Ciena® Corporation

565/5100/5200 Advanced Services Platform

FW Version: 11.2 and 11.21
HW Versions:
565 – Chassis (NT0H50DAE5 REV 004), Backplane SP Card (NT0H5066E5 Rev 04), QOTR/E Card (NT0H25BAE5 Rev 2), Filler Card (NT0H52ABE6 Rev 02);
5100 – Chassis (NTPM50AAE5 Rev 11), SP Card (NT0H41ABE5 Rev 8), QOTR/E Card (NT0H25BAE5 Rev 2), Filler Card (NT0H52ABE6 Rev 02);
5200 – Chassis (NT0H50AA Rev 014), SP Card (NT0H41ABE5 Rev 8), QOTR/E Card (NT0H25BAE5 Rev 2), OCM Card (NT0H40BCE5 Rev 18), Filler Card (NT0H52ABE6 Rev 02)

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.9

Prepared for:

Ciena® Corporation
1201 Winterson Road
Linthicum, MD 21090
United States of America

Phone: +1 (613) 599-6430
Email: feedback@ciena.com
http://www.ciena.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the 565/5100/5200 Advanced Services Platform from Ciena. This Security Policy describes how the 565/5100/5200 Advanced Services Platform meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) 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 the National Institute of Standards and Technology (NIST) and the Communication Security Establishment Canada (CSEC): http://csrc.nist.gov/groups/STM/cmvp.

The 565/5100/5200 Advanced Services Platforms are referred to in this document as the 565/5100/5200, the cryptographic modules, shelves (or shelf) or the modules. Additionally, each individual shelf is distinctively referred to by its model number: i.e., 565, 5100 or 5200.

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. Additional information for these modules is available from the following sources:

- The Ciena website (http://www.ciena.com/) contains information on the full line of products from Ciena.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

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

- Vendor Evidence document
- Finite State Model
- FIPS security kit
- Other Ciena technical documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Ciena. With the exception of this non-proprietary Security Policy, the FIPS 140-2 validation submission documentation is proprietary to Ciena and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Ciena.

2 565/5100/5200

2.1 Overview

The 565/5100/5200 product family of carrier-grade products consist of high-availability, configurable Wavelength Division Multiplexing (WDM) devices that integrate security capability into rack-mountable shelves. There are three separate chassis (shelves) in the 565/5100/5200 product family, as shown in Figure 2, Figure 3 and Figure 4 respectively (with front cover removed). The smallest device is the 565, and the two larger shelves are the 5100 and 5200.

The 565 is a compact and cost-optimized WDM platform that enables a variety of data, storage and video services to be cost-efficiently aggregated onto an optical wavelength-based network or service. The 5100 and 5200 are the leading convergence platforms for WDM applications. The 565/5100/5200 devices specialize in converging multiple networks into a simple, scalable and secure network.

The modules are intended to be deployed in high-bandwidth, high-availability (99.999% availability) networks. The highest-capability modules (5200) are intended to handle core networking, and the smaller platforms (5100 or 565) are designed for handling lower bandwidth requirements, as shown in Figure 1.

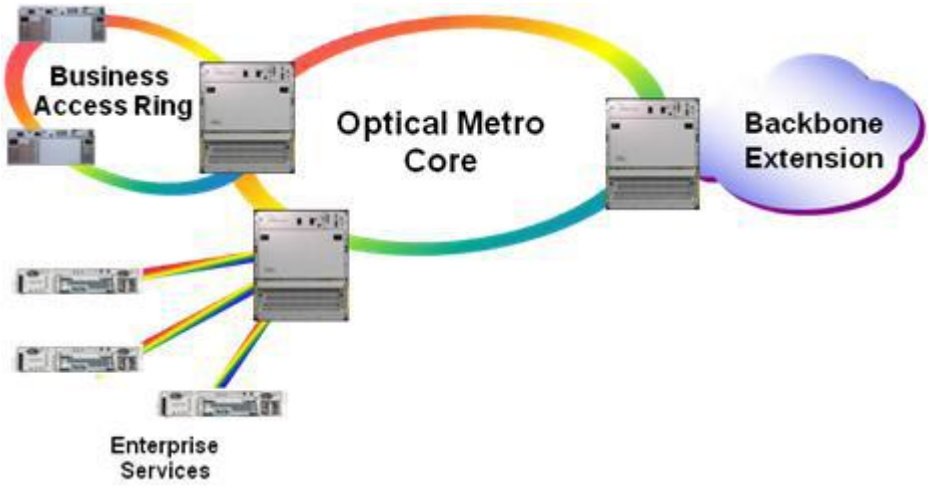

Figure 1 – 565/5100/5200 Shelf Deployment

The 565/5100/5200 shelves accept high-speed incoming traffic from numerous sources in many formats, encrypt the traffic, and then modulate the protected aggregate traffic as wavelengths on high-density fibre transmission lines. For example, an enterprise might place one 565 shelf at each of its locations, sending traffic over an optical metro core network to a headquarters' location with a 5200 shelf.

The 565/5100/5200 is validated at the FIPS 140-2 Section levels listed in Table 1. The overall security level of the module is 2. There are two validated versions of the 565/5100/5200, version 11.2 and version 11.21. 565/5100/5200 firmware version 11.21 includes a number of operational enhancements documented in Ciena PCN-0975-002. The issues rectified include:

- Automatic protection switch failure on 10G Muxponder connections with 1+1 line-side Automatic Protection Switching configuration as described in FSB 101-2012-139
- Loss of database redundancy on 5100 shelves - upon upgrade to Release 11.20, 5100 shelves may experience a loss of database redundancy leading to the network element getting into a Loss of Visibility state.

- Timing references may be invalidated on MOTR 20G cards - valid Layer 1 timing references may be invalidated in cases of persistent loss of signal on the line port, leading to potential bit errors until card is restarted.

The cryptographic and security features of both releases are identical.

Table 1 – Security Level Per FIPS 140-2 Section

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

2.2 Module Specification

All three of the 565/5100/5200 Advanced Services Platforms are hardware modules with multi-chip standalone embodiments. They are validated at overall Level 2 as shown in Table 1 above, with section 3 validated at Level 3. Sections 6 and 11 are not applicable to this hardware module validation.

The cryptographic boundary of the modules is defined as follows:

- The 565 cryptographic boundary surrounds the entire chassis
- The 5100 cryptographic boundary surrounds the front panel section of the chassis and the entire backplane main-board
- The 5200 cryptographic boundary surrounds the front panel section of the chassis and the entire backplane main-board

Each 565, 5100 and 5200 module contains a high-speed backplane main-board. The backplane is logically divided into two sections: the maintenance panel section and the front panel section. The maintenance panel section (top section) of the backplane provides ports and interfaces for configuring and managing the module, whereas the front panel section of the backplane provides circuit pack card interfaces (also referred to as slots). The circuit pack card interfaces can be populated with a number of circuit pack cards (also known as cards) that provide communications, security, and management services. The 5200 is a rack-mountable chassis (Part # NT0H50AA Rev 014) featuring twenty slots, and can accommodate up to sixteen traffic-carrying circuit packs for metro WDM deployments. The four other slots are reserved for special functions and are not available for traffic-carrying circuit packs. The 5100 is a smaller unit (Chassis Part # NTPM50AAE5 Rev 11) with six slots, four of which can accommodate circuit packs and two of which are

[1] N/A – Not Applicable
[2] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

reserved for non-traffic carrying functions. The 565 unit (Chassis Part # NT0H50DAE5 REV 004) provides the same type of services but has only three slots, two of which are available for traffic-carrying circuit packs. Various circuit pack cards that can be inserted into any of the 565/5100/5200 chassis are listed in Table 2. The 565/5100/5200 modules were tested and validated using only the circuit pack cards that are indicated with an asterisk (*) in Table 2. All other circuit pack cards are not included in the current validation.

Table 2 – List of Circuit Pack Cards

Cards	565	5100	5200
*Optical Transponder (OTR) 10G Quad with Encryption (QOTR/E) (Part # NT0H25BAE5 Rev 2)	✓	✓	✓
*Enhanced Shelf Processor (eSP) (Part # NT0H41ABE5 Rev 8)	N/A	✓	✓
*Optical Channel Manager (OCM) (Part # NT0H40BCE5 Rev 18)	N/A	N/A	✓
Optical Channel Laser/Detector (OCLD)	N/A	✓	✓
Optical Transponder (OTR)	✓	✓	✓
Optical Transponder (OTR) 10G Quad (QOTR)	✓	✓	✓
Multiplexer Optical Transponder (MOTR)	✓	✓	✓
Optical Channel Interface (OCI)	N/A	✓	✓
Automatic Per-Band Equalizer (APBE)	N/A	N/A	✓
Optical Fiber Amplifier (OFA)	N/A	N/A	✓
Optical Service Channel (OSC)	N/A	✓	✓
*Filler Card (Part # NT0H52ABE6 Rev 02)	✓	✓	✓
*Backplane SP Card (Part #NT0H5066E5 Rev 04)	✓	N/A	N/A

Most of the circuit pack cards listed in Table 2 are data carrying traffic cards. The circuit pack cards that are capable of performing cryptographic operations or store cryptographic keys or CSP[3]s are:

- The QOTR/E circuit pack card, which occupies two slot spaces in a chassis.
- The eSP circuit pack card, which occupies one non-traffic-carrying slot in the 5100 and 5200. (The 565 does not require an eSP card since its functionality is integrated into the 565 using the Shelf

[3] CSP – Critical Security Parameter

Processor (SP) card) For the rest of this document, both the SP and eSP circuit pack cards will be referred to jointly as an SP card.

- The OCM circuit pack card, which occupies one non-traffic-carrying slot in 5200. The OCM card acts as a cross point switch and manages the flow of traffic inside the 5200 module. On the 5200 devices, the OCM card is also used for storing the database containing configuration details, user credentials and various keys and CSPs. This card cannot be installed on 5100 or 565.

There are multiple combinations the 565/5100/5200 modules can be configured using various available circuit pack cards. Although Ciena affirms that the module can be configured with any particular combination of circuit pack cards, the modules were tested and validated only with the configuration detailed in Table 3.

Table 3 – 565/5100/5200 Advanced Services Platform Tested Configuration

Module Name	Configuration
565 Advanced Services Platform NT0H50DAE5 REV 004	1x SP Card NT0H5066E5 Rev 04 1x QOTR/E Card NT0H25BAE5 Rev 2 1x Filler Card NT0H52ABE6 Rev 02 1x FIPS Security Kit NT0H25BZ Rev 3
5100 Advanced Services Platform NTPM50AAE5 Rev 11	1x SP Card NT0H41ABE5 Rev 8 2x QOTR/E Card NT0H25BAE5 Rev 2 1x Filler Card NT0H52ABE6 Rev 02 1x FIPS Security Kit NT0H25BZ Rev 3
5200 Advanced Services Platform NT0H50AA Rev 014	1x SP Card NT0H41ABE5 Rev 8 8x QOTR/E Card NT0H25BAE5 Rev 2 2x OCM Card NT0H40BCE5 Rev 18 1x Filler Card NT0H52ABE6 Rev 02 1x FIPS Security Kit NT0H25BZ Rev 3

More detailed information about the placement of the circuit pack cards into the modules is provided in the list below:

- 565 – one SP card (which is incorporated as part of the chassis), one QOTR/E card (utilizing slots 1-2), and one filler card in slot 3
- 5100 – one SP card (slot 5), one Filler card (slot 6), and two QOTR/E cards (utilizing slots 1-2 & 3-4)
- 5200 – one SP card (slot 19), two OCM cards (slots 9 & 10), one Filler card (slot 20), and eight QOTR/E cards (utilizing the remaining slots)

Ciena affirms that the 565/5100/5200 modules can be configured with any combination of cards under the following conditions:

- The module shall contain one SP card at all times
- In the case of the 5100, the slot number 5 is reserved for the SP circuit pack card and the slot number 6 is reserved for an OSC circuit pack card
- In the case of the 5200, the slot number 9 and 10 is reserved for OCM circuit pack cards, the slot number 19 is reserved for the SP circuit pack card and the slot number 20 is reserved for an OSC circuit pack card

Circuit pack cards are available for most physical network interface types and speeds such as Gigabit Ethernet, 10 Gigabit Ethernet, and multiple capacities of Fibre-Channel and Optical Carrier circuits (OC-n). Some cards contain SFP[4] and XFP[5] pluggable units for both line-side and client-side entities that enable the

[4] SFP – Small Form-factor Pluggable

cards to operate at different wavelengths or protocol rates. Different circuit packs may also have different form-factors occupying one, two, three, or four slots. Circuit packs are inserted into available slots following the restrictions as mentioned above. The remaining empty slots receive filler cards to maintain air-flow through the chassis.

Neither the traffic-carrying cards mentioned above nor the SP card has the ability to perform bulk encryption at line speed. Only the QOTR/E circuit pack card, which includes a separate encryption chip (FPGA[6]), is capable of performing AES[7]-256 encryption at line speed (10 Gbps[8]) rates.

As previously noted, one SP card is required to operate and manage the shelf. On the 5200 and 5100, the SP is a separate card which occupies a reserved slot. On the 565 the SP card hardware is integrated into the chassis. Management traffic is directed to the SP. The SP is responsible for final transport of this traffic to all the other cards in the shelf across the backplane's bus. The management of the shelf is performed using these user interfaces:

- The System Manager Interface (SMI) manages the module using SNMP[9] v3. The SP will perform any required SNMP security, and then forwards commands to a destination card (QOTR/E card or other cards) across the backplane. The SNMP v1 and v2c protocols are disabled in FIPS-Approved mode of operation.
- The Optical Manager Element Adapter (OMEA) GUI[10] is used to manage the module using the TL1[11] management protocol commands.

2.3 Module Interfaces

The module's physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

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

Data input/output are the packets utilizing the services provided by the modules. Control input consists of Configuration or Administrative data entered into the modules. Any user can be given administrative capabilities only by the User with "Admin" privileges. Status output consists of the status provided by the logs, events, alarms via user interfaces. In the case of the 565, the status is also provided by the LEDs[12].

Each 565/5100/5200 module has a slightly different set of interfaces and therefore will be discussed separately. The 565/5100/5200 shelves each have card interfaces where any of the cards mentioned in Table 2 can be inserted.

2.3.1 565 Interfaces

The front panel of the 565 is shown in Figure 2 with front cover removed.

[5] XFP – 10 Gigabit Small Form-factor Pluggable
[6] FPGA – Field Programmable Gate Array
[7] AES – Advanced Encryption Standard
[8] Gbps – Gigabits per second
[9] SNMP – Simple Network Management Protocol
[10] GUI – Graphical User Interface
[11] TL1 – Transaction Language 1
[12] LEDs – Light Emitting Diodes

.

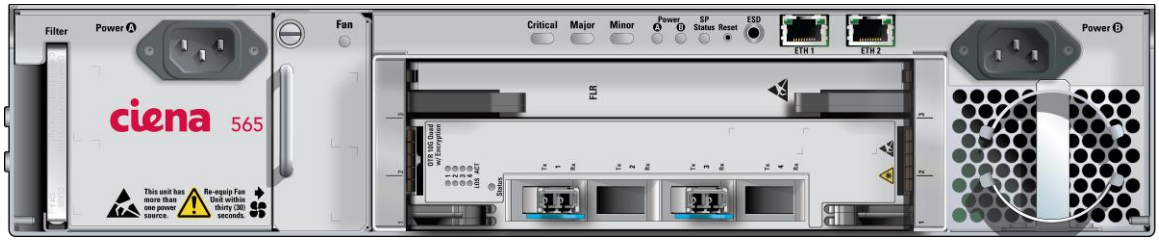

Figure 2 – 565 Front View

All of the 565 physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 4.

Table 4 – FIPS 140-2 Logical Interface Mappings for 565

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Ethernet ports	2	Data Input Data Output Control Input Status Output
QOTR/E Card Front Panel Interfaces	1	Data Input Data Output
Filler Card Interface slot	1	None
LEDs	3	Status Output
Power	2	Power Input

2.3.2 5100 Interfaces

The front panel of the 5100 is shown in Figure 3 with the front cover removed.

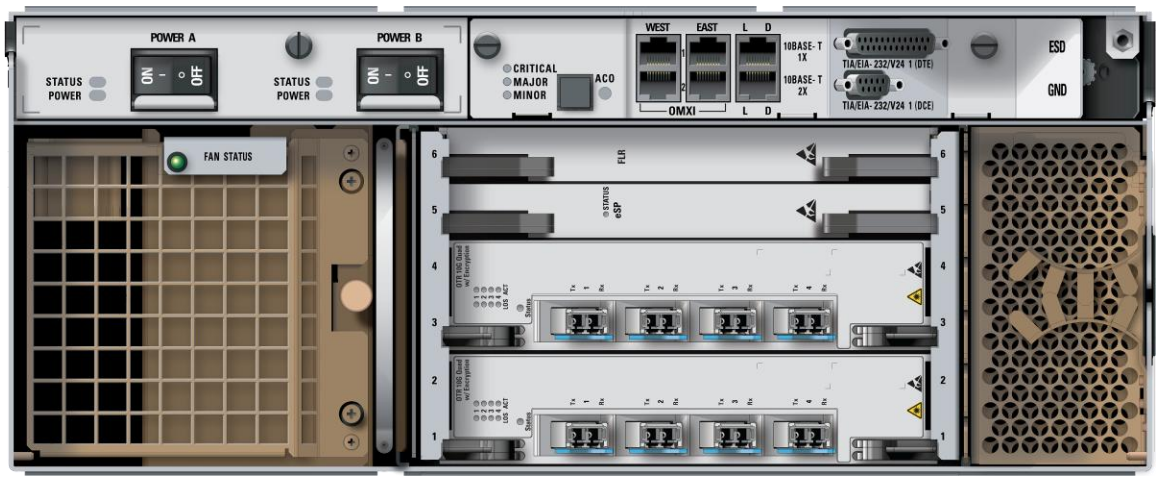

Figure 3 – 5100 Front View

.

All of the physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 5.

Table 5 – FIPS 140-2 Logical Interface Mappings for 5100

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Proprietary Backplane Interface for Maintenance Panel Card	1	Data Input Data Output Control Input Status Output
SP Card Front Panel Interfaces	1	None
QOTR/E Card Front Panel Interfaces	2	Data Input Data Output
FAN Status LED	1	Status Output
Proprietary Backplane Interface for Power Supply Card	2	Power Input

2.3.3 5200 Interfaces

The front panel of the 5200 is shown in Figure 4 with the front cover removed.

.

Figure 4 – 5200 Front View

All of the physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 6.

.

Table 6 – FIPS 140-2 Logical Interface Mappings for 5200

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Proprietary Backplane Interface for Telemetry card	2	Control Input Status Output
Proprietary Backplane Interface for OMX card	2	Control Input Status Output
Proprietary Backplane Interface for Alarm card	1	Control Input Status Output
Proprietary Backplane Interface for Ethernet card	1	Data Input Data Output Control Input Status Output
Proprietary Backplane Interface for Serial port	1	Control Input Status Output
SP Card Front Panel Interfaces	1	None
QOTR/E Card Front Panel Interfaces	8	Data Input Data Output
OCM Card Front Panel Interfaces	2	None
Proprietary Backplane Interface for Power Supply	2	Power Input

2.3.4 QOTR/E Card Interfaces

The QOTR/E card is a dual slot card, as pictured in Figure 5, which includes up to four XFP transceivers. Its XFP transceivers are hot-swappable, protocol-independent optical transceivers which either operate at a fixed wavelength within 5.0 to 11.1 Gbps or are tunable over a range of wavelengths. These four XFP interfaces provide two encrypted-line ports (port 1 and 2) and two clear-text ports (port 3 and 4). These ports can also be replaced to accommodate different wavelength interfaces (or protocols) for different network installations.

.

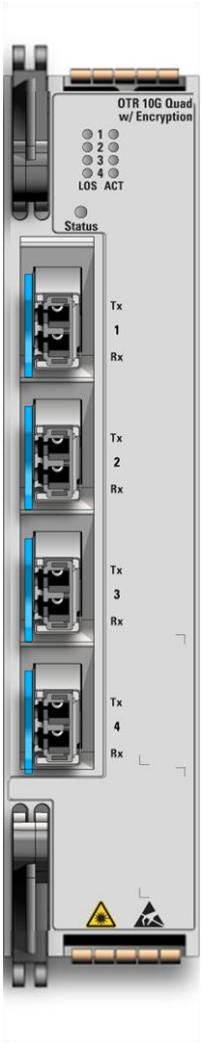

Figure 5 – QOTR/E Card Front Panel

All of the physical interfaces are separated into the logical interfaces defined by FIPS 140-2, as described in Table 7.

Table 7 – FIPS 140-2 Logical Interface Mappings for QOTR/E Card

Physical Port/Interface	Quantity	FIPS 140-2 Interface
XFP ports	4	Data Input Data Output
LEDs	9	None

2.3.5 SP Card Interfaces

The SP acts as a supervisory card for the 565/5100/5200 devices. Management traffic is directed to the SP, and then rerouted from the SP to other cards across the backplane bus. An SP is always configured into a

dedicated slot of the 5100 or 5200 shelf. A picture of an SP card is shown in Figure 6. The SP's physical interfaces are mapped into FIPS 140-2 logical interfaces in Table 8.

Figure 6 – SP Card Front Panel

Table 8 – FIPS 140-2 Logical Interface Mappings for SP Card

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Status LED	1	None

2.3.6 OCM Card Interfaces

The OCM card is a single slot card. The primary function of the OCM card is that of a cross point switch. The OCM card performs switching and manages the flow of traffic inside the module. The OCM card is also used for storing the database containing configuration details, user credentials and various keys and CSPs. The OCM card's physical interfaces are mapped into FIPS 140-2 logical interfaces as shown in Table 9.

Table 9 – FIPS 140-2 Logical Interface Mapping for OCM Card

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Status LED	1	None

.

2.4 Roles, Services and Authentication

The module supports identity-based authentication. There are two roles in the module (as required by FIPS 140-2) that users may assume: a Crypto Officer (CO) role and a User role. The User role is further sub-divided into classes based on their privileges as follows: Admin, Operator, Observer, Customer1 and Customer2. Descriptions of the services available to the Crypto Officer and User roles are provided below. Please note that the keys and Critical Security Parameters (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

2.4.1 Crypto Officer Role

The CO has the ability to provision and query cryptographic keys and CSPs. The CO has the ability to perform self test audits. Descriptions of the services available to the CO role are provided in Table 10 below.

Table 10 – Mapping of CO Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Change CO Password	Change the Crypto Officer (self) password via the SMI and TL1 interfaces	Command	Command response and status output	CO Password – W
Perform Self Tests	Perform on demand Power-up Self Tests by manually power cycling the module	Command	Command response	None
Show Status	Facilitates the user to check the current status of the module as well as check whether the module is in FIPS-Approved mode or not via the SMI and TL1 interfaces	Command and parameters	Status output	CO Password – X
Alarms Monitoring	Facilitates the user to view any active alarms via the SMI and TL1 interfaces	Command and parameters	Command response	CO Password – X
Events Monitoring	Facilitates the user to view all logged events via the SMI and TL1 interfaces	Command and parameters	Command response	CO Password – X

.

Service	Description	Input	Output	CSP and Type of Access
Zeroize Keys	Zeroize keys and CSPs over SMI	Command and parameters	Command response	CO Password – W SMI Session Monitor Key – W SNMPv3 Authentication Key – W SNMPv3 Privacy Key – W QOTR/E RSA Public Key – W QOTR/E RSA Private Key – W QOTR/E Authentication Pre-shared Key – W QOTR/E DH Key Pairs – W QOTR/E Message Authentication Key – W QOTR/E Message Encryption Key – W QOTR/E Session Encryption Key – W IKE DH Key Pairs – W IPSec IKE Message Authentication Key – W IPSec IKE Message Encryption Key – W IPSec IKE Session Encryption Key – W TLS/DTLS DH Key Pairs – W TLS/DTLS Session Key – W DRBG seed – W DRBG key value – W DRBG V value – W
ESA[13] Provisioning	Facilitates the user to configure the ESA RSA Passphrases for various QOTR/E cards over SMI	Command and parameters	Command response	CO Password – X ESA RSA Passphrase – W ESA RSA Encryption Key – W ESA RSA Signature Key – W
QOTR/E PSK provisioning	Facilitates the user to configure the QOTR/E Authentication Pre-shared Key for various QOTR/E cards via the SMI and TL1 interfaces	Command and parameters	Command response	CO Password – X QOTR/E Authentication Pre-shared Key – W

2.4.2 User Role

The User role is sub-divided into levels based on their privileges as follows: Admin, Operator, Observer, Customer1 and Customer2. The description of each user level is provided in Table 11 below.

[13] ESA – External Security Authentication

.

Table 11 – User Level Privileges

User Level	Description
Admin	The system administrator: • Has read and write access to all of the system configuration/status • Can commission and decommission shelves • Can view and clear security events and alarms • Can provision the severity of any alarm using System Manager • Can create, modify and delete other user profiles • Can zeroize keys on SP • Can perform on-demand power-up self tests • Can provision all data on the shelf with the exception of the Pre-Shared Key or certificate provisioning on the QOTR/E card
Operator	The typical user class: • Has read and write access to most of the system configuration/status • Can change user's own password
Observer	This user has read-only access; however, can change user's own password
Customer1	The Customer1 user: • Can access PM[14] data • Has read-only access to their customer owned network (equipment, facility and channel assignments) • Can change own password • Only sees service affecting alarms plus Optical Power, Far End Client Rx Signal Fail and PM alarms that concern their operation. All other events, user requests, and non-service affecting alarms are filtered
Customer2	The Customer2 user: • Can access PM data • Has read-only access to their customer owned network (equipment, facility and channel assignments) • Can change own password

Descriptions of the services available to the User role are provided in Table 12 below.

Table 12 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	User Level	Description	Input	Output	CSP and Type of Access
User Accounts Management	Admin	Manage various user accounts, password complexity and user privileges via the SMI and TL1 interfaces	Command and parameters	Command response	User Password – W, X

[14] PM – Performance Monitoring

.

Service	User Level	Description	Input	Output	CSP and Type of Access
Change User Password	Admin, Operator, Observer, Customer1, Customer2	Change the User (self) password via the SMI and TL1 interfaces	Command	Command response and status output	User Password – W
SNMP Configuration and Management	Admin	Facilitates the user to manage SNMP configurations via SMI only	Command and parameters	Command response	User Password – X SNMPv3 Authentication Key – W SNMPv3 Privacy Key – W SNMPv3 Proxy Authentication Key – X SNMPv3 Proxy Privacy Key – X
IPsec Configuration and Management	Admin	Facilitates the user to manage IPsec configurations via SMI only	Command and parameters	Command response	User Password – X IPSec IKE Authentication Pre-shared Key – X IKE DH Key Pairs – W IPSec IKE Message Authentication Key – W IPSec IKE Message Encryption Key – W IPSec IKE Session Encryption Key – W
Commission/ De-commission the Module	Admin	Commission/De-commission the module by following the user guides and Security Policy guidelines via SMI only	Command and parameters	Command response	None
Perform Self Tests	Admin	Perform on-demand Power-up Self Tests for the module by manually power cycling the module	Command	Command response	None

.

Service	User Level	Description	Input	Output	CSP and Type of Access
Show Status	Admin, Operator, Observer, Customer1, Customer2	Facilitates the user to check the current status of the module as well as check whether the module is in FIPS-Approved mode or not via the SMI and TL1 interfaces	Command and parameters	Status output	None
Alarms Monitoring	Admin, Operator, Observer, Customer1, Customer2	Facilitates the user to view any active alarms via the SMI and TL1 interfaces	Command and parameters	Command response	User Password – X
Events Monitoring	Admin, Operator, Observer, Customer1, Customer2	Facilitates the user to view all logged events via the SMI and TL1 interfaces	Command and parameters	Command response	User Password – X
Backup and Restore Database	Admin	Perform backup or restore of database containing authentication and configuration information via the SMI and TL1 interfaces	Command and parameters	Command response	Database Passphrase – W Database Encryption Key – W Database Signature Key – W
Software Upgrades	Admin	Facilitates the user to perform software upgrades via the SMI and TL1 interfaces	Command and parameters	Command response	User Password – X
Provision QOTR/E equipment	Admin, Operator	Facilitates the user to provision and configure various QOTR/E cards and related equipments in a module over the SMI and TL1 interfaces	Command and parameters	Command response	User Password – X

.

Service	User Level	Description	Input	Output	CSP and Type of Access
Provision QOTR/E facility	Admin, Operator	Facilitates the user to configure inventory and facility information over the SMI and TL1 interfaces	Command and parameters	Command response	User Password – X
Provision QOTR/E connections	Admin, Operator	Facilitates the user to provision and configure QOTR/E card connections over the SMI and TL1 interfaces	Command and parameters	Command response	User Password – X
Zeroize Keys	Admin	Zeroize keys and CSPs over SMI.	Command and parameters	Command response	CO or User Password – W RADIUS Shared Secret – W SMI Session Monitor Key – W SNMPv3 Authentication Key – W SNMPv3 Privacy Key – W SNMPv3 Proxy Authentication Key – W SNMPv3 Proxy Privacy Key – W ISA CA RSA Public Key – W ISA CA RSA Private Key – W ISA Shelf RSA Public Key – W ISA Shelf RSA Private Key – W QOTR/E DH Key Pairs – W QOTR/E Message – W Authentication Key – W QOTR/E Message Encryption Key – W QOTR/E Session Encryption Key – W IPSec IKE Authentication Pre-shared Key – W IKE DH Key Pairs – W IPSec IKE Message Authentication Key – W IPSec IKE Message Encryption Key – W IPSec IKE Session Encryption Key – W TLS/DTLS DH Key Pairs – W TLS/DTLS Session Key – W DRBG seed – W DRBG key value – W DRBG V value – W

.

Service	User Level	Description	Input	Output	CSP and Type of Access
ISA[15] Provisioning	Admin	Facilitates the user to provision and configure Inter-shelf communications such as notifications, shelf enrollment, etc over SMI	Command and parameters	Command response	User Password – X ISA CA RSA Public Key – X ISA CA RSA Private Key – X ISA Shelf RSA Public Key – X ISA Shelf RSA Private Key – X ISA RSA Passphrase – W ISA RSA Encryption Key – W ISA RSA Signature Key – W

2.4.3 Authentication

All services provided by the module require the user to assume a role and a specific identity. The module provides services only to authenticated users. The module performs identity-based authentication.

All users authenticate to the module using a username and password. All users are required to follow the complex password restrictions.

Table 13 lists the authentication mechanisms used by the module.

[15] ISA – Inter-shelf Security Authentication

.

Table 13 – Authentication Mechanism

Authentication Type	Strength
Password	The minimum length of the password is eight characters, with 86 different case-sensitive alphanumeric characters and symbols possible for usage. The chance of a random attempt falsely succeeding is 1: (86^8), or 1: 2,992,179,271,065,856. The fastest network connection supported by the module is 100 Mbps. Hence at most (100 $\times 10^6$ × 60 = 6 × 10^9 =) 6,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is 1 : [86^8 possible passwords / ((6 $\times 10^9$ bits per minute) / 64 bits per password)] 1: (86^8 possible passwords / 93,750,000 passwords per minute) 1: 31,916,578 or 1 in 31.9 million, which is less than 100,000 as required by FIPS 140-2
Public Key Certificates	The module supports RSA[16] digital certificate authentication of users during IPsec/IKE[17]. Using conservative estimates and equating a 2048 bit RSA key to a 112 bit symmetric key, the probability for a random attempt to succeed is 1:2^{112} or 1: 5.19 x 10^{33}. The fastest network connection supported by the module is 100 Mbps. Hence at most (100 $\times 10^6$ × 60 = 6 × 10^9 =) 6,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is 1: (2^{112} possible keys / ((6 × 10^9 bits per minute) / 112 bits per key)) 1: (2^{112} possible keys / 53,571,428 keys per minute) 1: 96,922,874,692,650,115,732,569,264 or 1 in 96.9 septillion, which is less than 100,000 as required by FIPS 140-2.

Simple Network Management Protocol (SNMP) v1/v2 services are disabled in the FIPS-Approved mode of operation. SNMP v3 is used only for management-related services. RADIUS[18] server authentication is secured over IPsec.

2.5 Physical Security

The 565/5100/5200 shelves are multi-chip standalone cryptographic modules.

All of the module's components are made up of production-grade material. The modules are enclosed in a hard and opaque metal case that completely encloses all of its internal components. There are only a limited set of vent holes provided in the case, and the view of the internal components of the module is obscured. Tamper-evident labels are applied to the case as well as removable front and rear covers to provide physical evidence of attempts to gain access to the module's internal components. All tamper evident labels are serialized and uniquely identified. The tamper-evident labels are silver seals with self-adhesive backings, as shown in Figure 7. The labels provide evidence of tampering when any unauthorized access to the module is attempted. Any attempt to access the module will result in one or more of the tamper-evident labels being damaged. A "dot" pattern is revealed when the label is removed or tampered with, as shown in Figure 8. The placement of tamper-evident labels can be found in Section 3.1 of this document. The CO must periodically ensure that the labels or shelves do not show any signs of tampering. Section 3.2.2 describes the physical security inspection methods the CO should follow.

[16] RSA – Rivest, Shamir and Adleman
[17] IKE – Internet Key Exchange
[18] RADIUS – Remote Authentication Dial In User Service

.

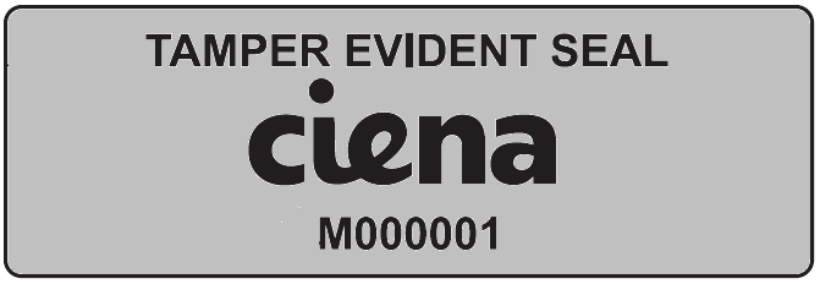

Figure 7 – Tamper Evident Label

Figure 8 – Evidence of Tampering

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

2.6 Operational Environment

FIPS 140-2 Operational Environment requirements do not apply to the 565/5100/5200 shelves, because these modules do not provide a general-purpose operating system (OS) to the user.

All firmware upgrades are digitally-signed and a self-test is performed during each upgrade.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms in Table 14.

Table 14 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number	
	SP	QOTR/E
AES-256 in ECB and Counter mode	N/A	1682
AES-128, AES-192 and AES-256 in CBC mode	1794	1796
AES-128, AES-192 and AES-256 in CFB-128 mode	1794	N/A
Triple-DES (Encrypt/Decrypt) in CBC mode (Three-Key)	1161	N/A
SHA-1, SHA-256 and SHA-512	1576	1578

.

Algorithm	Certificate Number	
	SP	QOTR/E
RSA ANSI X9.31 Key-pair Generate(2048 and 4096)	897	899
RSA PKCSv1.5 Signature Generate/Verify (2048 and 4096)	897	899
HMAC using SHA-1 and SHA-256	1058	1060
SP 800-90 (Counter based DRBG)	130	131

The module utilizes the following non-FIPS-approved but FIPS-allowed algorithm implementation:

- Diffie-Hellman (DH) for key agreement during IPsec: 2048-bit key (provides 112 bits of security)

Additionally, the module implements the following non-FIPS-approved algorithm that are disabled by default and not allowed for use in the FIPS-Approved mode of operation:

- MD5
- DES
- Blowfish

.

The module supports the critical security parameters (CSPs) as shown in Table 15.

Table 15 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
CO or User Password	Alpha-Numeric string	Entered into module over Ethernet port via SNMPv3 or IPSec	Exits the module in encrypted format as a part of the backup file	Stored within the module in plaintext in SP RAM[19] as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues zeroization commands over SMI or when the password is updated with a new one	Used for authenticating all Crypto Officers and Users
Database Passphrase	Alpha-Numeric string	Entered into module (by Admin Users only) over Ethernet port via SNMPv3 or IPSec	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	Used for deriving keys which are used to encrypt and sign the database file while performing database backup or restore functions

[19] RAM – Random Access Memory

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
Database Encryption Key	AES-256 key	Derived internally from Database Passphrase following the SP 800-132 specification (Section 5.4, Option 1)	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	These key is derived from Database Passphrase. This key is used to encrypt or decrypt the database backup/restore file
Database Signature Key	HMAC-SHA 256 key	Derived internally from Database Passphrase following the SP 800-132 specification (Section 5.4, Option 1)	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	These key is derived from Database Passphrase. This key is used to sign or verify the database backup/restore file
RADIUS Shared Secret	Shared secret	Entered into module over Ethernet port via SNMPv3 or IPSec	Exits the module in encrypted format as a part of the backup file	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues re-provisioning / reset commands over SMI	RADIUS server authentication for users
SMI Session Monitor Key	HMAC SHA-1-96 key	Generated internally by the SP during startup	Never exits the module	Stored within the module in plaintext in SP RAM			Zeroization can be performed by SP reboot	It is used to maintain and monitor the connectivity during a user session over SMI

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
SNMPv3 Authentication Key	HMAC SHA-1-96 key	Generated internally every time after SMI session is initiated	Exits the module over TLS	Stored within the module in plaintext in SP RAM			Zeroized with session termination	Used for authentication during user SMI sessions via SNMPv3
SNMPv3 Privacy Key	AES-128 key	Generated internally every time after SMI session is initiated	Exits the module over TLS	Stored within the module in plaintext in SP RAM			Zeroized with session termination	Used to encrypt user SMI sessions over SNMPv3
SNMPv3 Proxy Authentication Key	HMAC SHA-1-96 key	Default key; but can be modified by the User with Admin privileges	Exits the module in encrypted format as a part of the backup file	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues zeroization commands or when updated with a new one	Used for authentication during inter-shelf communication via SNMPv3
SNMPv3 Proxy Privacy Key	AES-256 key	Default key; but can be modified by the User with Admin privileges	Exits the module in encrypted format as a part of the backup file	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues zeroization commands or when updated with a new one	Used to encrypt inter-shelf communication over SNMPv3

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
ISA CA RSA Public Key	RSA-2048 Public Key	The module's Public key is generated by an SP card in the Enterprise primary shelf; In a peer shelf, the public key of the CA enters the module in plaintext	Exits the primary shelf module in encrypted format as a part of the backup file or in plaintext over secure TLS channel	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues zeroization commands over SMI	Used for authentication
ISA CA RSA Private Key	RSA-2048 Private Key	Generated internally by an SP card in the Enterprise primary shelf. No Private Key exists in a non-primary shelf	Never exits the module	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues zeroization commands over SMI	Used to sign other shelf certificates
ISA Shelf RSA Public Key	RSA-2048 Public Key	The module's Public key is generated by the SP card; a peer's ISA Shelf RSA Public Key enters the module in plaintext in a certificate	Exits the module in encrypted format (using ISA RSA Encryption Key) as a part of the enrolment process	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues zeroization commands over SMI	Each shelf has to have their own Shelf certificate that needs to be signed by the primary Shelf CA

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
ISA Shelf RSA Private Key	RSA-2048 Private Key	The module's Private key is generated internally only by the SP card	Exits the module in encrypted format (using ISA RSA Encryption Key)	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues zeroization commands over SMI	Used for authentication
ISA RSA Passphrase	Alpha-Numeric string	Entered into module (by Admin Users only) over Ethernet port via SNMPv3 or IPSec	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	Used for deriving keys which are used to encrypt and sign the ISA RSA key file; before exporting the RSA key file.
ISA RSA Encryption Key	AES-256 key	Derived internally from ISA RSA Passphrase following the SP 800-132 specification (Section 5.4, Option 1)	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	These key is derived from ISA RSA Passphrase. This key is used to encrypt or decrypt the ISA RSA key file
ISA RSA Signature Key	HMAC-SHA 256 key	Derived internally from ISA RSA Passphrase following the SP 800-132 specification (Section 5.4, Option 1)	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	These key is derived from ISA RSA Passphrase. This key is used to sign or verify the ISA RSA key file

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
QOTR/E RSA Public Key	RSA-2048 Public Key	Imported in an encrypted format (ESA RSA Encryption Key) format	Exits the module in encrypted format (using ESA RSA Encryption Key)	Stored within the module in encrypted format (via ESA RSA Encryption Key) format in QOTR/E flash memory			Zeroized when a CO issues zeroization commands over SMI	Used for authentication before encrypting traffic data
QOTR/E RSA Private Key	RSA-2048 Private Key	Imported in an encrypted format (ESA RSA Encryption Key) format	Exits the module in encrypted format (using ESA RSA Encryption Key)	Stored within the module in encrypted format (via ESA RSA Encryption Key) format in QOTR/E flash memory			Zeroized when a CO issues zeroization commands over SMI	Used for authentication before encrypting traffic data
ESA RSA Passphrase	Alpha-Numeric string	Entered into module (by CO users only) over Ethernet port via SNMPv3 or IPSec	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	Used for deriving keys which are used to install the ESA RSA keys on a QOTR/E card.
ESA RSA Encryption Key	AES-256 key	Derived internally from ESA RSA Passphrase following the SP 800-132 specification (Section 5.4, Option 1)	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	These key is derived from ESA RSA Passphrase. This key is used to encrypt or decrypt the ESA RSA key file

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
ESA RSA Signature Key	HMAC-SHA 256 key	Derived internally from ESA RSA Passphrase following the SP 800-132 specification (Section 5.4, Option 1)	Never exits the module	Stored within the module in plaintext in RAM			Zeroized when module reboots	These key is derived from ESA RSA Passphrase. This key is used to sign or verify the ESA RSA key file
QOTR/E Authentication Pre-shared Key	Alpha-Numeric string	Entered into module (by CO users only) over Ethernet port	Exits the module in encrypted format as a part of the backup file	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a CO issues zeroization commands over SMI	Used for peer authentication before encrypting traffic data
QOTR/E DH Key Pairs	2048-bit DH key pairs	Generated internally during DH key negotiation	The module's Public key is generated internally; while public key of a peer enters the module in plaintext. Private key never exits the module	Stored within the module in plaintext in QOTR/E RAM			Zeroization can be performed by reboot or session termination	Exchanging shared secret to derive encryption keys
QOTR/E Message Authentication Key	HMAC-SHA 256	Generated internally during DH key negotiation	Never exits the module	Stored within the module in plaintext in QOTR/E RAM			Zeroization can be performed by reboot or session termination	Used for peer authentication before encrypting messages
QOTR/E Message Encryption Key	AES 256	Derived from DH key negotiation	Never exits the module	Stored within the module in plaintext in QOTR/E RAM			Zeroization can be performed by reboot or session termination	Used to encrypt peer-to-peer messages

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
QOTR/E Session Encryption Key	AES 256	Derived from DH key negotiation	Never exits the module	Stored within the module in plaintext in QOTR/E RAM			Zeroization can be performed by reboot or session termination	Used to encrypt traffic data
IPSec IKE Authentication Pre-shared Key	Alpha-Numeric string	Entered into module (by Admin Users only) over Ethernet port	Exits the module in encrypted format as a part of the backup file	Stored within the module in plaintext in SP RAM as well as on OCM card flash memory	Stored within the module in plaintext in SP RAM and QOTR/E flash	Stored within the module in plaintext in SP RAM, SP flash and QOTR/E flash	Zeroized when a User with Admin privileges issues zeroization commands over SMI	Used for peer authentication before of IKE session
IKE DH Key Pairs	2048-bit DH key pairs	Generated internally during IKE negotiation	The module's Public key is generated internally; while public key of a peer enters the module in plaintext. Private key never exits the module	Stored within the module in plaintext in SP RAM			Zeroization can be performed by reboot or session termination	Exchanging shared secret to derive encryption keys during IKE
IPSec IKE Message Authentication Key	HMAC-SHA 256 or HMAC-SHA 1	Generated internally during DH key negotiation	Never exits the module	Stored within the module in plaintext in SP RAM			Zeroization can be performed by reboot or session termination	Used for peer authentication before encrypting IPSec packets
IPSec IKE Message Encryption Key	AES 128, AES 256 or Triple-DES (3 key)	Derived from DH key negotiation	Never exits the module	Stored within the module in plaintext in SP RAM			Zeroization can be performed by reboot or session termination	Used to encrypt peer-to-peer IPSec messages

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
IPSec IKE Session Encryption Key	AES 128, AES 256 or Triple-DES (3 key)	Derived from DH key negotiation	Never exits the module	Stored within the module in plaintext in SP RAM			Zeroization can be performed by reboot or session termination	Used to encrypt IPSec session data
TLS/DTLS DH Key Pairs	2048-bit DH key pairs	Generated internally during session negotiation by SP card	The module's Public key is generated internally; while public key of a peer enters the module in plaintext. Private key never exits the module	Stored within the module in plaintext in SP RAM			Zeroization can be performed by reboot or session termination	Exchanging shared secret to derive TLS/DTLS session keys
TLS/DTLS Session Key	Session key	Generated internally by the SP card	Never exits the module	Stored within the module in plaintext in SP RAM			Zeroization can be performed by reboot or session termination	Used to encrypt TLS/DTLS session data
DRBG seed	Random Value	Generated internally by all QOTR/E and SP card	Never exits the module	Stored within the module in plaintext in individual card RAM			Zeroization can be performed by reboot	Used to seed the DRBG
DRBG key value	Random value	Generated internally	Never exits the module	Stored within the module in plaintext in individual card RAM			Zeroized on reboot or when the values are updated based on the SP 800-90 specification	Used in the process of generating a random number

.

CSP	CSP Type	Generation / Input	Output	Storage			Zeroization	Use
				5200	5100	565		
DRBG V value	Random value	Generated internally	Never exits the module	Stored within the module in plaintext in individual card RAM			Zeroized on reboot or when the values are updated based on the SP 800-90 specification	Used in the process of generating a random number

.

2.8 Self-Tests

The 565/5100/5200 performs the Known Answer Tests (KAT) and Critical Function Tests at power-up as shown in Table 16.

Table 16 – Power-Up Self-Tests

Power-Up Test	Description
AES firmware KAT	KAT for AES-128, AES-192 and AES-256 in CBC and CFB-128 mode
AES hardware KAT (QOTR/E cards only)	KAT for AES-256 in ECB and counter mode
DRBG KAT	KAT for SP 800-90 Counter based DRBG
HMAC KAT	KAT for HMAC using SHA-1, SHA-1-96, SHA-256 and SHA-512
RSA key-pair KAT (QOTR/E cards only)	KAT for RSA key-pair generation
RSA pair-wise consistency test	KAT to test the RSA pair-wise consistency of generated key-pair
RSA sign/verify KAT	KAT for RSA signature generation/verification
SHA KAT	KAT for SHA-1, SHA-256 and SHA-512
SP and QOTR/E cards integrity test	Integrity test is performed on the load header as well as load body of SP and QOTR/E cards using 32-bit CRC
Triple-DES KAT	KAT for Triple-DES (Three-Key) in CBC mode

The 565/5100/5200 performs the power-up critical function tests as shown in Table 17.

Table 17 – Power-Up Critical Function Tests

Power-Up Test	Critical Function Tested
DRBG critical test	Critical function tests are performed for DRBG instantiation and reseed, as specified in SP 800-90
FPGA integrity test (QOTR/E cards only)	Integrity test is performed on the load binary of cryptographic FPGA present in QOTR/E card using 32-bit CRC
SP card load test (SP card only)	The firmware library is checked against the signature files using RSA every time the firmware is loaded on the SP card

The 565/5100/5200 performs the conditional self-tests as shown in Table 18.

.

Table 18 – Conditional Self-Tests

Conditional Test	Description
Continuous DRBG test	Continuous RNG test for SP 800-90 Counter based DRBG
Firmware upgrade test (SP card only)	Test is performed to verify the authenticity of the upgrades using RSA-2048
Manual key entry test	Manual key entry test is performed by forcing the operator to enter the manual key twice and comparing both keys
RSA pair-wise consistency test (QOTR/E cards only)	Test performed to check the RSA pair-wise consistency of generated key-pair

All previously mentioned self-tests are performed on a per card basis rather than at the module level.

2.9 Mitigation of Other Attacks

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

3 Secure Operation

The 565/5100/5200 meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 Initial Setup

Before powering-up the module, the CO must ensure that the required tamper-evident labels are correctly applied to the enclosure. The FIPS security kit (Part Number: NT0H25BZ Rev 3) consists of the following items:

- Tamper evident labels
- Alcohol wipe packs for cleaning the equipment prior to applying labels
- Security log book
- Security Policy CD[20] along with a printed copy

The CO shall perform the following steps to apply the tamper evident labels:

- Labels must be applied 1 hour before the module is placed into operation
- Ensure that the shelf surface temperature is above 10°C
- Clean all label placement locations using the alcohol wipe pack provided in the FIPS security kit. If the surface of the enclosure is extremely dirty or rough, scuff the painted area where label is to be applied prior to cleaning using a 400 grit emery paper (not a part of FIPS security kit)
- Ensure that the surface is clean and dry
- Apply the labels on the placement locations as described below:
    - Between the front panel and side (Label #1 and #2), between the top cover, side and maintenance panel (Label #3 and #4), between the rear panel and side (Label #5 and #6), between the rear panel and top cover (Label #7), and between the air filter and bottom chassis (Label #8), as shown in Figure 9 in the case of 5200;
    - Between the front panel and side (Label #1 and #2), between the rear panel and top cover (Label #3), and between the rear panel and bottom chassis (Label #4), as shown in Figure 10 in the case of 5100; or
    - Between the front panel and side (Label #1 and #2), between the top cover and side (Label #3 and #4), between the rear panel and side (Label #6), and between the rear panel and top cover (Label #5), as shown in Figure 11 in the case of 565
- Apply the labels firmly and please note that all the labels are wrapped around the edges
- Record the serial numbers on the labels along with its placement position in the security log book

[20] CD – Compact Disc

.

Figure 9 – Tamper Evident Label Placement for 5200

.

Figure 10 – Tamper Evident Label Placement for 5100

Figure 11 – Tamper Evident Label Placement for 565

3.2 Secure Management

The modules have a non-modifiable OS. A User with Admin privileges is responsible for commissioning the module. When a module is powered on for the first time, a User with Admin privileges must provision the module into FIPS mode by accessing the configuration tab and changing the "FIPS mode" field to "Enable". Once a module is provisioned into FIPS mode, the module will operate and remain in FIPS-Approved mode of operation unless the module is decommissioned by the User with Admin privileges or the physical security has been breached.

3.2.1 Initialization

As soon as the module is provisioned into "FIPS mode", it performs power-up self-tests and enters into FIPS-Approved mode of operation. The following features/services/algorithms are disabled by default and shall not be enabled or used:

- SNMP v1
- SNMP v2c
- Challenge – Response Authentication
- DES
- MD5
- Blowfish

It is the CO's responsibility to ensure that the module boots correctly. The CO shall ensure that the module is running in FIPS-Approved mode by verifying the "FIPS mode" status over SMI. The module is shipped with three user accounts (Admin, Operator and Observer) and their default passwords. The users must change the default password as part of the initial configuration. The User with Admin privileges should create a CO user. The CO must change the initial password to a personal password. All user passwords must follow the complex password restrictions as mentioned in section 2.4.3. Any user shall not enable any of the disabled services mentioned previously.

3.2.2 Management

IPsec must be configured to use FIPS-Approved cipher suites. Firmware upgrades are possible only if the digital signature is successfully verified and if the Firmware upgrade self-test has passed. The Database Passphrase, ISA RSA Passphrase and ESA RSA Passphrase shall be at least 8 characters long. For security strength details of passphrases please refer to Table 13. The following features/services are enabled to maintain security during FIPS-Approved mode of operation:

- IPsec for RADIUS server communications and OMEA services
- Telnet sessions are secured via use of DTLS[21]

The CO must periodically ensure that the labels or shelves do not show any signs of tampering. Evidence of tampering can be indicated by any of the following:

- Deformation of the label or "dot" pattern visible
- Label appearing broken or torn
- Missing label (in parts or full) from its expected position
- Warped or bent metal covers
- Scratches in the paint of the module
- Serial number on the labels do not match the log book entries

In case of any evidence indicating that the physical security has been violated, it is up to the CO to ensure that the module is secured in terms of its functionality and re-apply the tamper evident labels, following the

[21] DTLS – Datagram Transport Layer Security

procedure as described in section 3.1. If required, the CO should perform a reboot or follow the Zeroization process as described in section 3.2.3.

3.2.3 Zeroization

There are many critical security parameters within the module's cryptographic boundary, including public and private keys, session keys, and authentication credentials. The module's CSPs reside in multiple storage media; SP RAM and Flash, OCM Flash, and QOTR/E RAM and Flash. Ephemeral keys that reside in RAM will be zeroized when the module reboots or when a secure session is terminated. Keys that are stored in RAM or Flash are subject to the zeroization methods described in Table 15 of this Security Policy.

In order to zeroize the entire module (all keys stored in SP RAM and Flash, OCM Flash, and QOTR/E RAM and Flash), the User with Admin privileges and CO, together, will have to perform following consecutive and supervised steps:

1. User with Admin privileges will log in and zeroize the keys they are capable of zeroizing according to the zeroization methods described in Table 15.
2. The CO will then log in and zeroize all remaining keys according to the zeroization methods described in Table 15.

During both steps the module shall be under the direct control of both the User with Admin privileges and CO. After each zeroization step is complete, the SMI console will show a notification stating that zeroization has taken place.

3.3 User Guidance

A User must be diligent to follow complex password restrictions and must not reveal their password to anyone. Additionally, the User should be careful to protect FIPS log book, tamper evident labels and any secret or private keys in their possession.

.

4 Acronyms

This section describes the acronyms.

Table 19 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APBE	Automatic Per-Band Equalizer
C&L	Coupler & Splitter Tray
CA	Certificate Authority
CBC	Cipher Block Chaining
CD	Compact Disc
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRC	Cyclic Redundancy Check
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DCE	Data Circuit-Terminating Equipment
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DTE	Data Terminal Equipment
DTLS	Datagram Transport Layer Security
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESA	External Security Authentication
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
Gbps	Gigabits per second
GFSRM	Gigabit Ethernet/Fibre Channel SubRate Multiplexer
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
IKE	Internet Key Exchange

.

Acronym	Definition
IP	Internet Protocol
ISA	Inter-shelf Security Authentication
KAT	Known Answer Test
LED	Light Emitting Diode
MOTR	Multiplexer Optical Transponder
NIST	National Institute of Standards and Technology
nm	Nanometer
NVLAP	National Voluntary Laboratory Accreditation Program
OC	Optical Carrier
OCI	Optical Channel Interface
OCLD	Optical Channel Laser/Detector
OCM	Optical Channel Manager
OFA	Optical Fiber Amplifier
OMEA	Optical Manager Element Adapter
OMX	Optical Multiplexer
OMXI	Optical Multiplexer Interface
OS	Operating System
OSC	Optical Service Channel
OTR	Optical Transponder
PM	Performance Monitoring
QOTR	Quad Optical Transponder
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SFP	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SMI	System Manager Interface
SNMP	Simple Network Management Protocol
SRM	Subrate Multiplexer
Triple-DES	Triple Data Encryption Standard
TLI	Transaction Language I
TLS	Transport Layer Security
WDM	Wavelength Division Multiplexing

.

Acronym	Definition
XFP	10 Gigabit Small Form-Factor Pluggable

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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