



## Net Tool Optimizer (NTO) 7303

Hardware Version: NTO 7303 Chassis P/N 991-0082-01, NTO 7300 Series Supervisor Module P/N 992-0059-01 (QTY: 2), NTO 7300 Series Line Card with 16 QSFP+ ports P/N 992-0045-01, NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with NTO 7300 Series Advanced Feature Module Cassette with 16 SFP+ ports P/N 992-0067-01 (QTY: 2), NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with NTO 7300 Series 100G Port Interface Cassette P/N 992-0066-01 (QTY: 2), NTO 7300 Series Smart Blank Line Card P/N 992-0043-01, NTO 7300 Series PCM Line Card with 48 SFP+ ports P/N 992-0051-01, NTO 7300 Series ATIP Line Card with 48 SFP+ ports P/N 992-0050-01, NTO 7300 Series Fan Module Unit P/N 991-2013-01 (QTY: 6)

Firmware Version: 4.5.0.16

# FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1  
Document Version: 2.2

Prepared for:



**Ixia**  
26601 W. Agoura Road  
  
Calabasas, CA 91302  
United States of America

Phone: +1 818 871 1800  
[www.ixiacom.com](http://www.ixiacom.com)

Prepared by:



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

Phone: +1 703 267 6050  
[www.corsec.com](http://www.corsec.com)

# Table of Contents

---

- 1. Introduction .....4
  - 1.1 Purpose .....4
  - 1.2 References.....4
  - 1.3 Document Organization .....4
- 2. NTO 7303 .....5
  - 2.1 Overview .....5
  - 2.2 Module Specification ..... 11
  - 2.3 Module Interfaces ..... 13
  - 2.4 Roles, Services, and Authentication..... 15
    - 2.4.1 Crypto Officer Role ..... 16
    - 2.4.2 User Role..... 18
    - 2.4.3 SNMP User ..... 20
    - 2.4.4 Additional Services ..... 20
    - 2.4.5 Authentication ..... 21
  - 2.5 Physical Security..... 21
  - 2.6 Operational Environment ..... 21
  - 2.7 Cryptographic Key Management ..... 22
  - 2.8 EMI / EMC ..... 27
  - 2.9 Self-Tests ..... 27
    - 2.9.1 Power-Up Self-Tests..... 27
    - 2.9.2 Conditional Self-Tests ..... 28
  - 2.10 Mitigation of Other Attacks ..... 28
- 3. Secure Operation ..... 29
  - 3.1 Management..... 29
  - 3.2 Monitoring Status ..... 29
  - 3.3 Zeroization ..... 29
  - 3.4 CO and User Guidance ..... 29
    - 3.4.1 Initial Setup..... 30
    - 3.4.2 Configure the FIPS-Approved Mode..... 30
    - 3.4.3 Determining the FIPS-Approved Mode ..... 34
    - 3.4.4 Non-Approved Services ..... 35
- 4. Acronyms ..... 37

## List of Tables

---

- Table 1 – Security Level per FIPS 140-2 Section ..... 11
- Table 2 – FIPS-Approved Algorithm Implementations ..... 11
- Table 3 – NTO 7303 FIPS 140-2 Logical Interface Mappings ..... 15
- Table 4 – Crypto Officer Services..... 16
- Table 5 – User Services ..... 18

Table 6 – SNMP User Services ..... 20  
 Table 7 – Additional Services..... 20  
 Table 8 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs ..... 22  
 Table 9 – Non-Approved Services ..... 35  
 Table 10 – Non-Approved Algorithm Implementations ..... 36  
 Table 11 – Acronyms ..... 37

## List of Figures

---

Figure 1 – NTO 7303 Chassis P/N 991-0082-01 (Front view; fully populated).....6  
 Figure 2 – NTO 7303 Chassis P/N 991-0082-01 (Rear view; fully populated) .....7  
 Figure 3 – NTO Supervisor Module P/N 992-0059-01 (with fan modules removed) .....7  
 Figure 4 – NTO 7300 Series Line Card with 16 QSFP+ ports P/N 992-0045-01 .....8  
 Figure 5 – NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 (with interface cassettes removed) .....8  
 Figure 6 – NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with 2x NTO 7300 Series Advanced Feature Module Cassette with 16 SFP+ ports P/N 992-0067-01 .....8  
 Figure 7 – NTO 7300 Series Advanced Feature Module Cassette with 16 SFP+ ports P/N 992-0067-01 .....8  
 Figure 8 – NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with 2x NTO 7300 Series 100G Port Interface Cassette P/N 992-0066-01 .....8  
 Figure 9 – NTO 7300 Series 100G Port Interface Cassette P/N 992-0066-01 .....9  
 Figure 10 – NTO 7300 Series Smart Blank Line Card P/N 992-0043-01.....9  
 Figure 11 – NTO 7300 Series PCM Line Card with 48 SFP+ ports P/N 992-0051-01 .....9  
 Figure 12 – NTO 7300 Series ATIP Line Card with 48 SFP+ ports P/N 992-0050-01.....9  
 Figure 13 – NTO 7300 Series Fan Module Unit P/N 991-2013-01..... 10  
 Figure 14 – NTO 7303 Front Ports and Interfaces ..... 13  
 Figure 15 – NTO 7303 Rear Ports and Interfaces ..... 14  
 Figure 16 – Management Ethernet Ports and LEDs ..... 14

# 1. Introduction

---

## 1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Net Tool Optimizer (NTO) 7303 from Ixia. This Security Policy describes how the NTO 7303 meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.<sup>1</sup> and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at <http://csrc.nist.gov/groups/STM/cmvp>.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Net Tool Optimizer (NTO) 7303 is referred to in this document as NTO 7303, crypto module, or the module.

## 1.2 References

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

- The Ixia website ([www.ixiacom.com](http://www.ixiacom.com)) contains information on the full line of products from Ixia.
- The CMVP website (<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>) contains contact information for individuals responsible for answering technical or sales-related questions for the module.

## 1.3 Document Organization

The Security Policy document is one document that is part of the FIPS 140-2 submission documentation. In addition to this document, the submission documentation includes:

- Vendor Evidence
- Finite State Model
- Submission Summary
- Other supporting documentation as additional references

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

---

<sup>1</sup> US – United States

Ixia Net Tool Optimizer (NTO) 7303

## 2. NTO 7303

---

### 2.1 Overview

Designed to sit between a customer's network and security tools, the NTO 7303 is a solution that controls the flow of network traffic to destination security devices and applications. The module uses a pool of high-speed data interfaces that are intended to forward different classes of traffic based on filters applied to each interface. These filters allow the module to aggregate, filter, replicate, optimize, and perform load balancing on network data. These features help eliminate SPAN<sup>2</sup> and TAP<sup>3</sup> shortages, increase network visibility, and improve the overall performance of security tools.

Ixia allows customers to designate physical ports as network ports, which allow ingress of network data to the NTO 7303 system, and tool ports, which allow egress of network data to security devices and applications for processing. Dynamic filters, which provide rules for traffic entering or exiting the NTO 7303 system, can be applied to either network ports or tool ports.

The NTO 7303 is a 7U NEBS<sup>4</sup> level 3 certified system. The validated NTO 7303 configuration contains the following:

- NTO 7303 Chassis P/N 991-0082-01 – see Figure 1 and Figure 2
- 2x NTO 7300 Series Supervisor Module P/N 992-0059-01 running NVOS<sup>5</sup> v4.5.0.16. The supervisor modules control the line cards, expose the management interfaces, and control load balancing. Each supervisor assembly contains an Intel Core i7 3555LE processor. See Figure 3
- Six line cards, which provide the front panel ports for network connectivity. The line cards, which are listed below, contain an Intel Atom N2600 processor, except for the ATIP line card, which contains an Intel i7 3555LE processor.
  - NTO 7300 Series Line Card with 16 QSFP+ ports P/N 992-0045-01 – see Figure 4
  - NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with 2x NTO 7300 Series Advanced Feature Module Cassette with 16 SFP+ ports P/N 992-0067-01 – see Figure 5, Figure 6, and Figure 7
  - NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with 2x NTO 7300 Series 100G Port Interface Cassette P/N 992-0066-01 – see Figure 5, Figure 8, and Figure 9
  - NTO 7300 Series Smart Blank Line Card P/N 992-0043-01 – see Figure 10
  - NTO 7300 Series PCM<sup>6</sup> Line Card with 48 SFP+ ports P/N 992-0051-01 – see Figure 11
  - NTO 7300 Series ATIP<sup>7</sup> Line Card with 48 SFP+ ports P/N 992-0050-01 – see Figure 12
- 6x NTO 7300 Series Fan Module Unit P/N 991-2013-01 – see Figure 13

Each line card interfaces with the supervisor modules via an 8x40G Ethernet interface. The links from the line cards to the supervisor are configured into a logical 640G trunk interface.

---

<sup>2</sup> SPAN – Switched Port Analyzer

<sup>3</sup> TAP – Test Access Point

<sup>4</sup> NEBS – Network Equipment Building System

<sup>5</sup> NVOS – Network Visibility Operating System

<sup>6</sup> PCM – Packet Capture Module

<sup>7</sup> ATIP – Application Threat Intelligence Processor

Ixia Net Tool Optimizer (NTO) 7303



Figure 1 – NTO 7303 Chassis P/N 991-0082-01 (Front view; fully populated)

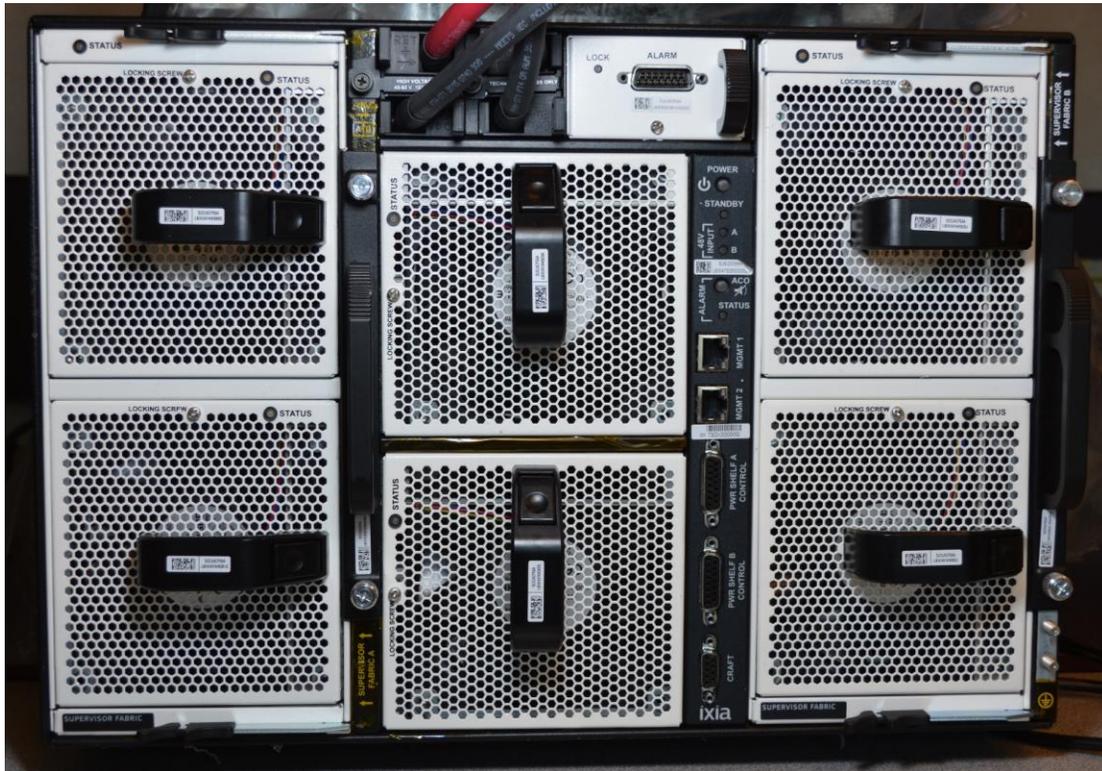


Figure 2 – NTO 7303 Chassis P/N 991-0082-01 (Rear view; fully populated)



Figure 3 – NTO Supervisor Module P/N 992-0059-01 (with fan modules removed)



Figure 4 – NTO 7300 Series Line Card with 16 QSFP+ ports P/N 992-0045-01

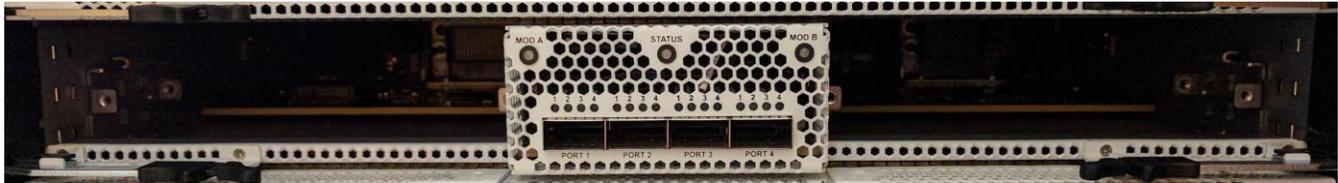


Figure 5 – NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 (with interface cassettes removed)



Figure 6 – NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with 2x NTO 7300 Series Advanced Feature Module Cassette with 16 SFP+ ports P/N 992-0067-01

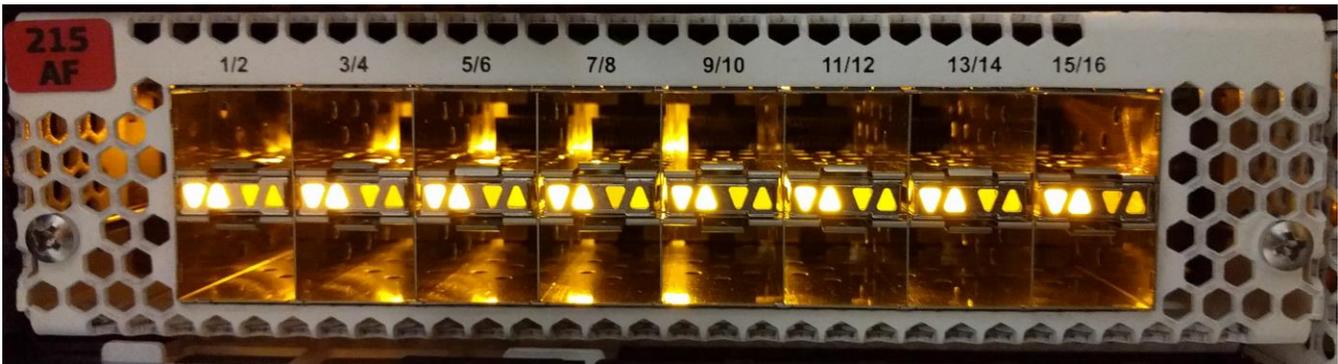


Figure 7 – NTO 7300 Series Advanced Feature Module Cassette with 16 SFP+ ports P/N 992-0067-01

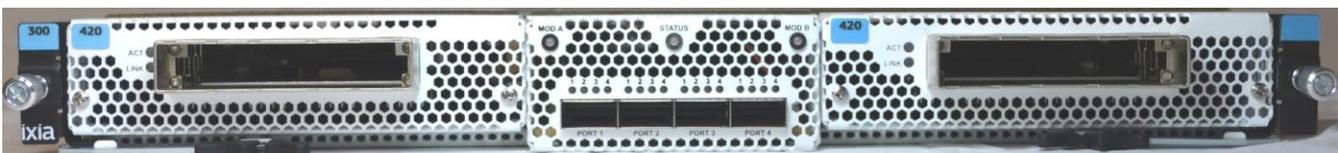


Figure 8 – NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with 2x NTO 7300 Series 100G Port Interface Cassette P/N 992-0066-01



Figure 9 – NTO 7300 Series 100G Port Interface Cassette P/N 992-0066-01

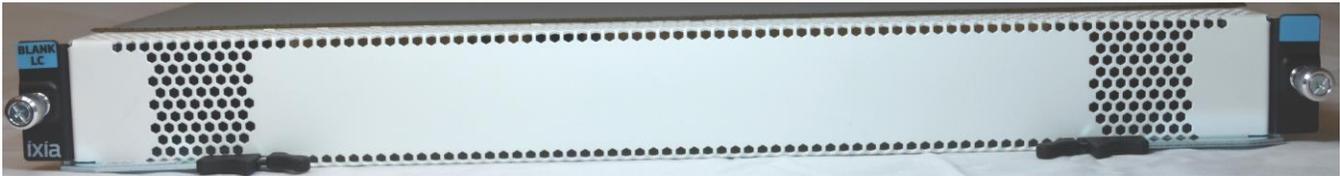


Figure 10 – NTO 7300 Series Smart Blank Line Card P/N 992-0043-01

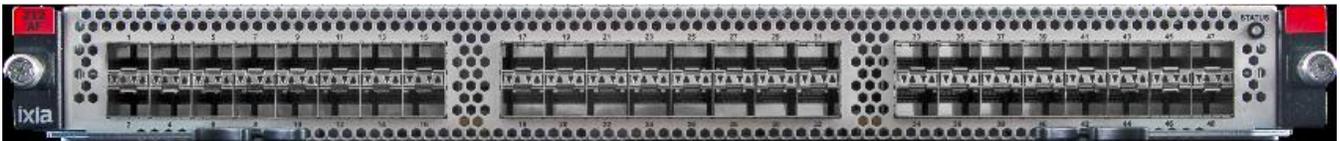


Figure 11 – NTO 7300 Series PCM Line Card with 48 SFP+ ports P/N 992-0051-01

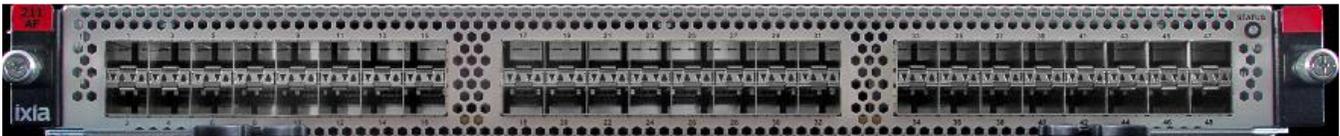


Figure 12 – NTO 7300 Series ATIP Line Card with 48 SFP+ ports P/N 992-0050-01



Figure 13 – NTO 7300 Series Fan Module Unit P/N 991-2013-01

The NTO 7303 provides an orthogonal (the backplane has no cable length to reduce delay) switching architecture. Network traffic flows from the network port, passes through any applied filters, and is sent to its destination via a tool port. Packets transition from one line card to another through the supervisor modules that comprise the backplane. The supervisor modules also apply load balancing to network traffic.

The firmware is based on Linux Kernel version 3.5. The firmware provides access to two primary management interfaces, both of which provide the same functionality. Connections to these interfaces are protected using TLSv1.2<sup>8</sup>. These include:

- Java Console – This interface provides a Java-based client that can be downloaded to a management workstation and used to manage the system.
- Web Console – This interface provides a web-based client that can be loaded in a web browser and used to manage the system.

In addition, the module provides a Web API<sup>9</sup> which can provide programmatic access to management services, as well as read-only SNMPv3 support which enables system settings to be viewed as well as for management traps to be sent to an SNMP manager. The Web API is protected via TLSv1.2 and the SNMPv3 interface is protected with AES and HMAC.

The module also provides remote syslog capabilities. Syslog traffic is protected with TLSv1.2.

Services offered via these interfaces are listed below in Table 4 and Table 5.

The NTO 7303 is validated at the FIPS 140-2 Section levels shown in Table 1:

---

<sup>8</sup> TLS – Transport Layer Security

<sup>9</sup> API – Application Programming Interface

Ixia Net Tool Optimizer (NTO) 7303

**Table 1 – Security Level per FIPS 140-2 Section**

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

## 2.2 Module Specification

The NTO 7303 is a Hardware module with a multiple-chip standalone embodiment. The module has been validated against Level 1 requirements. The cryptographic boundary of the NTO 7303 is defined by the hard metal casing making up the NTO 7303 chassis.

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

**Table 2 – FIPS-Approved Algorithm Implementations**

| Algorithm  | Certificate Number |
|--|--------------------|
| AES ECB <sup>11</sup> encryption/decryption with 128-, 192-, and 256-bit keys                | 4089               |
| AES CBC <sup>12</sup> encryption/decryption with 128- and 256-bit keys                       | 4089               |
| AES CFB128 <sup>13</sup> encryption/decryption with 128-, 192-, and 256-bit keys             | 4089               |
| AES CCM <sup>14</sup> encryption/decryption with 256 bit key                                 | 4089 <sup>15</sup> |
| RSA Key Pair Generation, Signature Generation, and Signature Verification with 2048-bit keys | 2213               |
| SHA <sup>16</sup> -1, SHA-256, SHA-512   | 3365               |
| HMAC <sup>17</sup> with SHA-1, SHA-256, SHA-512  | 2669               |

<sup>10</sup> EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

<sup>11</sup> ECB – Electronic Codebook

<sup>12</sup> CBC – Cipher Block Chaining

<sup>13</sup> CFB – Cipher Feedback

<sup>14</sup> CCM – Counter with CBC-MAC

<sup>15</sup> Please note that key sizes 128 and 192 listed on certificate #4089 are not accessible.

<sup>16</sup> SHA – Secure Hash Algorithm

<sup>17</sup> HMAC – (keyed-) Hashed Message Authentication Code

| Algorithm  | Certificate Number |
|--|--------------------|
| SP <sup>18</sup> 800-90A Hash DRBG <sup>19</sup>             | 1227               |
| Section 4.2 TLS v1.2 KDF (SP 800-135) CVL <sup>20</sup>      | 904                |
| Section 5.4 SNMPv3 KDF (SP 800-135) CVL                      | 904                |
| PBKDF <sup>21</sup> (SP 800-132 Option 1a with HMAC-SHA-512) | Vendor Affirmed    |
| CKG <sup>22</sup> (SP 800-133)                               | Vendor Affirmed    |

The cryptographic module implements Key Derivation Functions (KDFs) listed in NIST SP 800-135 as part of the TLS secure networking protocol and SNMP protocol. No parts of these protocols, other than the KDF, have been tested by the CAVP.

The password for the SP 800-132 is 12 bytes in length concatenated with a 16 byte string. The upper bound for the probability of having guessed the password at random is  $1/(26*26*10*32)^{12}$ . The salt is 64 bytes in length and the iteration count is 1024. The output size is 256 bits. Keys derived using PBKDF may only be used in storage applications.

The module implements the following non-Approved security functions. These algorithms and protocols are allowed for use in a FIPS-Approved mode of operation:

- RSA (key transport; key establishment methodology provides 112 bits of encryption strength)
- A Non-Deterministic Random Number Generator (NDRNG) is used to seed the approved SP 800-90A Hash DRBG. This seeding source provides a minimum number of bits of entropy of 7.9 out of 8 bits.

---

<sup>18</sup> SP – Special Publication

<sup>19</sup> DRBG – Deterministic Random Bit Generator

<sup>20</sup> CVL – Component Validation List

<sup>21</sup> PBKDF – Password Based Key Derivation Function

<sup>22</sup> CKG – Cryptographic Key Generation

---

Ixia Net Tool Optimizer (NTO) 7303

## 2.3 Module Interfaces

The NTO 7303 cryptographic module physical ports can be categorized according to the following logical interfaces defined by FIPS 140-2:

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

Figure 14, Figure 15, and Figure 16 show the physical ports and interfaces of the NTO 7303:

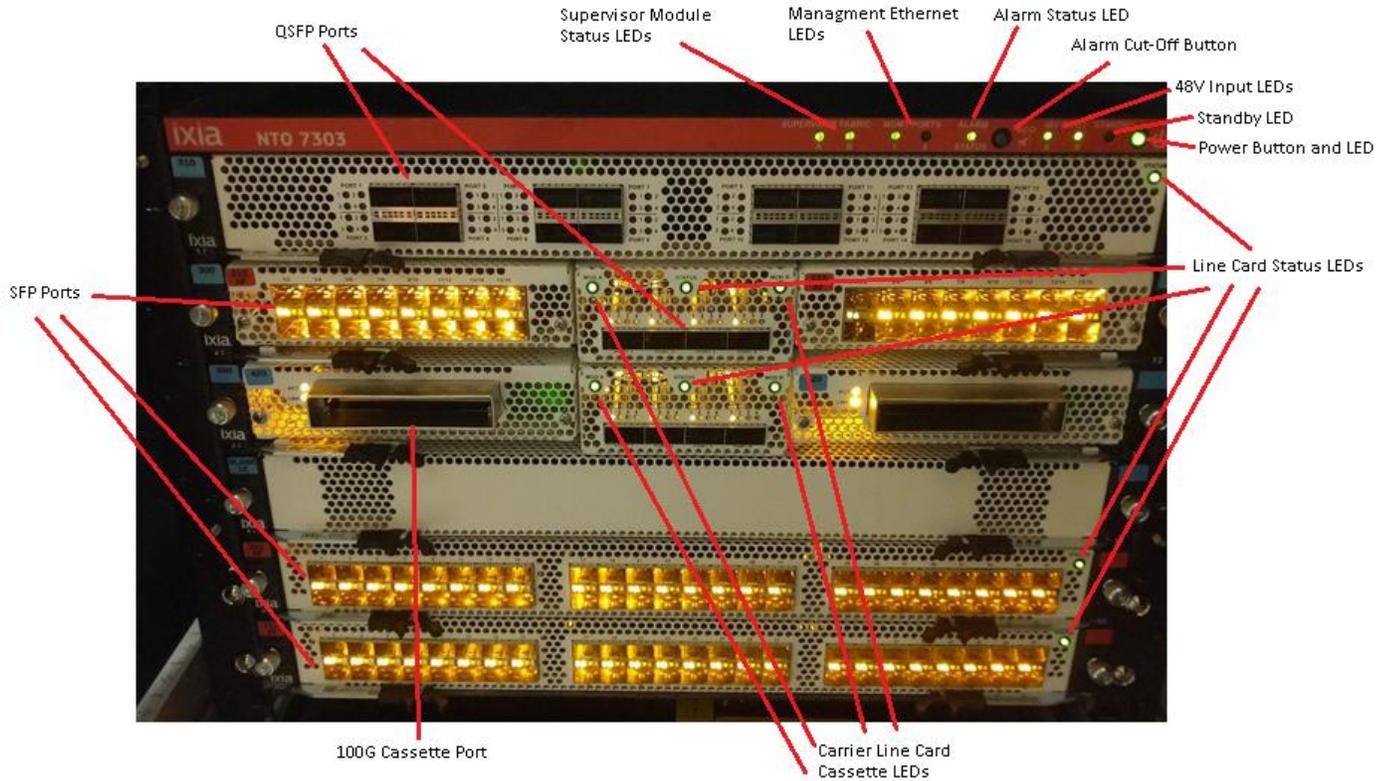


Figure 14 – NTO 7303 Front Ports and Interfaces

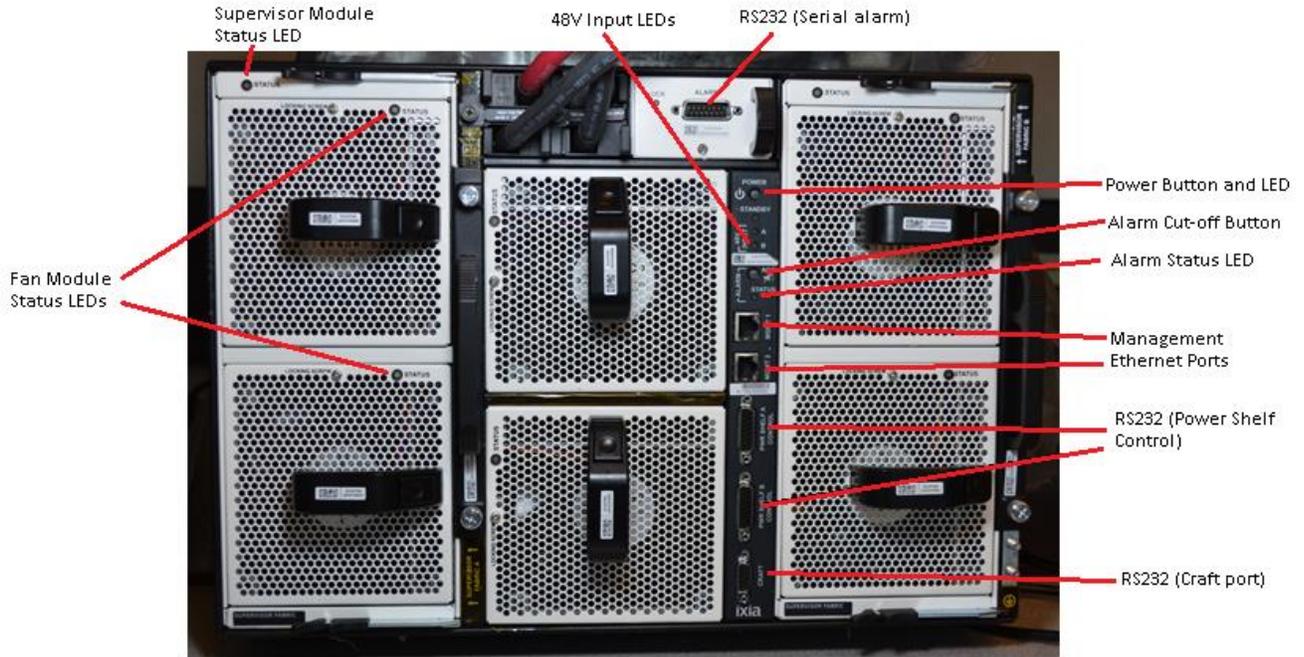


Figure 15 – NTO 7303 Rear Ports and Interfaces

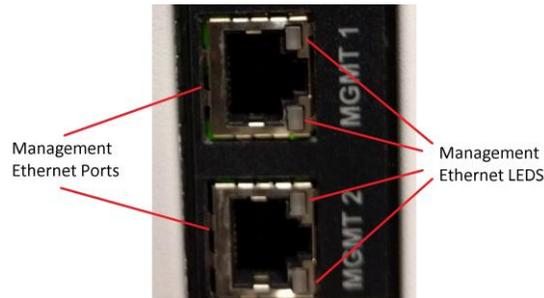


Figure 16 – Management Ethernet Ports and LEDs

Physical interfaces for the NTO 7303 are described in Table 3:

**Table 3 – NTO 7303 FIPS 140-2 Logical Interface Mappings**

| Physical Port                      | Quantity/Location                              | FIPS 140-2 Interface  |
|------------------------------------|--|---|
| Management Ethernet Ports          | 2, rear  | <ul style="list-style-type: none"> <li>Control Input</li> <li>Status Output</li> <li>Data Input</li> <li>Data Output</li> </ul> |
| Management Ethernet LEDs           | 2 LEDs per port, rear<br>1 LED per port, front | <ul style="list-style-type: none"> <li>Status Output</li> </ul>   |
| RS-232 Port (Serial alarm)         | 1, rear  | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| Alarm Cut-Off button               | 1, front<br>1, rear                            | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| Alarm Status LED                   | 1, front<br>1, rear                            | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| RS-232 Ports (Power shelf control) | 2, rear  | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| RS-232 Port (Serial Craft port)    | 1, rear  | <ul style="list-style-type: none"> <li>N/A (Disabled in FIPS-Approved mode)</li> </ul>  |
| SFP+ Ports                         | 128, front                                     | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| QSFP+ Ports                        | 24, front                                      | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| 100G Cassette Ports                | 2, front                                       | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| Supervisor Module Status LEDs      | 2, front<br>2, rear                            | <ul style="list-style-type: none"> <li>Status Output</li> </ul>   |
| Power Button and LED               | 1, front<br>1, rear                            | <ul style="list-style-type: none"> <li>Control Input</li> <li>Status Output</li> </ul>  |
| Standby LED                        | 1, front                                       | <ul style="list-style-type: none"> <li>Status Ouptut</li> </ul>   |
| 48V Input LEDs                     | 2, front<br>2, rear                            | <ul style="list-style-type: none"> <li>Status Output</li> </ul>   |
| Fan Module Status LEDs             | 6, rear  | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| Line Card Status LEDs              | 3, front                                       | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |
| Carrier Line Card Status LEDs      | 4, front                                       | <ul style="list-style-type: none"> <li>N/A</li> </ul>   |

## 2.4 Roles, Services, and Authentication

There are three roles that operators may assume: a Crypto Officer (CO), User, and SNMP User. The Crypto Officer (which corresponds to the module’s “System Administrator” account) is responsible for installing, configuring, and monitoring the module. Users (which correspond to any account that is not a “System Administrator”) are responsible for monitoring the module, configuring ports and filters, and managing group membership. The CO and User roles access the module remotely over a secure session provided by TLSv1.2. SNMP Users access read-only configuration information, which is protected with AES and HMAC.

The module supports multiple concurrent operators. No restrictions are set on the number of operators that may access the module at once. Access to module functionality is determined by the role of the account the operator is using to access the module.

The module implements role-based authentication. Crypto Officer and User accounts each have a unique username and password assigned to them. Role selection is accomplished explicitly by successfully authenticating to the Crypto Officer or User role using valid credentials that are associated with the desired role’s account. SNMP User accounts have a privacy password in addition to an authentication password. Role selection is accomplished by successfully authenticating with the privacy and authentication password associated with the SNMP user.

Keys and CSPs listed in the tables indicate the type of access required according to 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.
- None – No access is provided to the CSP or no CSP is applicable.

## 2.4.1 Crypto Officer Role

The Crypto Officer role has the ability to install, configure, and monitor all parts of the module. Descriptions of the services available to the Crypto Officer role are provided in Table 4 below.

**Table 4 – Crypto Officer Services**

| Service                                | Description  | CSP and Type of Access                           |
|--|--|--|
| Authenticate to the module             | Supply authentication credentials to access the control interface  | Crypto Officer Password – RX                     |
| Configure system and statistics        | View system information and configurations that affect the whole system, and view or reset statistics          | None   |
| View system status                     | View the operational status of the system.   | None   |
| Configure ports                        | Configure port settings for network port filtering, dynamic filtering, load balancing, and tool port filtering | None   |
| Configure filters and filter templates | Configure individual filters and filter templates  | None   |
| Configure monitors                     | Configure monitors to generate SNMP traps or syslog messages when specified events occur                       | None   |
| Configure load-balancing               | Configure load-balancing for the system.   | None   |
| Configure resources                    | Configure resources for packet capture.  | None   |
| Manage groups                          | Configure and manage groups and group owners   | None   |
| Manage users                           | Create, edit, and delete operator accounts and modify permissions  | Crypto Officer Password – W<br>User Password – W |

| Service                                  | Description   | CSP and Type of Access  |
|--|---|---|
| Change password                          | Change the password for the Crypto Officer account or any other operator account  | Crypto Officer Password – W   |
| Manage logs                              | Configure and manage local and remote logs and logging capabilities   | None  |
| Power down                               | Shut down the module and zeroize all session keys in volatile memory  | All CSPs stored in RAM <sup>23</sup> – W  |
| Restart                                  | Reboot the module, zeroize all session keys in volatile memory, and execute power-on self-tests on demand                 | All CSPs stored in RAM – W  |
| Upgrade firmware                         | Apply a new firmware update to the module   | Firmware load test key – RX   |
| Factory reset                            | Restore module to factory defaults  | All CSPs stored in Flash – W  |
| Establish management TLS session         | Use the Java Console or Web Console to establish a management session using TLS and perform any of the available services | Web RSA public key – RX<br>Web RSA private key – RX<br>TLS server session key – WX<br>TLS server HMAC key – WX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX |
| Decrypt management data                  | Decrypt incoming data sent to the management interfaces   | TLS server session key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX  |
| Encrypt management data                  | Encrypt outgoing data sent from the management interfaces   | TLS server session key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX  |
| Produce SHA digest                       | Create a digest using the SHA-1 and SHA-256 algorithms for use with TLS   | None  |
| Produce HMAC digest                      | Create a keyed hash using the HMAC-SHA-1 and HMAC-SHA-256 algorithms for use with TLS                                     | TLS server HMAC key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX   |
| Generate web RSA key pair                | Generate RSA key pair for use with web TLS sessions   | Key store HMAC key – WX<br>Key store AES key – WX<br>Web RSA public key – W<br>Web RSA private key – W<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX         |
| Generate web certificate signing request | Generate certificate signing request for use with web TLS sessions  | Key store HMAC key – RX<br>Key store AES key – RX<br>Web RSA private key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX                                  |
| Import web TLS certificate               | Import a certificate file to replace the web TLS certificate currently in use by the module                               | Key store HMAC key – RX<br>Key store AES key – RX<br>Web RSA public key – W   |

<sup>23</sup> RAM – Random Access Memory  
Ixia Net Tool Optimizer (NTO) 7303

| Service                                     | Description  | CSP and Type of Access  |
|---|--|---|
| Configure syslog parameters                 | Configure settings that affect the syslog functionality  | None  |
| Generate syslog RSA key pair                | Generate RSA key pair for use with web TLS sessions  | Key store HMAC key – WX<br>Key store AES key – WX<br>Syslog RSA public key – W<br>Syslog RSA private key – W<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX           |
| Generate syslog certificate signing request | Generate certificate signing request for signing with a third-party certificate authority      | Key store HMAC key – RX<br>Key store AES key – RX<br>Syslog RSA private key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX                                       |
| Import syslog TLS certificate               | Import a certificate file to replace the syslog TLS certificate currently in use by the module | Key store HMAC key – RX<br>Key store AES key – RX<br>Syslog RSA public key – W  |
| Establish syslog TLS session                | Establish a TLS session with the syslog server   | Syslog RSA public key – RX<br>Syslog RSA private key – RX<br>TLS client session key – RWX<br>TLS client HMAC key – RWX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX |
| Configure SNMP parameters                   | Configure settings that affect the SNMP functionality  | None  |
| Configure SNMPv3 encryption                 | Update the encryption keys used for SNMPv3 connections   | SNMPv3 privacy password – W<br>SNMPv3 authentication password – W   |
| Export log file                             | Export a copy of the logs in encrypted format  | Log encryption key – RWX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX   |

## 2.4.2 User Role

The User role has the ability to monitor the module and manage ports and filters. Users can also manage group membership. Descriptions of the services available to the User role are provided in Table 5 below.

**Table 5 – User Services**

| Service                    | Description  | CSP and Type of Access |
|----------------------------|--|------------------------|
| Authenticate to the module | Supply authentication credentials to access the control interface  | User Password – RX     |
| View system and statistics | View system information and statistics   | None                   |
| View system status         | View that operational status of the system.  | None                   |
| Configure ports            | Configure port settings for network port filtering, dynamic filtering, load balancing, and tool port filtering | None                   |

| Service                                | Description   | CSP and Type of Access  |
|--|---|---|
| Configure filters and filter templates | Configure individual filters and filter templates                                     | None  |
| View monitors                          | View monitors that generate SNMP traps or syslog messages when specified events occur | None  |
| Manage groups                          | Configure and manage groups   | None  |
| Change password                        | Change the current operator's account password  | User Password – W   |
| Establish management TLS session       | Establish management session using TLS and perform any of the available services      | Web RSA public key – RX<br>Web RSA private key – RX<br>TLS server session key – WX<br>TLS server HMAC key – WX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX |
| Decrypt management data                | Decrypt incoming data sent to the management interfaces                               | TLS server session key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX  |
| Encrypt management data                | Encrypt outgoing data sent from the management interfaces                             | TLS server session key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX  |
| Produce SHA digest                     | Create a digest using the SHA-1 and SHA-256 algorithms for use with TLS               | None  |
| Produce HMAC digest                    | Create a keyed hash using the HMAC-SHA-1 and HMAC-SHA-256 algorithms for use with TLS | TLS server HMAC key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX   |

### 2.4.3 SNMP User

The SNMP User role has the ability to monitor the module and manage SNMP traps for ports and filters. Descriptions of the services available to the SNMP User role are provided in Table 6 below.

**Table 6 – SNMP User Services**

| Service                  | Description  | CSP and Type of Access  |
|--------------------------|--|---|
| Read network settings    | Read the network settings for the given interface  | None  |
| Read statistics          | Read statistics for the given type   | None  |
| Read history             | Read the historical data of the given type   | None  |
| Read filters             | Read the filters defined for the module  | None  |
| Establish SNMPv3 session | Establish an SNMPv3 session to view system settings  | SNMPv3 authentication password – RX<br>SNMPv3 privacy password – RX<br>SNMPv3 encryption key – WX<br>SNMPv3 HMAC key – WX |
| Produce HMAC digest      | Create a keyed hash using the HMAC-SHA-1 and HMAC-SHA-256 algorithms for use with TLS and SNMP | SNMPv3 HMAC key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX                           |
| Decrypt SNMP data        | Decrypt incoming data sent to the SNMP interface   | SNMPv3 encryption key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX                     |
| Encrypt SNMP data        | Encrypt outgoing data sent from the SNMP interface   | SNMPv3 encryption key – RX<br>SP 800-90A DRBG Output – RX<br>SP 800-90A Hash DRBG values V and C – RX                     |

### 2.4.4 Additional Services

The module provides a limited number of services for which the operator is not required to assume an authorized role. Table 7 lists the services for which the operator is not required to assume an authorized role. None of the services listed in the table modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the module.

**Table 7 – Additional Services**

| Service                          | Description  | CSP and Type of Access |
|----------------------------------|--|------------------------|
| Perform on-demand self-tests     | Perform power-on self-tests on demand                              | None                   |
| View firmware version            | Show the module’s current firmware version, including build number | None                   |
| Download Java Console            | Download a copy of the Java Console file to the local workstation  | None                   |
| Receive/transmit network traffic | Send network data through the module                               | None                   |

## 2.4.5 Authentication

The module implements explicit role-based authentication. The CO and Users each have a unique username and password assigned to their accounts. When logging in, the operator will pass the username and password of the account to the module via a TLS tunnel protected with AES encryption. In the case of SNMP, operators must supply an authentication and privacy password. Operators assume the roles associated with the credentials that were submitted during the authentication process and the interface accessed. In order for an operator to change roles, they must log out of any active sessions and re-authenticate. The results of previous authentications are cleared when the module is powered off.

Passwords that are generated after the module has been configured to operate in the FIPS-Approved mode of operation are 15 characters minimum and must include at least one upper- and lower-case letter, number, and special character. The probability for guessing a 15 character password in the worst case is 1 in 1,230,428,359,612,438,187,500,000,000. The probability of guessing the password within one minute is 1:2,460,856,719,224,876,375.

SNMPv3 privacy and authentication passwords set by the CO should adhere to the complexity requirements for CO and User roles. In this case, the probability is far lower given both the privacy and authentication passwords must both be guessed in order to successfully establish a SNMPv3 session.

## 2.5 Physical Security

The Ixia NTO 7303 is a hardware module with a multi-chip standalone embodiment that consists of production-grade materials that use standard passivation techniques. The NTO 7303 chassis is a hard metal enclosure that is physically contiguous.

## 2.6 Operational Environment

The module's operational environment is non-modifiable and is comprised of the NVOS<sup>24</sup> v4.5.0.16 firmware running on the NTO 7303 appliance.

---

<sup>24</sup> NVOS – Network Visibility Operating System  
Ixia Net Tool Optimizer (NTO) 7303

## 2.7 Cryptographic Key Management

The module supports the CSPs listed in Table 8 below.

**Table 8 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs**

| CSP                    | CSP Type                 | Generation / Input   | Output  | Storage   | Zeroization   | Use  |
|------------------------|--------------------------|--|---|---|---|--|
| Web RSA public key     | RSA 2048-bit public key  | <ul style="list-style-type: none"> <li>Generated internally using the approved SP 800-90A DRBG; or</li> <li>Imported by CO as part of a certificate file over TLS</li> </ul> | Exported by CO as part of a certificate signing request file over TLS | Stored on non-volatile Flash in AES encrypted key store | <ul style="list-style-type: none"> <li>Zeroized when existing key is replaced with a new key; or</li> <li>Zeroized by “Factory reset” operation.</li> </ul> | Used by the management interfaces for TLS authentication                               |
| Web RSA private key    | RSA 2048-bit private key | Generated internally using the approved SP 800-90A DRBG  | Never exits the module  | Stored on non-volatile Flash in AES encrypted key store | <ul style="list-style-type: none"> <li>Zeroized when existing key is replaced with a new key; or</li> <li>Zeroized by “Factory reset” operation.</li> </ul> | Used by the management interfaces for TLS authentication                               |
| TLS server session key | AES 128- or 256-bit key  | Imported from client using RSA key transport   | Never exits the module  | Stored in RAM in plaintext                              | <ul style="list-style-type: none"> <li>Zeroized by session termination; or</li> <li>Zeroized by power cycling the module</li> </ul>                         | Used for encrypting and decrypting inbound and outbound traffic during the TLS session |

| CSP                    | CSP Type                           | Generation / Input   | Output  | Storage   | Zeroization   | Use  |
|------------------------|------------------------------------|--|---|---|---|--|
| TLS server HMAC key    | HMAC SHA-1 key or HMAC SHA-256 key | Generated internally using the approved SP 800-90A DRBG  | Never exits the module  | Stored in RAM in plaintext                              | <ul style="list-style-type: none"> <li>Zeroized by session termination; or</li> <li>Zeroized by power cycling the module</li> </ul>                         | Used in TLS v1.2 sessions  |
| Syslog RSA public key  | RSA 2048-bit public key            | <ul style="list-style-type: none"> <li>Generated internally using the approved SP 800-90A DRBG; or</li> <li>Imported by CO as part of a certificate file over TLS</li> </ul> | Exported by CO as part of a certificate signing request file over TLS | Stored on non-volatile Flash in AES encrypted key store | <ul style="list-style-type: none"> <li>Zeroized when existing key is replaced with a new key; or</li> <li>Zeroized by "Factory reset" operation.</li> </ul> | Used by the syslog client for TLS authentication   |
| Syslog RSA private key | RSA 2048-bit private key           | Generated internally using the approved SP 800-90A DRBG  | Never exits the module  | Stored on non-volatile Flash in AES encrypted key store | <ul style="list-style-type: none"> <li>Zeroized when existing key is replaced with a new key; or</li> <li>Zeroized by "Factory reset" operation.</li> </ul> | Used by the syslog client for TLS authentication   |
| TLS client session key | AES 128- or 256-bit key            | Generated internally using the approved SP 800-90A DRBG  | Exported to syslog server using RSA key transport                     | Stored in RAM in plaintext                              | <ul style="list-style-type: none"> <li>Zeroized by session termination; or</li> <li>Zeroized by power cycling the module</li> </ul>                         | Used for encrypting and decrypting inbound and outbound traffic during Syslog TLS sessions |

| CSP                     | CSP Type                               | Generation / Input   | Output                 | Storage   | Zeroization   | Use  |
|-------------------------|--|--|------------------------|---|---|--|
| TLS client HMAC key     | HMAC SHA-1 key or HMAC SHA-256 key     | Generated internally using the approved SP 800-90A DRBG      | Never exits the module | Stored in RAM in plaintext                                | <ul style="list-style-type: none"> <li>Zeroized by session termination; or</li> <li>Zeroized by power cycling the module</li> </ul>                                   | Used in TLS v1.2 sessions  |
| SNMPv3 encryption key   | AES 128-, AES 192-, or AES 256-bit key | Generated internally using the approved SP 800-90A DRBG      | Never exits the module | Stored in RAM in plaintext                                | <ul style="list-style-type: none"> <li>Zeroized by session termination; or</li> <li>Zeroized by power cycling the module</li> </ul>                                   | Used for encrypting and decrypting inbound and outbound traffic during SNMPv3 sessions |
| SNMPv3 HMAC key         | HMAC SHA-1 key or HMAC SHA-256 key     | Generated internally using the approved SP 800-90A DRBG      | Never exits the module | Stored in RAM in plaintext                                | <ul style="list-style-type: none"> <li>Zeroized by session termination; or</li> <li>Zeroized by power cycling the module</li> </ul>                                   | Used for SNMPv3 authentication   |
| SNMPv3 password privacy | Passphrase                             | Input manually by the CO via the Java Console or Web Console | Never exits the module | Stored on non-volatile Flash in RSA 2048-encrypted format | <ul style="list-style-type: none"> <li>Zeroized when existing password is replaced with a new password; or</li> <li>Zeroized by "Factory reset" operation.</li> </ul> | Used to authenticate operators   |

| CSP                                 | CSP Type                  | Generation / Input   | Output                 | Storage   | Zeroization   | Use   |
|-------------------------------------|---------------------------|--|------------------------|---|---|---|
| SNMPv3 authentication password      | Passphrase                | Input manually by the CO via the Java Console or Web Console | Never exits the module | Stored on non-volatile Flash in RSA 2048-encrypted format | <ul style="list-style-type: none"> <li>Zeroized when existing password is replaced with a new password; or</li> <li>Zeroized by "Factory reset" operation.</li> </ul>         | Used to authenticate the SNMPv3 endpoint                                |
| Firmware load test key              | RSA 2048-bit public key   | Hard coded into the module                                   | Never exits the module | Stored in the module's firmware image                     | <ul style="list-style-type: none"> <li>Never zeroized</li> </ul>  | Used by the module during firmware updates to verify the firmware image |
| Log encryption key                  | AES 256-bit key           | Generated internally using the approved SP 800-90A DRBG      | Never exits the module | Stored in RAM in plaintext                                | <ul style="list-style-type: none"> <li>Zeroized by session termination; or</li> <li>Zeroized by power cycling the module</li> </ul>   | Used during encryption of log files                                     |
| SP 800-90A Hash DRBG values V and C | Random seed bits          | Generated internally using a hardware RNG                    | Never exits the module | Stored in RAM in plaintext                                | <ul style="list-style-type: none"> <li>Zeroized by reseed function; or</li> <li>Zeroized by unstantiate function; or</li> <li>Zeroized by power cycling the module</li> </ul> | Used for seeding the SP 800-90A DRBG during instantiation or reseed     |
| SP 800-90A DRBG Output              | Output from the Hash-DRBG | Generated using the Hash-DRBG                                | Never exits the module | Stored in RAM in plaintext                                | <ul style="list-style-type: none"> <li>Zeroized by the unstantiate function</li> </ul>  | Used for generating cryptographic keys for approved functions           |

| CSP                     | CSP Type                | Generation / Input                                | Output                 | Storage                                  | Zeroization   | Use   |
|-------------------------|-------------------------|---|------------------------|--|---|---|
| Crypto Officer Password | Authentication password | Entered by the Crypto Officer                     | Never exits the module | Stored on non-volatile Flash using SHA-1 | <ul style="list-style-type: none"> <li>Zeroized by "Factory reset" operation</li> </ul>   | Used to authenticate the Crypto Officer                                   |
| User Password           | Authentication password | Entered by the User                               | Never exits the module | Stored on non-volatile Flash using SHA-1 | <ul style="list-style-type: none"> <li>Zeroized by "Factory reset" operation</li> </ul>   | Used to authenticate the User   |
| Key store HMAC key      | HMAC-SHA-512 key        | Generated internally using PBKDF input parameters | Never exits the module | Stored in RAM in plaintext               | <ul style="list-style-type: none"> <li>Zeroized by power cycling the module; or</li> <li>Zeroized at the completion of the key derivation function</li> </ul> | Used for deriving the key store AES key                                   |
| Key store AES key       | AES-CCM 256-bit key     | Generated internally using PBKDF                  | Never exits the module | Stored in RAM in plaintext               | <ul style="list-style-type: none"> <li>Zeroized by power cycling the module; or</li> <li>Zeroized at the completion of the encryption function</li> </ul>     | Used for encryption for storage of Web and Syslog RSA private/public keys |

## 2.8 EMI / EMC

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

## 2.9 Self-Tests

The module performs power-up self-tests automatically after power is applied and no further intervention is required from the operator. Conditional tests are performed when the conditions require. Data output and cryptographic operations are inhibited until the module has successfully passed all the power-up self-tests. If any of the self-tests fail (with the exception of the firmware load test), an error message indicating the failure is written to the system log, the module enters a critical error state, and the System LED is illuminated red. In this state, cryptographic operations are halted and the module inhibits all data output from the module. The only action that can be taken in this state is to power cycle the module to trigger the execution of the power-up self-tests. The error condition is considered to have been cleared if the module successfully passes all of the subsequent power-up-self-tests. If the module continues to fail subsequent power-up self-tests, the module is considered to be malfunctioning or compromised and the module should be sent to Ixia for repair or replacement.

### 2.9.1 Power-Up Self-Tests

The NTO 7303 performs the following self-tests at power-up:

- Firmware integrity check with an Error Detection Code (CRC<sup>25</sup>-32)
- Known Answer Tests (KATs)
  - AES-ECB encrypt KAT
  - AES-ECB decrypt KAT
  - AES-CCM encrypt KAT
  - AES-CCM decrypt KAT
  - RSA signature generation KAT
  - RSA signature verification KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - SHA-512 KAT
  - HMAC (with SHA-1) KAT
  - HMAC (with SHA-256) KAT
  - HMAC (with SHA-512) KAT
  - Hash DRBG KAT
- SP 800-90A Health Checks:
  - Instantiate
  - Generate
  - Reseed

---

<sup>25</sup> CRC – Cyclic Redundancy Check

Ixia Net Tool Optimizer (NTO) 7303

## 2.9.2 Conditional Self-Tests

The NTO 7303 performs the following conditional self-tests:

- Firmware load test with 2048-bit RSA key
- Pairwise Consistency Test (PCT) for RSA key pair generation
- Continuous test on DRBG
- Continuous test on NDRNG
- SP 800-90A Health Checks:
  - Reseed

## 2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

## 3. Secure Operation

---

The NTO 7303 meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-approved mode of operation.

Except where otherwise stated below, the CO should follow the guidance as described in the *Ixia Net Tool Optimizer (NTO) 7303 Installation Guide, NVOS 4.5, August 2016* and *Ixia Net Tool Optimizer (NTO) 7303 User Guide, NVOS 4.5, August 2016*.

### 3.1 Management

When configured according to the Crypto Officer guidance in this Security Policy, the module only runs in a FIPS-Approved mode of operation. The Crypto Officer shall configure the module via the Web Console or Java Console as prescribed in this Security Policy.

### 3.2 Monitoring Status

The CO shall be responsible for regularly monitoring the module's status to verify that it continues to operate in the FIPS-Approved mode of operation. When configured according to the Crypto Officer's guidance, the module only operates in the FIPS-Approved mode.

A CO logged in via the Web Console or Java Console can view the operational status on the System screen. If a cryptographic error is encountered, the system will display an error message via the web start page, the regular management interface will not be accessible, and the System LED will be illuminated red.

### 3.3 Zeroization

All of the module's stored keys and CSPs are capable of being zeroized. The module stores the keys listed in Table 8 in either the RAM or non-volatile Flash storage. Zeroization of ephemeral keys and CSPs in RAM are zeroized during session termination or power cycling. Zeroization of keys and CSPs stored in Flash can be accomplished by:

1. Logging into the Java Console
2. Clicking on the **File** menu
3. Clicking on the **Factory Reset** command
4. Clicking **OK** to verify that the system should return to default settings

Once invoked, the effect of the Factory Reset command is immediate and does not allow sufficient time to compromise any stored plaintext CSPs. After zeroization, the module will need to be reinitialized to return to an operational state.

### 3.4 CO and User Guidance

The CO shall be in charge of receiving, installing, initializing, and maintaining the NTO 7303 module. COs or Users must not reveal their password to anyone. The CO shall power cycle the module if the module has encountered a

---

Ixia Net Tool Optimizer (NTO) 7303

critical error and becomes non-operational. If power cycling module does not correct the error condition, the module is considered to be compromised or malfunctioned, and should be sent back to Ixia for repair or replacement.

The following sections provide important instructions and guidance to the CO for secure installation and configuration of the NTO 7303.

### 3.4.1 Initial Setup

Upon receiving the NTO 7303 hardware, the CO shall check that the system is not damaged and that all required parts and instructions are included. The CO shall refer to the *Ixia NTO 7300/7303 Installation Guide, NVOS 4.5, August 2016*, for initial setup instructions.

The line cards shall be installed according to the validated configuration in the following order, by slot number:

1. NTO 7300 Series Line Card with 16 QSFP+ ports P/N 992-0045-01
2. NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with 2x NTO 7300 Series Advanced Feature Module Cassette with 16 SFP+ ports P/N 992-0067-01
3. NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with 2x NTO 7300 Series 100G Port Interface Cassette P/N 992-0066-01
4. NTO 7300 Series Smart Blank Line Card P/N 992-0043-01
5. NTO 7300 Series PCM Line Card with 48 SFP+ ports P/N 992-0051-01
6. NTO 7300 Series ATIP Line Card with 48 SFP+ ports P/N 992-0050-01

After the CO has finished setting up the module, the management interfaces can be accessed to continue initializing the module in the FIPS-Approved mode of operation, outlined in the sections below.

For additional information, refer to *Ixia 7300 Series User Guide, NVOS 4.5, August 2016*, chapter entitled “Configure Government Security Settings”.

### 3.4.2 Configure the FIPS-Approved Mode

The NTO 7303 is shipped and initially operates with FIPS settings not configured. The following instructions must be followed to ensure the module operates in a FIPS-Approved mode of operation.

#### 3.4.2.1 Turning On FIPS Cryptography

The CO shall enable FIPS cryptography. This ensures that the system will use only FIPS-Approved cryptographic algorithms and key sizes. FIPS cryptography can be enabled using either the Java Console or Web Console to perform the following steps:

1. Navigate to the **System** tab
2. Click on the **Settings** tab
3. Click on the **Disabled** setting for **FIPS Encryption**
4. In the **Enable FIPS Encryption** window, enter your password and then click **Enable FIPS Encryption**
5. Click **OK** in the confirmation prompt
6. The system will reboot
7. FIPS Encryption will now be reported as **Enabled**

### 3.4.2.2 *Configure Strong Passwords for Password-Based Authentication*

The CO shall configure strong passwords for operator authentication. Enabling strong passwords ensures that the module enforces the use of passwords that are a minimum of 15 characters in length and contain at least one number, one upper-case letter, one lower-case letter or special character. The strong passwords feature is enabled and configured by using either the Java Console or Web Console to perform the following steps:

1. Navigate to the **System** tab
2. Click on the **Settings** tab
3. Under **Remote Services**, click on the text that appears next to **Authentication**
4. In the **Set Authentication Mode** window, configure **Local**<sup>26</sup> authentication and ensure that **Enable password policies** and **Enable DoD Security Policies** are enabled
5. Set the **Minimum password length** greater than or equal to 15
6. Configure the **Lock users after** value to between 35 and 365 days
7. Click **OK** in the **Set Authentication Mode** window
8. Click **OK** again at the confirmation prompt
9. Click **OK** again at the information prompt
10. The operator will be forced to login again and then change the account password so that it conforms to the now enabled DoD password policy
11. Authentication will now be reported as **Local**

### 3.4.2.3 *Enable TLS/HTTPS*

The CO shall enable TLS/HTTPS. Enabling TLS/HTTPS ensures that management sessions using either the Java Console or Web Console are encrypted. TLS/HTTPS is enabled by using either the Java Console or Web Console to perform the following steps:

1. Navigate to the **System** tab
2. Click on the **Settings** tab
3. Under **General**, click on **Disabled** next to **TLS/HTTPS**
4. In the **TLS/HTTPS Configuration** window, enable the **Enable console encryption** option
5. Click **OK** in the **TLS/HTTPS Configuration** window
6. Click **OK** again at the confirmation prompt
7. Click **OK** again at the information prompt
8. The system will reboot
9. TLS/HTTPS will now be reported as **Enabled**

### 3.4.2.4 *Change the TLS/HTTPS Certificate*

The CO shall replace the default TLS/HTTPS certificate. The TLS/HTTPS certificate is replaced by using either the Java Console or Web Console to perform the following steps:

1. Navigate to the **System** tab
2. Click on the **Settings** tab
3. Under **General**, click on **Enabled** next to **TLS/HTTPS**
4. In the **TLS/HTTPS Configuration** window, click **Generate CSR...**
5. Complete the fields in the **Certificate Signing Request** window
6. Click **Update** in the **Certificate Signing Request** window
7. Click **OK** at the information prompt

---

<sup>26</sup> References to local authentication throughout this document should be considered as: an authentication method that uses locally stored operator accounts (as opposed to RADIUS accounts) and is used to authenticate operators accessing the Java Console and Web Console interfaces.

8. Click **Generate CSR...** in the **Certificate Signing Request** window
9. Click **OK** at the confirmation prompt
10. In the **Save** window, select a save location for the certificate file and then click **OK**
11. Click **OK** at the confirmation prompt
12. Click **Close** in the **Certificate Signing Request** window
13. Supply the certificate signing request to a trusted certification authority and request a TLS server certificate to be generated; for more information, refer to *Ixia Net Tool Optimizer (NTO) 7303 User Guide, NVOS 4.5, August 2016*, chapter entitled "Uploading Custom TLS/HTTPS Certificates"
14. Once the certificate has been signed, click **Upload** in the **TLS/HTTPS Configuration** window
15. In the **Browse** window, browse to and select the newly created server certificate file and click **Open**
16. Click **OK** in the **TLS/HTTPS Configuration** window
17. The default TLS/HTTPS certificate has been replaced

#### 3.4.2.5 **Disable the Craft Port**

The CO shall disable the Craft Port. The craft port is disabled by using either the Java Console or Web Console to perform the following steps:

1. Navigate to the **System** tab
2. Click on the **Settings** tab
3. Under **General**, click **Enabled** next to **Serial port access**
4. Click **OK** at the confirmation prompt
5. Serial port access will now be reported as **Disabled**

#### 3.4.2.6 **Disable Tcl**

The CO shall disable Tcl. Tcl is disabled by using either the Java Console or Web Console to perform the following steps:

1. Navigate to the **System** tab
2. Click on the **Settings** tab
3. Under **General**, click **Enabled** next to **Tcl**
4. Click **OK** at the confirmation prompt
5. Tcl will now be reported as **Disabled**

#### 3.4.2.7 **Configuring SNMP (Optional)**

If SNMP is used then the following instructions shall be implemented, otherwise SNMP shall remain disabled. SNMP, if used, is configured by using the Web Console to perform the following steps:

1. Navigate to the **System** tab
2. Click on the **Settings** tab
3. Click the text next to **SNMP**
4. In the **Set SNMP Configuration** window, make sure **Enable SNMP Requests** is checked
5. Under **Access Control (Community String or Local User<sup>27</sup>)** click **Add**
6. In the **Add SNMP Access Control** window, configure the SNMP version to be **V3**
7. Type the username for the SNMP user in the **SNMP user name** field
8. Configure the **Security level** to **Authentication and privacy required**
9. Under **Authentication** make sure **Protocol** is set to **HMAC\_SHA\_96<sup>28</sup>**

---

<sup>27</sup> Local User refers to a locally stored operator account.

<sup>28</sup> While the GUI indicates the Authentication Protocol as HMAC\_SHA\_96, the underlying algorithm is actually SHA-1.

Ixia Net Tool Optimizer (NTO) 7303

10. Under **Authentication** make sure the **Password** and **Confirm Password** fields are set to the desired SNMP login password (See note below)
11. Under **Privacy** make sure the **Protocol** field is set to one of:
  - a. AES128
  - b. AES192
  - c. AES256
12. Under **Privacy** make sure the **Password** and **Confirm Password** fields are set to the desired SNMP privacy secret (See note below)
13. Click **OK** in the **Add SNMP Access Control** window
14. Click **OK** in the **Set SNMP Configuration** window

**\*NOTE:** The SNMP configuration does not automatically enforce password complexity requirements. The CO shall take care to make sure that SNMP passwords match the following complexity requirements:

- Password must be at least 15 characters in length
- Password must contain at least one upper-case letter
- Password must contain at least one lower-case letter
- Password must contain at least one number
- Password must contain at least one special character

#### **3.4.2.8 Configuring Syslog Encryption and Installing a Certificate (Optional)**

If using a Syslog server to obtain syslogs from the module then the following instructions shall be implemented, otherwise Syslog shall remain disabled. If using Syslog, then the following steps shall be executed using the Java Console or Web Console:

1. Navigate to the **System** tab
2. Click on the **Settings** tab
3. Under **Remote Services**, click the text next to **Syslog** to open the Syslog configuration dialog
4. Click **Add** and enter the DNS Name or IPv4 Address of the external Syslog server
5. Check **Enable TLS Encryption**
6. Click **OK**
7. Click **OK**
8. Click **Generate CSR**
9. Configure all of the appropriate information and click **Update**
10. Click **OK** at the information prompt
11. Click **Generate CSR**
12. Click **OK**
13. In the **Save** window, choose a save location for the certificate request file and click **OK**
14. Click **Close**
15. Supply the certificate signing request to a trusted certification authority and request a TLS client certificate to be generated; for more information, refer to *Ixia Net Tool Optimizer (NTO) 7303 User Guide, NVOS 4.5, August 2016*, chapter entitled "Add a Syslog Server"
16. Click **Upload** under **Client Certificate**
17. In the **Choose TLS Certificate File**, select the TLS client certificate generated in the previous step
18. Click **OK**
19. Request the trusted root certificate from your certificate authority
20. Under **Server Trusted Root**, click **Upload**
21. In the **Choose TLS certificate** window, select the trusted root certificate and click **OK**

22. Click **OK**

### 3.4.2.9 ATIP SSL/TLS Decryption

ATIP SSL/TLS decryption is disabled by default and shall remain disabled.

Once all of the above steps have been completed the module is now operating in the FIPS-approved mode of operation.

## 3.4.3 Determining the FIPS-Approved Mode

The CO can verify that the module is operating in the FIPS-Approved mode of operation by performing the following checks:

1. Password-based authentication is enabled and DoD password policy is enabled. Use the Web Console or Java console to navigate to **System** and then **Settings**. Open the configuration settings for Authentication and ensure that it is set to **Local**. In addition, ensure that **Enable password** policies and **Enable DoD Security Policies** are checked, and that the **Minimum password length** has been set to 15. For more information, see Section 3.4.2.2.
2. Using the Web Console or Java Console, authenticate to the module navigate to **System** and then **Settings**. On the Settings page, ensure the following:
  - a) FIPS encryption is **Enabled**
  - b) TLS/HTTPS is **Enabled**
  - c) Serial port access is **Disabled**
  - d) Tcl is **Disabled**
  - e) Syslog is either **Not Set**, or an IP address or DNS name is present
  - f) SNMP is either **Enabled** or **Disabled**
3. Verify SNMP Settings – this is only required if SNMP is enabled in the previous step. If SNMP is enabled, using the Web Console or Java Console, navigate to **System** and then **Settings**. On the **Settings** page, click on **Enabled** which appears next to SNMP which will open the **Set SNMP Configuration (Community String or Local User) Pane**. The summary for each entry should report the following:
  - a) Version: **V3**
  - b) Security Level: **Authentication and privacy required**
  - c) Auth Protocol: **HMAC\_SHA\_96**
  - d) Priv Protocol: **AES-128** or **AES-192** or **AES-256**
  - e) For more information, see instructions in Section 3.4.2.7 above
4. Verify Syslog Settings – this is only required if Syslog is enabled in Step 4. If syslog is enabled, using the Web Console or Java Console, navigate to **System** and then **Settings**. On the **Settings** page, click the link next to **Syslog**. Perform the following:
  - a) Select the syslog server from the list of servers, and click **Modify**
  - b) Verify that **Enable TLS encryption** is set for the syslog server
  - c) Click **Cancel**
  - d) Verify that the Subject and Issued by fields are correct for both the **Server Trusted Root Certificate** and the **Client Certificate**
  - e) Select the syslog server again and click **Test**
  - f) For more information, see instructions in Section 3.4.2.8 above
5. Verify that ATIP SSL/TLS Decryption is not configured. Using the Java Console, perform the following:
  - a) Click on **Diagram**.
  - b) In the **Resources** view, right click on the ATIP box and select **Launch ATIP**.

- c) Click on the **NF** button (top right corner) and then click on **SSL**.
- d) Ensure that **Enable Passive SSL Decryption** is unchecked.

Once the module has been configured to be in the FIPS-Approved mode, the CO shall ensure that it remains in the FIPS-Approved mode until it is ready to be decommissioned. At this time, the module can be factory reset to revert to a non-FIPS-Approved mode. The factory reset command can be entered from the Java Console by going to **File** → **Factory Reset** with any CO account.

### 3.4.4 Non-Approved Services

The services in Table 9 are non-Approved and therefore shall not be used in an Approved mode of operation. Installing and configuring the module per Section 3 of this SP will ensure that the non-Approved services will not be used.

In addition, the “ATIP SSL Decryption” feature only becomes available in a non-Approved mode of operation; thus it does not map to any of the services in section 2.4 above.

**Table 9 – Non-Approved Services**

| Service  | Algorithm                                    | Use                 |
|--|--|---------------------|
| Encrypt SNMP data (Table 6)<br>Decrypt SNMP data (Table 6)       | DES  | SNMPv3              |
| Produce HMAC digest (Table 6)                                    | HMAC-MD5                                     | SNMPv3              |
| Hash function to support “Produce HMAC digest” service (Table 6) | MD5  | SNMPv3              |
| Encryption/Decryption  | AES-CBC, AES-GCM (all key sizes)             | ATIP SSL Decryption |
| Encryption/Decryption  | TDES-CBC (all key sizes)                     | ATIP SSL Decryption |
| Encryption/Decryption  | RC4 (all key sizes)                          | ATIP SSL Decryption |
| Message Authentication   | HMAC-SHA-1,<br>HMAC-SHA-256,<br>HMAC-SHA-384 | ATIP SSL Decryption |
| Key Agreement  | ECDH (all key sizes)                         | ATIP SSL Decryption |
| Digital Signature Generation/Verification                        | ECDSA (all key sizes)                        | ATIP SSL Decryption |
| Digital Signature Generation/Verification<br>Key Transport       | RSA (all key sizes)                          | ATIP SSL Decryption |
| Hashing  | MD5  | ATIP SSL Decryption |
| Hashing  | SHA-1,<br>SHA-256,<br>SHA-384                | ATIP SSL Decryption |

When the module is installed and configured as per Section 3 of this SP, the following non-Approved services are disabled and no longer available for use.

**Table 10 – Non-Approved Algorithm Implementations**

| Service  | Algorithms                            |
|--|---------------------------------------|
| Key Generation<br>Key Transport<br>Digital Signature Generation/Verification | RSA with key size less than 2048 bits |

# 4. Acronyms

Table 11 provides definitions for the acronyms used in this document.

**Table 11 – Acronyms**

| Acronym | Definition                                |
|---------|---|
| AES     | Advanced Encryption System                |
| AFM     | Advanced Feature Module                   |
| ANSI    | American National Standards Institute     |
| API     | Application Programming Interface         |
| ATIP    | Application Threat Intelligence Processor |
| CBC     | Cipher Block Chaining                     |
| CCM     | Counter Mode with CMAC                    |
| CFB     | Cipher Feedback                           |
| CFP     | C Form-Factor Pluggable                   |
| CKG     | Cryptographic Key Generation              |
| CMVP    | Cryptographic Module Validation Program   |
| CO      | Cryptographic Officer                     |
| CRC     | Cyclic Redundancy Check                   |
| CSE     | Communications Security Establishment     |
| CSP     | Critical Security Parameter               |
| CTR     | Counter                                   |
| DH      | Diffie-Hellman                            |
| DRBG    | Deterministic Random Bit Generator        |
| EC      | Elliptic Curve                            |
| ECB     | Electronic Codebook                       |
| EMC     | Electromagnetic Compatibility             |
| EMI     | Electromagnetic Interference              |
| FIPS    | Federal Information Processing Standard   |
| G       | Gigabit                                   |
| HMAC    | (keyed-) Hash Message Authentication Code |
| KAT     | Known Answer Test                         |
| KDF     | Key Derivation Function                   |
| LCD     | Liquid Crystal Display                    |
| NDRNG   | Non-Deterministic Random Number Generator |
| NEBS    | Network Equipment Building Standards      |

| Acronym | Definition                                       |
|---------|--|
| NIST    | National Institute of Standards and Technology   |
| NTO     | Net Tool Optimizer                               |
| NVOS    | Network Visibility Operating System              |
| OS      | Operating System                                 |
| PBKDF   | Password Based Key Derivation Function           |
| PCM     | Packet Capture Module                            |
| PKCS    | Public Key Cryptography Standard                 |
| QSFP    | Quad Small Form-Factor Pluggable                 |
| RAM     | Random Access Memory                             |
| RNG     | Random Number Generator                          |
| RSA     | Rivest Shamir and Adleman                        |
| SFP     | Small Form-Factor Pluggable                      |
| SHA     | Secure Hash Algorithm                            |
| SNMP    | Simple Network Management Protocol               |
| SP      | Special Publication                              |
| SPAN    | Switch Port Analyzer                             |
| TACACS  | Terminal Access Controller Access Control System |
| TAP     | Test Access Point                                |
| TLS     | Transport Layer Security                         |
| U       | Unit (Rack space measurement)                    |
| USB     | Universal Serial Bus                             |

---

Prepared by:  
**Corsec Security, Inc.**



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

Phone: +1 703 267 6050

Email: [info@corsec.com](mailto:info@corsec.com)

<http://www.corsec.com>

---