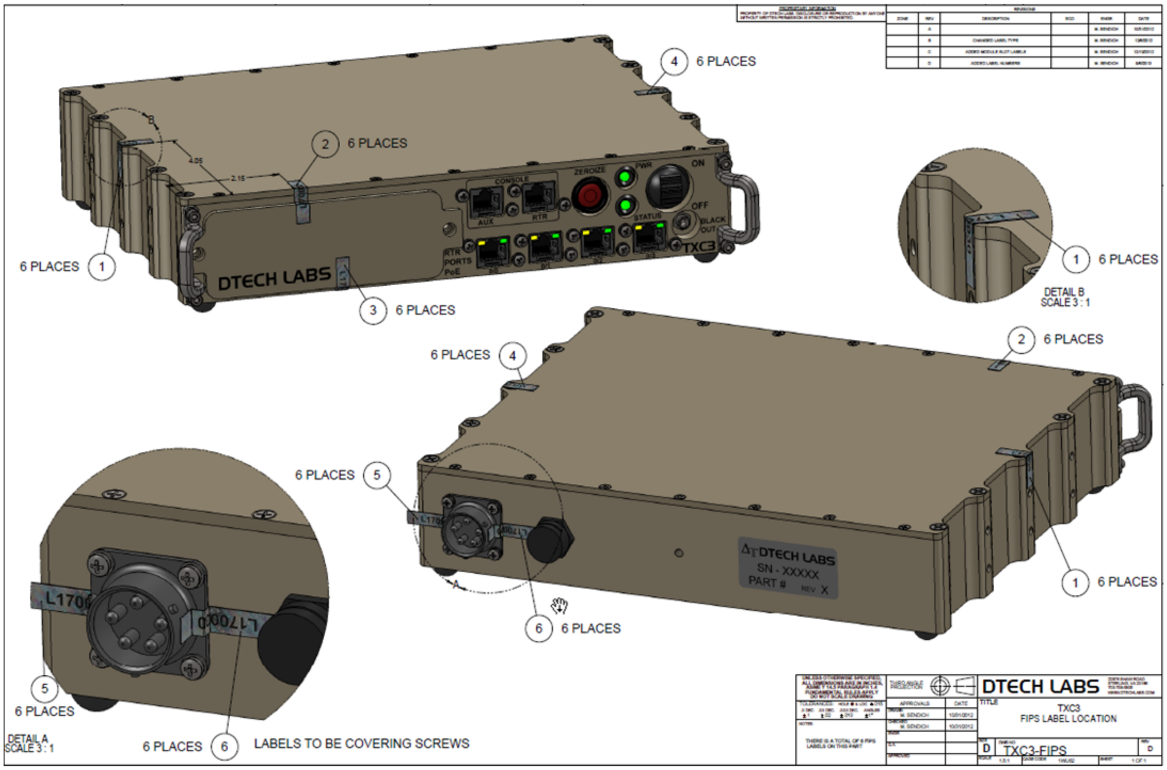

Figure 7: TXC3-FIPS Tamper Evidence

The TXC3 (Hardware version "-FIPS") encloses Cisco 5915 ESR in opaque material comprised of machined aluminum (minimum .090 wall thickness). The crypto module on the Cisco 5915 is not accessible or visible from the exterior of the enclosure as all interfaces are made available on the external face of the product through a custom interface board. Although the Cisco 5915 Module supports a maintenance role in FIPS mode via its JTAG interface of the boards edge finger connectors, that connector and those signals are encapsulated by the interface board and terminated so there is no access to this interface, therefore no maintenance role is available in this product without the complete disassembly which would be evident due to the use of the warranty/tamper seals shown in the figure above. The physical specifications of the TXC3 are as follows: 10.5" x 8.38" 2", 5.5 pounds. The Crypto Officer role shall be responsible for ensuring that the module is physically secure and will have control over unused seals.

2.5 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

2.5.1 Approved Cryptographic Algorithms

The routers support the following FIPS-2 approved algorithm implementations:

Algorithm	**Algorithm Certificate Number**	
	IOS	**Freescale MPC8358E**
AES	**2031**	**962 and 1535**
Triple-DES	**1310**	**757**
SHS	**1779**	**933**
HMAC	**1232**	**537**
DRBG	**196**	**N/A**
RSA[1]	**1055**	**N/A**

Table 4: Approved Cryptographic Algorithms

2.5.2 Non-Approved Cryptographic Algorithms

The module provides negotiation of security services for IPsec in accordance with RFC 3457 as an extension of phase 2 of the protocol defined in RFC 2409.

The module supports the following non-approved cryptographic algorithms that shall not be used in FIPS mode of operation:

- DES
- DES MAC
- HMAC MD4
- HMAC MD5
- MD5
- NDRNG
- RC4
- MD4

The modules support the following key establishment/derivation schemes:

- Diffie-Hellman[2] (key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

[1] Please note that modulus sizes 1024 and 1536 bits are no longer allowed for Signature Generation or Key Generation. SHA-1 is also not allowed for digital signature generation.

[2] Please note that the use of Diffie-Hellman keys that are less than 2048 bits are not allowed. Only 2048 bits must be used.

- RSA key transport (key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- Internet Key Exchange Key Establishment (IKEv1/IKEv2)
- GDOI (key wrapping; key establishment methodology provides between 112 and 256 bits of encryption strength)

The module supports the following algorithms with non-Approved key sizes. As such, these algorithms with non-Approved key sizes are no longer allowed in FIPS mode:

FIPS186-2:
ALG[ANSIX9.31]: Key(gen)MOD: 1024, 1536 PubKey Values: 65537
ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024 , 1536 , SHS: SHA-1, SHA-256, SHA-512, 2048 , SHS: SHA-1

2.6 Cryptographic Key Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. The zeroization method for each individual keys or CSPs can be found in table 4 below. All cryptographic keys are exchanged and entered electronically or via Internet Key Exchange (IKE)/Group Domain of Interpretation (GDOI), and all CSPs are entered into the module by the Crypto Officer role.

The module generates cryptographic keys whose strengths are modified by available entropy.

The module supports the following keys and critical security parameters (CSPs):

ID	Algorithm	Size	Description	Storage	Zeroization Method
DRBG V	SP 800-90A CTR_DRBG	128-bits	Generated by entropy source via the SP 800-90A CTR_DRBG derivation function. It is stored in DRAM with plaintext form	DRAM (plaintext)	Automatically when the router is power cycled
DRBG key	SP 800-90A CTR_DRBG	256-bits	This is the 256-bit DRBG key used for SP 800-90A CTR_DRBG	DRAM (plaintext)	Automatically when the router is power cycled
DRBG entropy input	SP 800-90A CTR_DRBG	256-bits	HW based entropy source used to construct seed	DRAM (plaintext)	Automatically when the router is power cycled
DRBG seed	SP 800-90A CTR_DRBG	384-bits	Generated by entropy source via the SP 800-90A CTR_DRBG derivation function. Input to the DRBG to determine the internal state of the DRBG	DRAM (plaintext)	Automatically when the router is power cycled
Diffie-Hellman private exponent	Diffie-Hellman	2048 bits[3]	The private exponent used in Diffie-Hellman (DH) exchange. Generate by the module.	DRAM (plaintext)	Automatically after shared secret

			Zeroized after DH shared secret has been generated.		generated.
Diffie-Hellman Shared Secret	Diffie-Hellman	2048-bits[3]	Shared secret derived by the Diffie-Hellman Key exchange	DRAM (plaintext)	Automatically after session is terminated
Skeyid	Keyed SHA-1	160-bits	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)	Automatically after IKE session terminated.
skeyid_d	Keyed SHA-1	160-bits	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session encryption key	Triple-DES/AES	168-bits/256-bits	The IKE session encrypt key. Derived in the module	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session authentication key	SHA-1 HMAC	160-bits	The IKE session authentication key. Derived in the module.	DRAM (plaintext)	Automatically after IKE session terminated.
ISAKMP preshared	Secret	At least eight characters	The key used to generate IKE skeyid during preshared-key authentication. It is entered by the Crypto Officer. “no crypto isakmp key” command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext or encrypted)	“# no crypto isakmp key”
IKE RSA Authentication private Key	RSA	1024/1536/2048-bits[4]	RSA private key for IKE authentication. Generated by the module, set as IKE RSA Authentication Key with the “crypto keyring” or “ca trust-point” command. The IKE RSA private key will have an associated IKE RSA Authentication public key.	NVRAM (plaintext)	“# crypto key zeroize rsa"
IKE RSA Authentication public key	RSA	1024/1536/2048-bits[4]	RSA public key for IKE authentication. Generated by the module, set as IKE RSA Authentication Key with the “crypto keyring” or “ca trust-point” command. The IKE RSA public key will have an associated IKE RSA Authentication private key.	NVRAM (plaintext)	“# crypto key zeroize rsa"
IPSec encryption key	Triple-DES/AES	168-bits/256-bits	The IPSec encryption key. Derived in the module . Zeroized when IPSec session is terminated.	DRAM (plaintext)	Automatically when IPSec session terminated.
IPSec authentication key	SHA-1 HMAC	160-bits	The IPSec authentication key. Derived in the module. The zeroization is the same as above.	DRAM (plaintext)	Automatically when IPSec session terminated.
GDOI Key encryption Key (KEK)	Triple-DES/AES	Triple-DES (168-bits)/AES (128/192/256-bits)	This key is generated by using the “GROUPKEY-PULL” registration protocol with GDOI. Generate by the module. It is used protect GDOI rekeying data.”	DRAM (plaintext)	Automatically when session terminated.
GDOI Traffic Encryption Key (TEK)	Triple-DES/AES	Triple-DES (168-bits)/AES	This key is generated by using the “GROUPKEY-PULL” registration protocol and updated using the “GROUPKEY-	DRAM (plaintext)	Automatically when session terminated.

		(128/192/ 256-bits)	PUSH” registration protocol with GDOI. Generate by the module. It is used to encrypt data traffic between Get VPN peers		
GDOI TEK Integrity key	HMAC SHA-1	160-bits	This key is generated by using the “GROUPKEY-PULL” registration protocol and updated using the “GROUPKEY-PUSH” registration protocol with GDOI. Generate by the module. It is used to ensure data traffic integrity between Get VPN peers.	DRAM (plaintext)	Automatically when session terminated.
SSH RSA private key	RSA	1024/1536 /2048 bits[4]	This key is used for message signing when performing SSH authentication. Generated by the module. The SSH RSA private key will have an associated SSH RSA Authentication public key.	NVRAM (plaintext or encrypted)	“# crypto key zeroize rsa”
SSH RSA public key	RSA	1024/1536 /2048 bits[4]	This key is used for message signing when performing SSH authentication. Generated by the module. The SSH RSA public key will have an associated SSH RSA Authentication private key.	NVRAM (plaintext or encrypted)	“# crypto key zeroize rsa”
SSH session key	TDES /AES	TDES (Key Size 168 bits)/AES (Key Size 128/192/256 bits)	This is the SSH session key. It is used to encrypt all SSH data traffics traversing between the SSH client and SSH server. It is derived in the module.	DRAM (plaintext)	Automatically when SSH session terminated
SSH session authentication key	HMAC-SHA-1	160 bits	This key is used to perform the authentication between the SSH client and SSH server. It is derived in the module.	DRAM (plaintext)	Automatically when SSH session terminated
User password	Shared Secret	At least eight characters	The password of the User role. It is entered by Crypto Officer. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
Enable password	Shared Secret	At least eight characters	The plaintext password of the CO role. It is entered by the Crypto Officer. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
Enable secret	Shared Secret	At least eight characters	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. It is entered by the Crypto Officer. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
RADIUS secret	Shared Secret	At least eight characters	The RADIUS shared secret. It is entered by the Crypto Officer. This shared secret is zeroized by executing the “no radius-server key” command.	NVRAM (plaintext or encrypted), DRAM (plaintext)	“# no radius-server key”
TACACS+ secret	Shared Secret	At least eight characters	The TACACS+ shared secret. It is entered by the Crypto Officer. This shared secret is zeroized by executing the “no tacacs-server key” command.	NVRAM (plaintext or encrypted), DRAM (plaintext)	“# no tacacs-server key”

TLS Server RSA private key	RSA	1024/1536 /2048-bits bits[4]	Identity certificates for module itself and also used in TLS negotiations. This CSP is used for both SSL VPN and SIP Gateway Signaling Over TLS Transport. The TLS RSA private key will have an associated TLS RSA Authentication public key.	NVRAM (plaintext or encrypted)	Automatically when session terminated
TLS Server RSA public key	RSA	1024/1536 /2048-bits bits[4]	Identity certificates for module itself and also used in TLS negotiations. This CSP is used for both SSL VPN and SIP Gateway Signaling Over TLS Transport. The TLS RSA public key will have an associated TLS RSA Authentication private key.	NVRAM (plaintext or encrypted)	Automatically when session terminated
TLS pre-master secret	Shared Secret	384	Shared secret created using asymmetric cryptography from which new session keys can be derived. This key was entered into the module via RSA key wrapping.	DRAM (plaintext)	Automatically when session terminated
SSL Traffic Keys	Triple-DES/AES/HMAC SHA-1 keys	Triple-DES (168 bits)/AES (128/192/256-bits)/HMAC (160-bits)	Derived in the module. Used to protect the traffics between SSL/TLS VPN peers.	DRAM (plaintext)	Automatically when session terminated

Table 5: Cryptographic Keys and CSPs

[3] Please note that the use of Diffie-Hellman keys that are less than 2048 bits are not allowed. Only 2048 bits must be used.

[4] Please note that RSA 1024 bits and 1536 bits are allowed only for Signature Verification. Key Generation and Signature Generation no longer allow the use of 1024 and 1536 bit keys.

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed below.

	CSP	DRBG V	DRBG Key	Diffie Hellman private exponent	Diffie Hellman Shared Secret	Skeyid	skeyid_d	IKE session encrypt key	IKE session authentication key	ISAKMP preshared	IKE RSA Authentication private Key	IPSec encryption key	IPSec authentication key	GDOI Key encryption Key (KEK)	GDOI Traffic Encryption Key (TEK)	GDOI TEK Integrity Key	SSH RSA Private Key	SSH session key	SSH session authentication key	User password	Enable password	Enable secret	RADIUS secret	TACACS+ secret
Role/Service																								
User Role																								
Status Function																								
Network Function		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r				
Terminal Function																								
Directory Services																								
Perform Self-tests																								
VPN Function						r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d					
CO Role																								
Configure the module											r w													
Define Rules and Filters																								
Status Functions																								
Manage the module		d	d																	r w d	r w d	r w d	r w d	r w d
Set Encryption/ Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d	r w d	r w d					
Perform Self-tests																								

r = read w = write d= delete

Table 6: CSP/Role/Service Access Policy

2.7 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. All self-tests are implemented by the firmware and associated hardware component. An example of self-tests run at power-up is a cryptographic known answer test (KAT) on each of the FIPS-approved cryptographic algorithms and on the Diffie-Hellman algorithm. Examples of tests performed at startup are a software integrity test using an EDC. Examples of tests run periodically or conditionally include: a bypass mode test performed conditionally prior to executing IPSec, and a continuous random number generator test. If any of self-tests fail, the router transitions into an error state. In the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Examples of the errors that cause the system to transition to an error state:

- IOS image integrity checksum failed
- Microprocessor overheats and burns out
- Known answer test failed
- NVRAM module malfunction.

2.7.1 Self-tests performed by the IOS and Hardware

- IOS Self Tests
    - POST tests
        - Firmware Integrity test
        - AES Known Answer test
        - DRBG Known Answer test
        - HMAC-SHA-1 Known Answer test
        - RSA Known Answer Test (both signature/verification)
        - SHA-1/256/512 Known Answer test
        - Triple-DES Known Answer test
    - Conditional tests
        - RSA PWCT test
        - Conditional bypass test
        - CRNG test on DRBG
        - CRNG tests on non-approved RNGs

- Hardware Self Tests
    - POST tests
        - AES Known Answer Test
        - HMAC-SHA-1 Known Answer Test
        - Triple-DES Known Answer Test

3 Secure Operation of the M3-SE-RTR2 and TXC3

The M3-SE-RTR2 and TXC3 module meets all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode.

Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 *Physical Security*

To ensure the physical security of the unit, inspect the installation of the tamper evident labels as described in Section 2.4. If the labels have not been installed, contact DTECH LABS, Inc. at support@dtechlabs.com or via phone at (877)-389-2772 to request the labeling kit (P/N: DT-FIPS-TEL) and refer to section 2.4 prior to proceeding.

3.2 *Initial Setup*

1. The Crypto Officer must disable IOS Password Recovery by executing the following commands:

   ```
   configure terminal
   no service password-recovery
   end
   show version
   ```

   NOTE: Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

3.3 *System Initialization and Configuration*

1. The Crypto Officer must perform the initial configuration. IOS version 15.2(2)GC, filename: c5915-adventerprisek9-mz.SPA.152-2.GC.bin is the only allowable image; no other image should be loaded.
2. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

   ```
   config-register 0x0102
   ```

3. The Crypto Officer must create the “enable” password for the Crypto Officer role. The password must be at least 8 characters (all digits; all lower and upper case letters; and all special characters except ‘?’ are accepted) and is entered when the Crypto Officer first engages the “enable” command. The Crypto Officer enters the following syntax at the “#” prompt:

   ```
   enable secret [PASSWORD]
   ```

4. The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

   ```
   line con 0
   password [PASSWORD]
   ```

```
        login local
```

5. The Crypto Officer shall only assign users to a privilege level 1 (the default).
6. The Crypto Officer shall not assign a command to any privilege level other than its default.
7. The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. RADIUS and TACACS+ shared secret key sizes must be at least 8 characters long.

3.4 IPSec Requirements and Cryptographic Algorithms

1. The only type of IPSec key establishment methods that is allowed in FIPS mode are Internet Key Exchange (IKE) and Group Domain of Interpretation (GDOI).
2. Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

   ah-sha-hmac

   esp-sha-hmac

   esp-3des

   esp-aes
3. The following algorithms are not FIPS approved and should not be used during FIPS-approved mode:

   DES

   DES MAC

   HMAC MD4

   HMAC MD5

   MD4

   MD5

   RC4

3.5 Protocols

1. SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP *gets* and *sets*. Since SNMP v2C uses community strings for authentication, only *gets* are allowed under SNMP v2C.

3.6 Remote Access

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec, using FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.

2. SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.

3.7 HTTPS/TLS management is not allowed in FIPS mode.

3.8 Identifying Operation in an Approved Mode

The following activities are required to verify that that the module is operating in an Approved mode of operation.

1. Verify that the length of User and Crypto Officer passwords and all shared secrets are at least eight (8) characters long, include at least one letter, and include at least one number character, as specified in the "Secure Operation of the M3-SE-RTR2 and TXC" section of this document.

2. Issue the following commands: 'show crypto ipsec sa', 'show crypto isakmp policy', and 'show crypto gdoi policy'. Verify that only FIPS approved algorithms are used.

3.9 Notes on Services

All services are available in both FIPS and non-FIPS mode, therefore it is the Crypto Officers' responsibility to ensure the following configurations in FIPS and Non-FIPS modes respectively:

For **FIPS mode**:

- Disable Telnet access. Users should log in using **SSHv2** only. (V1 is not compliant)
- Disable remote authentication through RADIUS/TACACS+. Only users local to the switch can be authenticated.
- Disable SNMP v1 and v2. Any existing user accounts on the switch that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy. SNMP v3 over a **secure IPSec** tunnel may be employed for authenticated, secure SNMP *gets* and *sets*. Since SNMP v2C uses community strings for authentication, only *gets* are allowed under SNMP v2C.
- Disable VRRP.
- Delete all IKE policies that either have MD5 for authentication or DES for encryption. Modify the policies so they use SHA for authentication and 3DES/AES for encryption.
- Delete all SSH Server RSA1 key-pairs.
- Disable HTTP Web-server
- Only allow SCP for copying files (Secure Copy with SSH)

- Only key sizes with strengths equal to or greater than 112 bits of security are allowed

Non-FIPS Mode:

- Telnet Access allowed
- Smaller passwords sizes may be alowed
- Remote authentication is allowed as it uses TCP for transport and both username/pass are encrypted
- SNMPv1-3 may be used
- VRRP may be allowed
- No restriction on IKE policy algorithms
- SSHv1 may be allowed
- HTTP web-server may be allowed
- May allow file transfer types allowed (ftp, scp, rcp, tftp..etc)
- Key sizes with strengths less than 112 bits of security are allowed