FIPS 140-2 Non-Proprietary Security Policy
for
OmniSwitch AOS 8.3.1.R01

FIPS Security Level: 2
Document Version: 1.3.3
Date: March 27, 2019

Prepared For:

ALE USA Inc.
26801 West Agoura Road
Calabasas, CA
USA 91301
https://www.al-enterprise.com/

Prepared By:

EWA-Canada, Ltd.
1223 Michael Street North, Suite 200
Ottawa, Ontario
Canada K1J 7T2
http://www.intertek.com/cybersecurity/ewa-canada/

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

This non-proprietary Security Policy for the OmniSwitch AOS 8.3.1.R01 series of Cryptographic Modules by Alcatel-Lucent Enterprise describes how the modules meet the security requirements of FIPS 140-2 and how to run the modules in a secure FIPS 140-2 mode of operation.

This document was prepared as part of the Level 2 FIPS 140-2 validation of the modules. The following table lists the modules' FIPS 140-2 security level for each section.

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

Table 1 - FIPS 140-2 Section Security Levels

1.2 Background

Federal Information Processing Standards Publication (FIPS PUB) 140-2 – *Security Requirements for Cryptographic Modules* details the requirements for cryptographic modules. More information on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP), the FIPS 140-2 validation process, and a list of validated cryptographic modules can be found on the CMVP website:

http://csrc.nist.gov/groups/STM/cmvp/index.html

More information about Alcatel-Lucent Enterprise and the OmniSwitch Products can be found on the Alcatel Lucent Enterprise website:

https://www.al-enterprise.com/

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE.

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1.3 Document Organization

This non-proprietary Security Policy is part of the Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 FIPS 140-2 submission package. Other documentation in the submission package includes:

- Product documentation
- Vendor evidence documents
- Finite state model
- Additional supporting documents

The Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 is also referred to in this document as the AOS Cryptographic Modules, cryptographic modules, or the modules.

1.4 Module Versions Supported

The following hardware model versions were tested and make up the AOS 8.3.1.R01 series of Cryptographic Modules:

Series	Model
6860	6860-24 6860-P24 6860-48 6860-P48 6860E-24 6860E-P24 6860E-48 6860E-P48 6860E-U28
6865	6865-P16X
6900	6900-X20 6900-X40 6900-T20 6900-T40 6900-Q32 6900-X72

Table 2 - FIPS 140-2 Hardware Versions

All of the hardware versions listed above utilize the AOS 8.3.1.R01 firmware.

1.5 Platform Series Overview

1.5.1 OmniSwitch 6860

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Alcatel-Lucent OmniSwitch® 6860 Stackable LAN Switches (SLS) are compact, high-density Gigabit Ethernet (GigE) and 10 GigE platforms designed for the most demanding converged networks.

In addition to high performance and availability, the OmniSwitch(OS) 6860(E) offers enhanced quality of service (QoS), deep packet inspection (DPI), and comprehensive security features to secure the network edge while accommodating user and device mobility with a high degree of integration between the wired and wireless LAN.

The enhanced models of the OmniSwitch 6860 family also supports emerging services such as application fingerprinting for network analytics and up to 60 watts of Power over Ethernet (PoE) per port, making it ready to meet the evolving business needs of enterprise networks.

These versatile LAN switches can be positioned:

- At the edge of mid- to large-sized converged enterprise networks
- At the aggregation layer
- In a small enterprise network core
- In the data center for GigE server connectivity and SDN applications

1.5.2 OmniSwitch 6865

The Alcatel-Lucent OmniSwitch® 6865 series of switches are industrial grade, high-density, advanced Ethernet platforms designed for operating reliably in the harshest of environmental & severe temperature environments.

OS6865 switches are rugged, high bandwidth switches that are ideal for industrial and mission-critical applications that require wider operating temperature ranges, stringent EMC/EMI requirements and an optimized feature set for high security, reliability, performance and easy management. These switches run on the widely deployed & field-proven Alcatel-Lucent Operating system offering SPB-M based VPNs and other advanced routing & switching capabilities.

The OS6865 series offers a unique mix of features to cater to the Hardened Ethernet applications such as IEEE 1588v2 PTP capabilities for timing requirements of industrial devices, HPoE (75W PoE) for those power hungry devices on the access network, SPB-M for fast, cost-efficient roll-out of VPN services on the edge and a comprehensive suite of security features to secure the network edge. These switches are easy to deploy with our award winning Intelligent-Fabric technology which offers out-of-the-box plug-and-play, Zero-touch provisioning and network automation. The OS6865 family offers advanced system & network level resiliency features and convergence through standardized protocols.

These versatile industrial switches are ideal for deployment in transportation and traffic control systems, power utilities, video surveillance systems and outdoor installations.

1.5.3 OmniSwitch 6900

The Alcatel-Lucent Enterprise OmniSwitch™ 6900 Stackable LAN and data center switches are compact, high-density 10 Gigabit Ethernet (GigE) and 40 GigE platforms. In addition to high performance and extremely low latency, they offer VXLAN, OpenFlow, Shortest Path Bridging (SPB), data center bridging (DCB) capabilities, QoS, Layer-2 and Layer-3 switching, as well as system and network level resiliency.

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

They are designed for the most demanding software-defined operations in virtualized or physical networks and converged data centers. With their modular approach, the OmniSwitch 6900s support lossless configurations and native fibre channel ports for high-speed storage I/O consolidation.

They can be positioned as converged top-of-rack or spine switches in data center environments as well as core and aggregation devices in campus networks.

2 Module Overview

The OmniSwitch AOS 8.3.1.R01 series of switches are rugged and high bandwidth switches running on the widely-deployed and field-proven Alcatel-Lucent Operating System (AOS). These switches are ideal for industrial and mission-critical applications that require wider operating temperature ranges, more stringent EMC/EMI requirements, and an optimized feature set for high security, reliability, performance, and easy management. For the purposes of FIPS 140-2, the modules are classified as hardware modules with a multi-chip standalone embodiment.

2.1 Cryptographic Module Specification

The cryptographic boundary of the modules are defined to be the entire enclosure of the modules. Depicted below is the module block diagram, which indicates the direction and types of information flow between module components as well as highlighting the cryptographic boundary of the module.

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

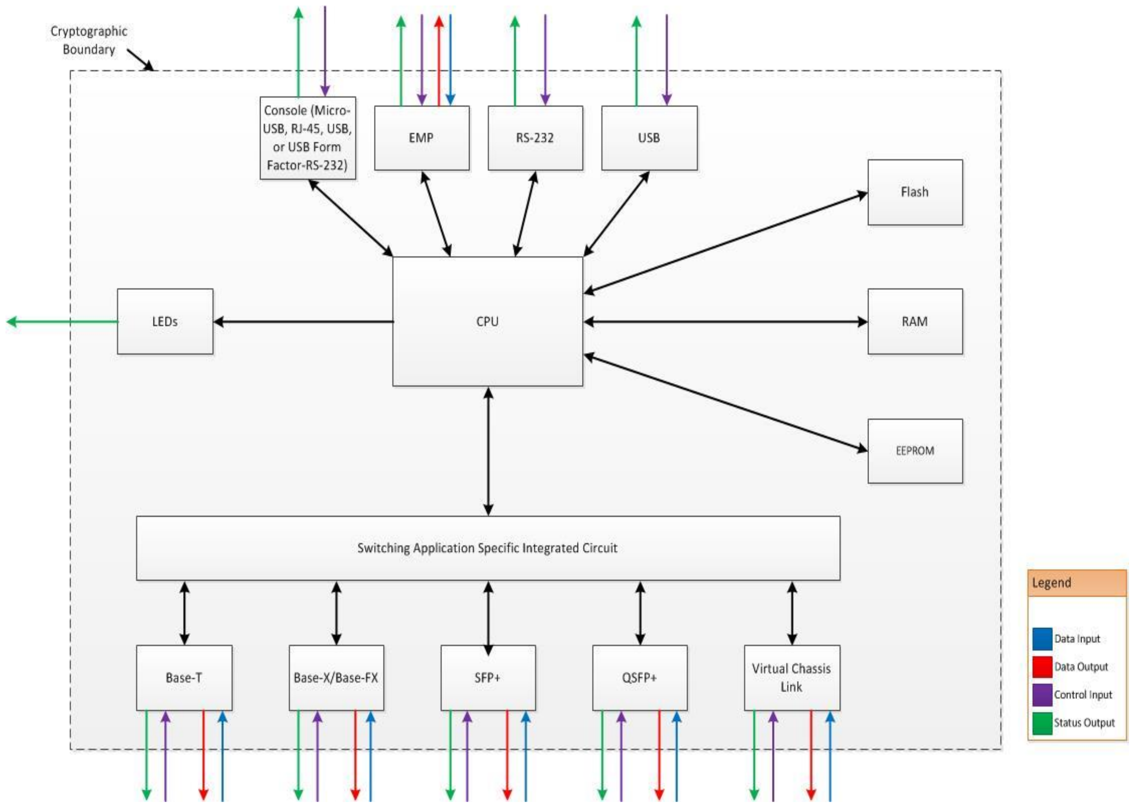

Figure 1 - Block Diagram

Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 Cryptographic Module Security Policy © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.2 Cryptographic Module Ports and Interfaces

The modules' physical ports and interfaces are those of which comprise the modules. For the OmniSwitch series of routers, the physical ports and interfaces would be as follows:

- EMP (Ethernet Management Port), RS-232, micro-USB, RJ-45, USB, SFP, SFP+, QSFP+, Base-T, Base-X/Base-FX, and Virtual Chassis Link Ports
- LEDs
- Power supplies

Tables 3, 4, and 5 provide the mapping between the physical interfaces for the 6860, 6865, and 6900 series modules to their corresponding FIPS 140-2 defined interfaces:

FIPS 140-2 Interface	Physical Interface
Data Input	EMP (Ethernet Management Port)
	Base-T ports
	Base-X/Base-FX ports
	SFP+ Ports
	Virtual Chassis Link Ports
Data Output	EMP
	Base-T ports
	Base-X/Base-FX ports
	SFP+ Ports
	Virtual Chassis Link Ports
Control Input	EMP
	Console Port (micro-USB)
	USB Port
	RS-232 Port
	Base-T ports
	Base-X/Base-FX ports
	SFP+ Ports
	Virtual Chassis Link Ports
Status Output	Status LEDs
	Console Port (micro-USB)
	USB Port
	RS-232 Port
	EMP
	Base-T ports
	Base-X/Base-FX ports
	SFP+ Ports
	Virtual Chassis Link Ports
Power Input	Hardware Power Connector
	Ethernet (PoE)

Table 3 - Module Interface Mappings for the OmniSwitch 6860 Series of Switches

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

FIPS 140-2 Interface	Physical Interface
Data Input	SFP+ Ports
	Base-X SFP Ports
	Base-T Ports
Data Output	SFP+ Ports
	Base-X SFP Ports
	Base-T Ports
Control Input	Console Port (RJ-45)
	USB Port
	SFP+ Ports
	Base-X SFP Ports
	Base-T Ports
Status Output	Status LEDs
	Console Port (RJ-45)
	USB Port
	SFP+ Ports
	Base-X SFP Ports
	Base-T Ports
Power Input	Hardware Power Connector
	Ethernet (PoE)

Table 4 - Module Interface Mappings for the OmniSwitch 6865

FIPS 140-2 Interface	Physical Interface
Data Input	EMP (Ethernet Management Port)
	SFP+ Ports
	Base-T Ports
	QSFP+ Ports
Data Output	EMP
	SFP+ Ports
	Base-T Ports
	QSFP+ Ports
Control Input	Console Port (USB)
	Console Port (USB Form Factor – RS-232)
	Console Port (RJ-45)
	USB Port
	EMP
	SFP+ Ports
	Base-T Ports
	QSFP+ Ports
Status Output	Status LEDs
	Console Port (USB)
	Console Port (USB Form Factor – RS-232)
	Console Port (RJ-45)
	USB Port
	EMP
	SFP+ Ports
	Base-T Ports
	QSFP+ Ports
Power Input	Hardware Power Connector
	Ethernet (PoE)

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table 5 - Module Interface Mappings for the OmniSwitch 6900 Series of Switches

2.3 Roles & Services

2.3.1 Roles

The module has two operator roles: Crypto Officer and User. The Crypto Officer is an administrative role that is responsible for initialization, configuration, and monitoring of services that are supported by the modules. The User role can perform cryptographic services that are provided by the modules.

The modules implement explicit role-based authentication. An operator assumes the role of Crypto Officer or User based on the credentials (username and password) they use to login to the modules.

2.3.2 Services

Table 6 below specifies the services that are available to a module operator. In the CSP Access column, Read and Execute mean the CSP is used by the modules to perform the service, and Write means the CSP is generated, modified or deleted by the modules.

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Service	Operator	Description	Input	Output	Key/CSP	CSP Access
Create Operator Account	User/Crypto Officer	Creation of an Operator Account	Operator Password	N/A	Crypto Officer Password, User Password	Write
Modify Operator Account	User/Crypto Officer	Change the Operator Password	Existing Operator Password, Proposed Operator Password	N/A	Crypto Officer Password, User Password	Write
Delete Operator Account	User/Crypto	Deletion of an existing Operator Account	N/A	N/A	Crypto Officer Password, User Password	Write
Establish TLS Session	User	Establishment of a TLS Session	(EC) Diffie-Hellman Key Pair, RSA/ECDSA Key Pair	TLS Session Encryption Key, TLS Session Message Authentication Key	Diffie-Hellman Private Key, Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman Public Key, RSA Public Key, RSA Private Key, ECDSA Public Key, ECDSA Private Key, TLS Pre-master Secret, TLS Master Secret, AES-CBC TLS Session Encryption Key, AES-GCM TLS Session Encryption Key, TLS Session Message Authentication Key	Read/Write/Execute
Establish SSH Session	User	Establishment of a SSH Session	(EC) Diffie-Hellman Key Pair, RSA/ECDSA Key Pair	SSH Session Encryption Key, SSH Session Message Authentication Key	Diffie-Hellman Private Key, Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman Public Key, RSA Public Key, RSA Private Key, ECDSA Public Key, ECDSA Private Key, SSH Pre-master Secret, SSH Master Secret, AES-CBC SSH Session Encryption Key, SSH Session Message Authentication Key	Read/Write/Execute
Generate Random Number	User	Generates random bits for using in key generation	Number of random bits requested	Random bits	DRBG Entropy, DRBG Seed, DRBG “Key” Value, DRBG Seed	Read/Execute
Generate Asymmetric Key	User	Generates asymmetric key pair	Key size	Asymmetric key pair	ECDSA Public Key, ECDSA Private Key, RSA Public Key, RSA Private Key	Read/Write/Execute

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Service	Operator	Description	Input	Output	Key/CSP	CSP Access
Hash	User	Calculates a hash using SHA	Plaintext data	Hashed data	N/A	N/A
Authenticate	User/Crypto Officer	Operator authenticates to a module via Console or SSH	Operator Password/ SSH RSA Private Key	N/A	User Password, Crypto Officer Password, SSH RSA Private Key, SSH RSA Public Key, Diffie-Hellman Private Key, Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman Public Key, SSH Pre-master Secret, SSH Master Secret, AES-CBC SSH Session Encryption Key, SSH Session Message Authentication Key	Read/Execute
Installation, Uninstallation, and Initialization	Crypto Officer	Install, initialize, configure, uninstall	N/A	N/A	N/A	N/A
Key Agreement	User	Perform key agreement of (EC) Diffie-Hellman for use in TLS/SSH key exchange	EC DH public key and private Key	TLS/SSH Session Key	Diffie-Hellman Private Key, Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman Public Key	Read/Write/Execute
Self-Test	User/Crypto Officer	Performs self-tests	N/A	Pass or fail return code	SHA-256 FLASH Integrity Test Hash	Read
Show Status	User/ Crypto Officer	Displays module status and version	N/A	Module status	N/A	Execute
Zeroize	User/Crypto Officer	Zeroize CSPs	N/A	N/A	All keys/CSPs with the exception of the User/Crypto Officer passwords and the SHA-256 FLASH Integrity Test Hash	Write

Table 6 - Services

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.4 Authentication Mechanism

The modules implement explicit role-based authentication. An operator assumes the role of Crypto officer or User based on the credential they use to login to the modules. In order for an operator to change roles, they must first log out of the current role they have assumed. This will require the operator to re-authenticate to the modules with the appropriate username and password combination.

When configured for operation in the Approved Mode, the modules accept passwords that varying in length from 15 to 30 characters. Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["@", "#","$", "%", "^", "&", "*", "(", ")", “~”, “{“, “}”, “[“, ”]”, “:”, “;”, “|“,“\“, “/”, “.”, “<” and “>"]. This makes up a total of 84 possible characters that can be used in a password. In addition, specifying an asterisk (*) as one or more characters in a password is allowed as long as every character is not an asterisk.

If we assume that a user selects a password of length 15 (the lower-bound for password length), then there is a 1 in $84^{15} - 1$ chance that a random attempt will succeed or a false acceptance will occur, which is a rate much less than the minimum rate of 1 in 1,000,000.

The maximum throughput data rate that can by supported by any of the modules is 2.56 terabits/seconds, which corresponds to a rate of 2,560,000 megabits/second or 2,560,000,000,000 bits/second (or 2.56 x 10^{12}bits/second). If we assume the maximum rate is consistent for one minute, then this results in the processing of 1.536 x 10^{14} bits of data (2.56 x 10^{12}bits/second x 60 seconds) or 1,152,000,000,000,000 bytes. Given that a maximum of 1,152,000,000,000 bytes of data can be processed in one minute, if we solely consider passwords of length 15 (the minimum length allowed in the Approved Mode), then the number of password combinations that can be processed in a minute is 76,800,000,000,000 (1,152,000,000,000,000 bytes ÷ 15 bytes/password). Given the number of password combinations that can be processed in a minute, we can conclude that the probability of a random attempt succeeding or a false acceptance occurring is approximately 1 in 1.049958 x 10^{15} (76,800,000,000,000 combinations/minute ÷ $84^{15} - 1$ total combinations), which is a rate far below the minimum rate of 1 in 100,000.

In addition to password authentication, users have the ability to authenticate to the module using public key authentication (RSA 2048-bit), when the modules are configured for use of SSH. Given that 2^{2048} > $84^{15} - 1$, we can conclude that the public key authentication mechanism for SSH has a rate below the required FIPS 140-2 threshold that a random attempt will succeed or a false acceptance will occur.

2.5 Physical Security

All keys and CSPs are protected by the module’s tamper evident enclosure. In order to operate in the Approved Mode of Operation, tamper evident seals shall be applied to the modules. It is the responsibility of the Crypto Officer to properly place all tamper evident seals as described in this section, and the Crypto Officer should maintain control of unused seals. The tamper-evident seals are only available as part of the OmniSwitch FIPS kit, part number OS-FIPSKIT. The seals are not available individually.

The Tamper-evident seals are extremely fragile and must be handled with care to prevent damage to the label. They cannot be removed without visible signs of damage to the labels. The tamper seals include a non-repeating serial number, which is used to prevent unauthorized replacement.

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 2 – ALE USA Inc. OmniSwitch Tamper Evident Seal

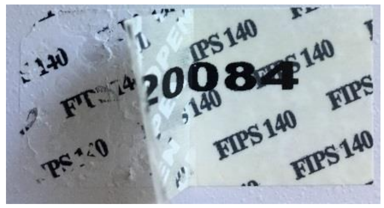

Figure 3 - ALE USA Inc. OmniSwitch Tamper Evident Seal showing signs of tamper

The Crypto Officer must apply the tamper evident seals to the areas shown in the proceeding Figures of this section. The following guidance is to be adhered by the Crypto Officer for application of the tamper labels:

1. The labels must be applied at 10ºC (50ºF) or above.
2. Turn off the OmniSwitch before cleaning or applying labels.
3. See OmniSwitch hardware guide for instructions and safety warnings on unmounting and mounting the OmniSwitch in a rack.
4. Clean the chassis of all grease, dirt or oil before applying tamper-evident labels. Alcohol-based cleaning pads are recommended. Ensure that it is completely dry before installation.
5. Curing time is 48 hours after application of labels. The OmniSwitch is not FIPS 140-2 level 2 compliant until the curing completes.
6. Ensure that air intake or exhaust holes are not significantly covered.

If the tamper evident seals are found to be damaged or broken during inspection, the Crypto Officer can return the module to a FIPS approved mode of operation byrestoring the module to a factory default state, reinitializing, and applying new tamper evident labels.

Any attempt to open the device will damage the tamper evident seals or the material of the module's enclosure. Signs of tampering include curled corners, rips, slices, red discoloration, and the word “OPEN”. The Crypto Officer should inspect the tamper evident labels periodically to verify that they are intact.

2.5.1 Label Placements for OmniSwitch 6860 models

The OmniSwitch 6860 models require 3 labels.

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

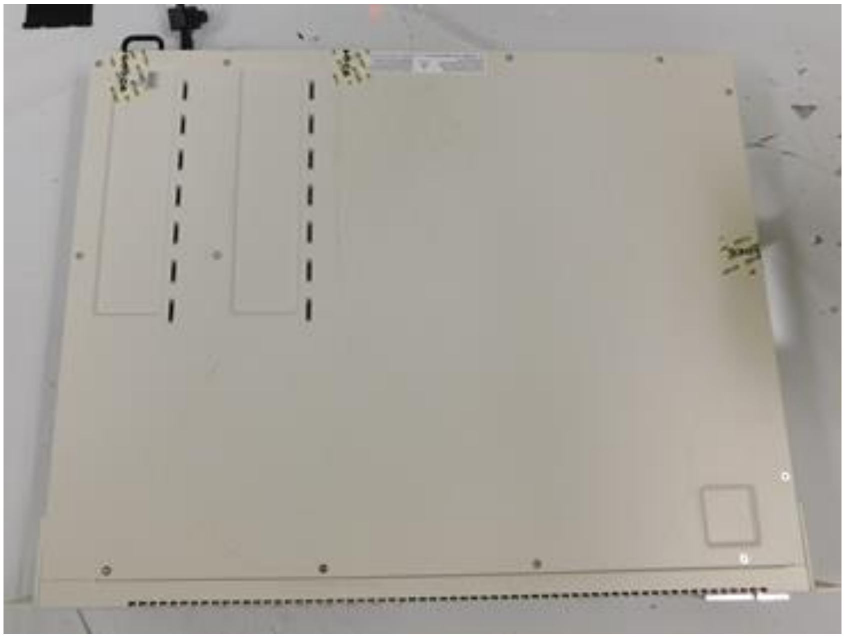

Figure 4 – Label Placements for OmniSwitch 6860-24/6860-P24 models

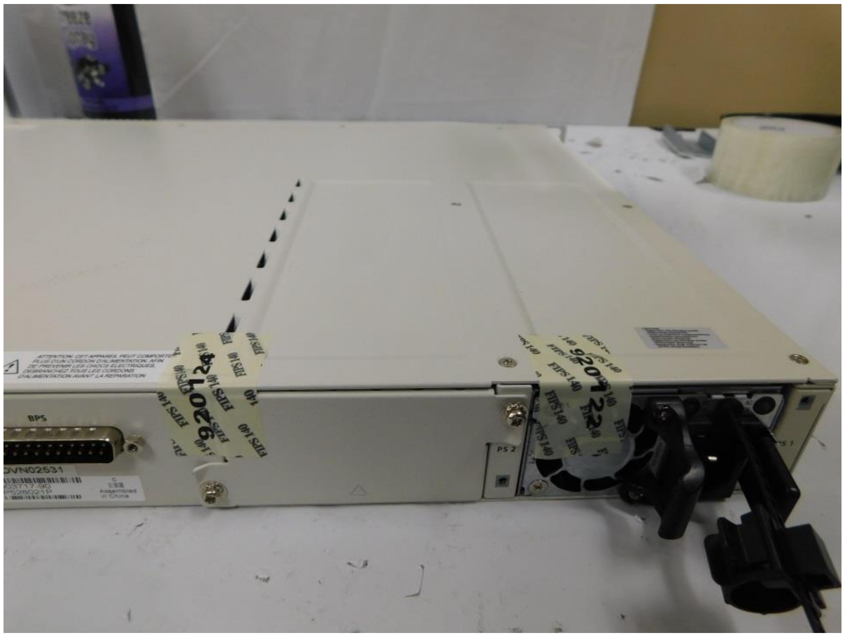

Figure 5 – Placement of rear tamper seals for OmniSwitch 6860

Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 Cryptographic Module Security Policy © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

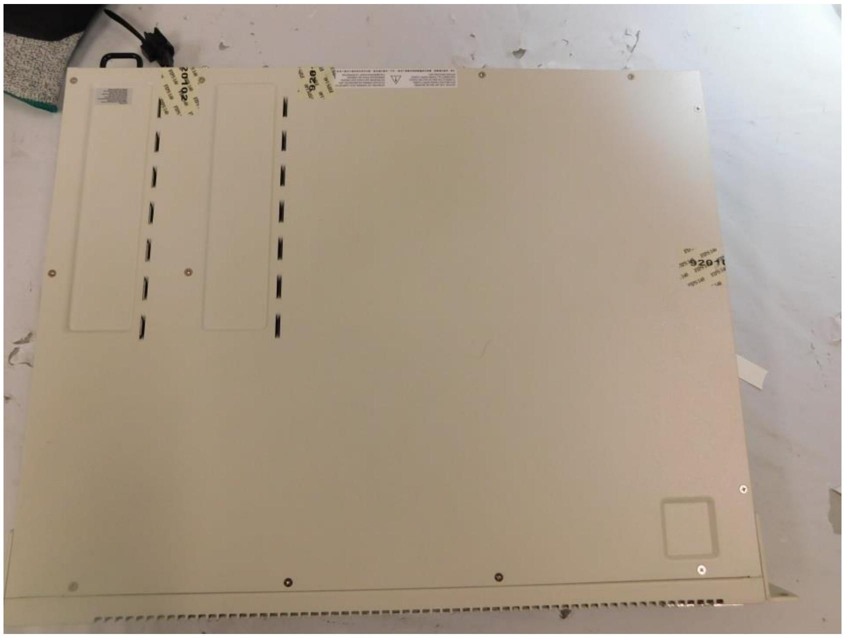

Figure 6 – Label Placements for OmniSwitch 6860-48/6860-P48 models

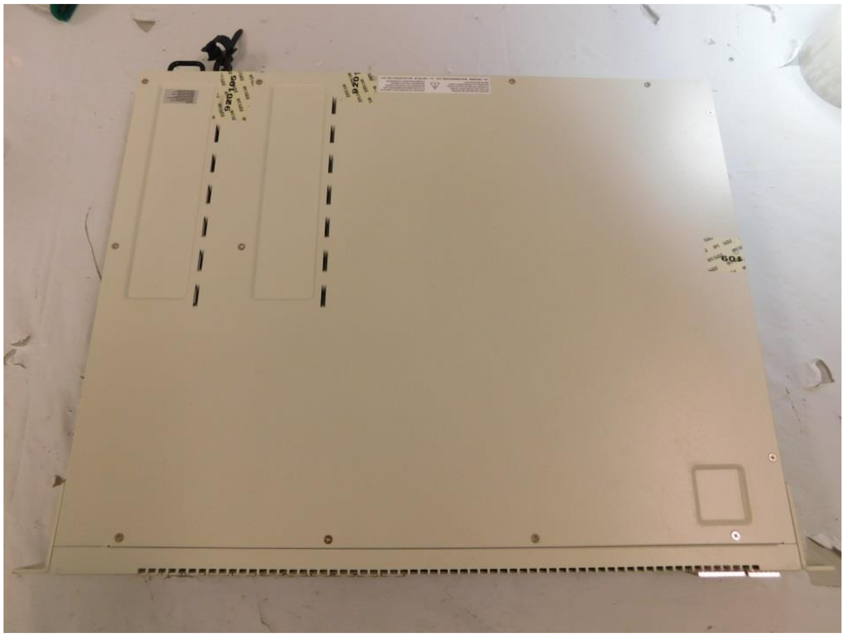

Figure 7 – Label Placements for OmniSwitch 6860E-24

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

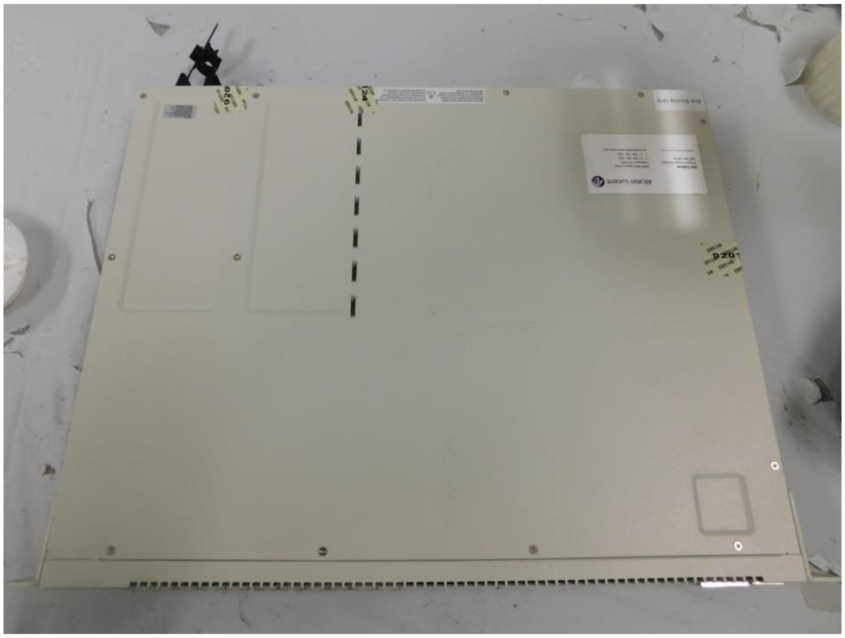

Figure 8 – Label Placements for OmniSwitch 6860E-P24

Figure 9 – Label Placements for OmniSwitch 6860E-48/6860E-P48 models

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 10 – Label Placements for OmniSwitch 6860E-U28

2.5.2 Label Placements for OmniSwitch 6865-P16X model

The OmniSwitch 6865-P16X requires 2 labels.

Figure 11 – Front Label Placement for OmniSwitch 6865-P16X

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 12 – Bottom/Right Label Placement for OmniSwitch 6865-P16X

2.5.3 Label Placements for OmniSwitch 6900-X20/6900-T20 models

The OmniSwitch 6900-X20 and 6900-T20 models require 5 labels.

Figure 13 – Front Label Placements for OmniSwitch 6900-X20 and 6900-T20

Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 Cryptographic Module Security Policy © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 14 – Rear Label Placements for OmniSwitch 6900-X20 and 6900-T20

2.5.4 Label Placements for OmniSwitch 6900-X40/6900-T40 models

The OmniSwitch 6900-X40 and 6900-T40 models require 6 labels.

Figure 15 – Front Label Placements for OmniSwitch 6900-X40 and 6900-T40

Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 Cryptographic Module Security Policy © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 16 – Rear Label Placements for OmniSwitch 6900-X40 and 6900-T40

2.5.5 Label Placements for OmniSwitch 6900-Q32/6900-X72 models

The OmniSwitch 6900-Q32 and 6900-X72 models require 4 labels.

Figure 17 – Front Label Placement for OmniSwitch 6900-Q32 and 6900-X72

Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 Cryptographic Module Security Policy © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

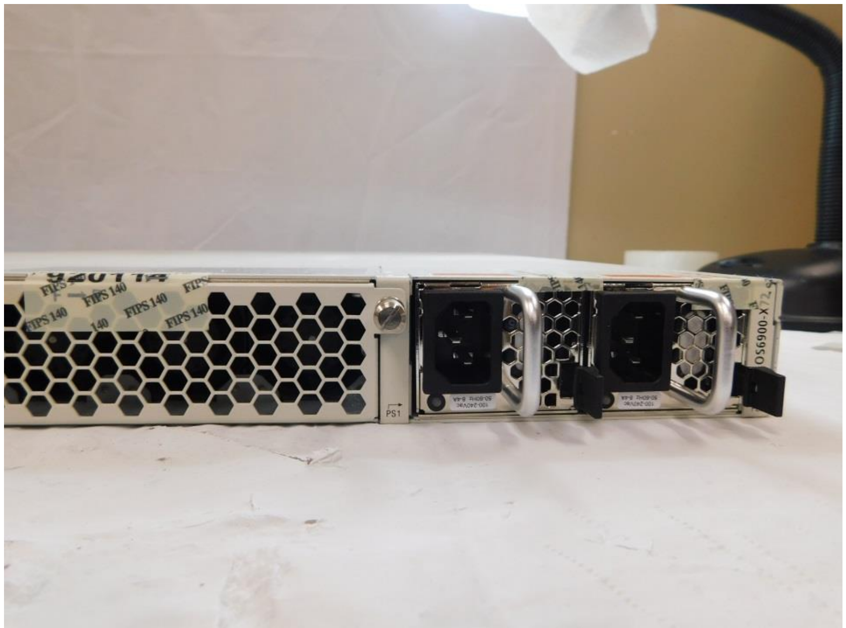

Figure 18 – Rear Label Placements for OmniSwitch 6900-Q32 and 6900-X72

2.6 Operational Environment

The Cryptographic Modules' operating environments are non-modifiable. Therefore, the FIPS 140-2 operational environment requirements are not applicable to the modules.

2.7 Cryptographic Key Management

2.7.1 Algorithm Implementations

2.7.1.1 Approved Algorithms

A list of FIPS-Approved algorithms implemented by the module can be found in Table 7.

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or	Use
#4285 #4286 #4287	AES	FIPS 197, SP800-38A	CBC	128/192/256 bits	Data Encryption and Decryption
#4440 #4441 #4443	AES	FIPS 197, SP800-38A	ECB	128/256 bits	Data Encryption and Decryption

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

#4440 #4441 #4443	AES	SP800-38D	GCM (IV generated internally per Section 8.2.1 of SP 800-38D)	128/256 bits	Data Encryption and Decryption
Vendor Affirmed	CKG[1]	SP 800-133			Key Generation
#1184 #1185 #1186	CVL TLS 1.0/1.1, TLS 1.2, SSH	SP 800-135	-	-	Key Derivation
#1345 #1346 #1347	DRBG	SP800-90A	Hash_DRBG HMAC_DRBG CTR_DRBG	-	Deterministic Random Bit Generation
#1078 #1079 #1081	ECDSA	FIPS 186-4	PKG, SigGen, SigVer	P-256 P-384 P-521	Digital Signature Generation and Verification
#2821 #2822 #2823	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-1-96[2] HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	512/1024 bits	Message Authentication
AES Cert. #4285 and HMAC Cert. #2821	KTS	Per IG D.9	-	128/256 bits	key establishment

[1] Resulting Symmetric keys and seeds used for asymmetric key generation are an unmodified output from an Approved DRBG.
[2] Used in the SSHv2 protocol. This usage is in compliance with FIPS 140-2 Implementation Guidance A.8 Use of HMAC-SHA-1-96 and Truncated HMAC.

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

AES Cert. #4286 and HMAC Cert. #2822	KTS	Per IG D.9	-	128/256 bits	key establishment
AES Cert. #4287 and HMAC Cert. #2823	KTS	Per IG D.9	-	128/256 bits	key establishment
AES Cert. #4440 and HMAC Cert. #2821	KTS	Per IG D.9	-	128/256 bits	key establishment
AES Cert. #4441 and HMAC Cert. #2822	KTS	Per IG D.9	-	128/256 bits	key establishment
AES Cert. #4443 and HMAC Cert. #2823	KTS	Per IG D.9	-	128/256 bits	key establishment
#2306 #2307 #2308	RSA	FIPS 186-4	-	2048 bits	Key Generation

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

#2306 #2307 #2308	RSA	FIPS 186-4	SHA-1 SHA-256 SHA-384 SHA-512 (ANSI X9.31 and PKCS1 v1.5)	2048 bits	Digital Signature Generation and Verification
#2421 #2425 #2427	RSA	FIPS 186-4	SHA-1 SHA-256 SHA-384 SHA-512 (SSA-PSS)	2048 bits	Digital Signature Generation and Verification
#3523 #3524 #3525	SHS	FIPS 180-4	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	-	Message Digest

Table 7 - FIPS-Approved Algorithm Implementations

2.7.1.2 Non-Approved but Allowed Algorithms

A list of non-Approved but Allowed algorithms implemented by the module can be found in Table 8.

Algorithm	Caveat	Use
Diffie-Hellman	Provides 112 bits of encryption strength.	Key establishment
EC Diffie-Hellman Support Curves: P-256, P-384, P-521	Provides between 128 and 256 bits of encryption strength.	Key establishment
RSA Key Wrapping	Provides 112 bits of encryption strength	Key establishment
NDRNG		Used to provide seed input into the module's Approved DRBG.[3]

Table 8 - Non-Approved but Allowed Algorithm Implementations

[3] The estimated amount of minimum entropy provided by the NDRNG is 279.68688 bits.

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.7.1.3 Non-Approved Algorithms

A list of non-Approved algorithms implemented by the modules can be found in Table 9.

Algorithm	Use
MD5	Hashing Algorithm
SHA-1	Signature Generation (non-compliant)
Triple-DES	Encryption/Decryption (non-compliant)

Table 9 - Non-Approved Algorithm Implementations

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.7.2 Key Management Overview

Key or CSP	Usage	Storage	Storage Method	Input	Output	Zeroization	Access
AES-CBC SSH Session Encryption Key (128/192/256 bit)	Used by SSH for session encryption.	RAM	Plaintext	None	None	Power-Off/Termination of SSH Session	CO: Z User: RWZ
AES-CBC TLS Session Encryption Key (128/192/256 bit)	Used to encrypt traffic in TLS (bulk encryption algorithm)	RAM	Plaintext	None	None	Power-Off / Termination of TLS Session	CO: Z User: RWZ
AES-GCM TLS Session Encryption Key[4] (128/256 bit)	Used to encrypt traffic in TLS (bulk encryption algorithm)	RAM	Plaintext	None	None	Power-Off / Termination of TLS Session	CO: Z User: RWZ
DRBG Entropy	Key Generation	RAM	Plaintext	None	None	Power-Off	CO: Z User: RWZ
DRBG "Key" Value	Key Generation	RAM	Plaintext	None	None	Power-Off	CO: Z User: RWZ
DRBG Seed	Key Generation	RAM	Plaintext	None	None	Power-Off	CO: Z User: RWZ
DRBG "V" Value	Key Generation	RAM	Plaintext	None	None	Power-Off	CO: Z User: RWZ
Diffie-Hellman Private Key (2048 bits)	Used for TLS and SSH Key Exchange	RAM	Plaintext	None	None	Power-Off / Termination of TLS or SSH Session	CO: Z User: RWZ
Diffie-Hellman Public Key (2048 bits)	Used for TLS and SSH Key Exchange	RAM	Plaintext	None	Output Electronically	Power-Off / Termination of TLS or SSH Session	CO: Z User: RWZ
EC Diffie-Hellman Private Key (P-256, P-384, P-521)	Used for TLS and SSH Key Exchange	RAM	Plaintext	None	None	Power-Off / Termination of TLS or SSH Session	CO: Z User: RWZ
EC Diffie-Hellman Public Key (P-256, P-384, P-521)	Used for TLS and SSH Key Exchange	RAM	Plaintext	None	Output Electronically	Power-Off / Termination of TLS or SSH Session	CO: Z User: RWZ

[4] In the event that module power is lost and restored, the calling application must ensure that any AES-GCM keys used for encryption or decryption are re-distributed.

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Key or CSP	Usage	Storage	Storage Method	Input	Output	Zeroization	Access
ECDSA Public Key (P-256, P-384, P-521)	Used for TLS and SSH for authentication of the handshake.	Flash Memory	Plaintext	None	Output Electronically	Creation of a new ECDSA Key Pair / Issuing the 'delete' command	CO: Z User: RWZ
ECDSA Private Key (P-256, P-384, P-521)	Used for TLS and SSH for authentication of the handshake.	Flash Memory	Plaintext	None	None	Creation of a new ECDSA Key Pair / Issuing the 'delete' command	CO: Z User: RWZ
RSA Public Key (2048 bits)	Used for TLS and SSH for authentication of the handshake.	Flash Memory	Plaintext	None	Output Electronically	Creation of a new RSA Key Pair / Issuing the 'delete' command	CO: Z User: RWZ
RSA Private Key (2048 bits)	Used for TLS and SSH for authentication of the handshake.	Flash Memory	Plaintext	None	None	Creation of a new RSA Key Pair / Issuing the 'delete' command	CO: Z User: RWZ
TLS Pre-master Secret	Shared secret component used in TLS exchange for TLS sessions.	RAM	Plaintext	None	Output Electronically	Power-Off/Termination of TLS Session	CO: Z User: RWZ
TLS Master Secret	Shared secret used in TLS exchange for TLS sessions.	RAM	Plaintext	None	None	Power-Off/Termination of TLS Session	CO: Z User: RWZ
SSH Pre-master Secret	Shared secret component used in SSH exchange for SSH sessions.	RAM	Plaintext	None	Output Electronically	Power-Off/Termination of SSH Session	CO: Z User: RWZ
SSH Master Secret	Shared secret used in SSH exchange for SSH sessions.	RAM	Plaintext	None	None	Power-Off/Termination of SSH Session	CO: Z User: RWZ
TLS Session Message Authentication Key HMAC-SHA1-1/ /HMAC-SHA-256/HMAC-SHA-384/	Used to authenticate TLS traffic.	RAM	Plaintext	None	None	Power-Off/Termination of TLS Session	CO: Z User: RWZ

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Key or CSP	Usage	Storage	Storage Method	Input	Output	Zeroization	Access
SSH Session Message Authentication Key HMAC-SHA1/ HMAC-SHA-1-96/HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512	Used by SSH for data integrity.	RAM	Plaintext	None	None	Power-Off/Termination of SSH Session	CO: Z User: RWZ
SHA-256 FLASH Integrity Test Hash	Used to verify the integrity of the firmware image (as part of the Power-Up Self-Tests)	Flash Memory	Plaintext	None	None	Never zeroized	CO: R User: R
SSH RSA private key (2048 bits)	The RSA private key used for SSH Session authentication (in lieu of a password).	Flash Memory	Plaintext	None	None	Creation of a new RSA Key Pair	CO: Z User: RWZ
SSH RSA Public Key (2048 bits)	The RSA public key used for SSH Session authentication (in lieu of a password).	Flash Memory	Plaintext	None	Output Electronically	Creation of a new RSA Key Pair	CO: Z User: RWZ
Crypto Officer Password	Password (hashed using SHA-256)	Flash Memory	Hashed using SHA-256	Input by operator via console port	None	Deletion of Operator Account	CO: RWZ User: Z
User Password	Password (hashed using SHA-256)	Flash Memory	Hashed using SHA-256	Input by operator via console port	None	Deletion of Operator Account	CO: Z User: RWZ

Table 10 - Cryptographic Keys, Key Components, and CSPs

Access includes Write (W), Read (R), and Zeroize (Z).

The SSH and TLS protocols have not been reviewed or tested by the CAVP or the CMVP.

2.7.3 Key Generation & Input

Keys/CSPs that can be input into the module by the operator include:

- Crypto Officer Password
- User Password

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

All other keys/CSPs are generated using the SP 800-90A DRBGs or derived by the module using the SSH and TLS KDFs.

The module implements SP 800-90A compliant DRBG services for the creation of shared secret components used in the the generation of session keys (symmetric keys) and for the generation of asymmetric Keys (ECDSA and RSA keys) as shown in Tables 6 and 10. The pre-shared secret components used in the shared secret computation are an unmodified output from an Approved DRBG. ECDSA and RSA keys are generated in accordance with FIPS 186-4.

For random number generation the calling application should use entropy sources that meet the security strength required in SP 800-90A. This entropy is supplied by means of callback functions. Those functions must return an error if the minimum entropy strength cannot be met. The modules' Approved SP 800-90 DRBGs are seeded once with entropy input and a nonce provided by the modules' NDRNG at module initialization.

2.7.4 Key Output

The modules output the following keys/CSPs electronically in plaintext form:

- Diffie-Hellman Public Key
- EC Diffie-Hellman Public Key
- ECDSA Public Key
- RSA Public Key
- SSH RSA Public Key
- TLS Pre-master Secret
- SSH Pre-master Secret

2.7.5 Storage

All keys and CSPs are stored in either Flash memory or RAM. The Flash memory is mainly used for persistent storage of the AOS images along with logs and config files. The RAM provides run-time memory to the CPU during the execution of the AOS software.

Persistent keys and CSPs that remain in the module beyond power-off are stored in Flash memory. All session keys and non-persistent keys/CSPs are stored in RAM.

Session keys and non-persistent keys/CSPs that are stored in RAM are associated with a process ID, which is associated with the operator invoking the service that spawned the process ID. Thus, session and non-persistent keys/CSPs are associated with the operator invoking the service.

Persistent keys and CSPs that remain in the modules beyond power-off are stored in Flash memory and have appropriate 'read' and 'write' permissions assigned solely to the operator that created the key/CSP.

2.7.6 Zeroization

All TLS/SSH session related-keys and CSPs (session keys, pre-master secrets, master secrets, EC Diffie-Hellman Key pairs, and Diffie-Hellman Key pairs) are zeroized upon termination of the

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

TLS/SSH session or by powering off the modules. DRBG-related keys and CSPs are stored in RAM and are zeroized upon powering-off the modules. RSA and ECDSA key pairs are stored in Flash memory and can be zeroized only through creation of a new key pair or by issuing a command to zeroize the key pair.

The modules maintain a file called ‘imgsha256sum’ that is located in Flash memory. On start-up, sha-256 hashes of the files that make-up the modules’ firmware are computed and compared to the hashes stored in the ‘imgsha256sum’ file. If they match, then the intregrity test succeeds; otherwise, the modules’ enter the Error state. The ‘imgsha256sum’ file is not zeroized.

In addition, the Crypto-Officer and User passwords are only zeroized upon deletion of an operator’s account.

2.8 Electromagnetic Interference / Electromagnetic Compatibility

The OmniSwitch AOS 8.3.1.R01 series of Cryptographic Modules have been tested and conform to the FCC EMI/EMC requirements in 47 Code of Federal Regulation, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A.

2.9 Self Tests

2.9.1 Power Up Self Tests

The modules perform the following tests automatically upon power up:

Algorithm	Type	Description
AES	KAT[5]	Encryption and decryption are tested separately, CBC mode, 128 bit length
AES GCM	KAT	Encryption and decryption are tested separately, 256 bit key length
CVL	KAT	SP 800-135 TLS 1.0/1.1,TLS 1.2, and SSH
CTR-based DRBG	KAT	AES, 256 bit with and without derivation function
Hash-based DRBG	KAT	SHA-256
HMAC-based DRBG	KAT	HMAC-SHA-256
SHS[6]	KAT	SHA-1, SHA-256, SHA-384, SHA-512
HMAC	KAT	HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512
ECDSA	PCT[7]	Keygen, sign and verify using P-224 and K-233 with SHA512.
Module Integrity	KAT	SHA-256
RSA	KAT	Signature generation and verification are tested separately using 2048 bit key, SHA-256, PKCS#1

Table 11 - Power-On Self-Tests

Power-on self tests return 1 if all self tests succeed, and 0 if not. If a self-test fails, the modules enter the error state and all data output is inhibited. During self-tests, cryptographic functions

[5] KAT: Known Answer Test
[6] SHA KATs are tested as part of HMAC KATs
[7] PCT: Pairwise Consistency Test

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

cannot be performed until the tests are complete. If a self-test fails, subsequent invocation of any cryptographic function calls will fail. The only way to recover from a self-test failure is by power-cycling the modules.

2.9.2 Conditional Self Tests

The modules performs the following conditional self tests:

Algorithm	Modes and Key Sizes

DRBG	• Continuous Random Number Generation Test
	• SP 800-90A DRBG Health Tests
	  ○ Instantiate
	  ○ Reseed
	  ○ Generate
	  ○ Uninstantiate

NDRNG	Continuous Random Number Generation Test
ECDSA	Pairwise consistency test for Sign/Verify
RSA	Pairwise consistency test for both Sign/Verify and Encrypt/Decrypt

Table 12 - Conditional Self-Tests

In the event of a DRBG self-test failure the calling application must uninstantiate and re-instantiate the DRBG per SP 800-90A requirements.

2.10 Design Assurance

Configuration management for the modules are provided by Agile, and Perforce for software. Each configuration item along with major and minor versions are identified through these tools.

Documentation version control is performed manually by updating the document date as well as the major and minor version numbers in order to uniquely identify each version of a document.

2.11 Mitigation of Other Attacks

The modules do not claim to mitigate any attacks outside the requirements of FIPS 140-2.

 © ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

3 Secure Operation

The AOS Cryptographic Modules meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in the FIPS-Approved mode of operation.

When the "aaa common-criteria admin-state enable" command is entered on the modules, FIPS 140-2 compliant encryption is used by the OmniSwitch devices in the various management interfaces such as SSH and TLS.

These strong cryptographic algorithms ensure secure communication with the device to provide interoperability, high quality, cryptographically-based security for IP networks through the use of appropriate security protocols, cryptographic algorithms, and keys and prevent any form of hijacking/hacking or attack on the device through the secure mode of communication.

When configured according to the instructions below in section 3.1 and 3.2 the module does not support a non-FIPS mode of operation.

3.1 Initialization and Configuration

The following procedure is used to configure the FIPS mode on the switch:

1. Enable the FIPS/Common-Criteria mode on an OmniSwitch using the following command:
```
-> aaa common-criteria admin-state enable
WARNING: Common Criteria configuration is applied only after reload.
```

2. **Confirm that the FIPS/Common-Critiera mode configuration has been enabled for the Admin state. Write the changes to the boot configuration**
```
-> show aaa common-criteria config
Admin State: Enabled,
Operational State: Disabled
-> write memory
```

3. Reboot the system, an reconfirmation message is displayed. Type "Y" to confirm reload.
```
-> reload from working no rollback-timeout
-> Confirm Activate (Y/N) : y
```

4. Use the **show aaa common-criteria config** to view the configured and running status of the FIPS mode on the modules.
```
-> show aaa common-criteria config
Admin State: Enabled
Oper State: Enabled
```

5. To finalize configuration of the modules in the Approved mode of operation, the IPsec protocol management interface shall be manually disabled after FIPS mode is enabled to achieve a complete secure device.

   Disabling the IPsec management interface can be achieved by issuing the following commands to the modules:
```
-> no ipsec policy
-> no ipsec sa
```


© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Note: When configured in the Approved mode of operation, the modules have disabled the use of the FTP, Telnet, SNMP, and HTTP/HTTPS (the web-based interface used for switch management) protocols.

3.2 Crypto Officer Guidance

The Crypto-Officer (CO) is responsible for initializing and configuring the module into the FIPS-Approved mode of operation. Prior to following the guidance in the section “Initialization and configuration”, the CO is responsible for the completing the following prerequisites:

• The SSH/TLS clients should support the secure FIPS standard cryptographic algorithms to communicate with an OmniSwitch device on FIPS mode.

• User-specific certificates/ keys have to be generated using FIPS compliant cryptographic algorithms. There are no checks to verify the FIPS compliance of the certificate/keys in the flash.

• When takeover happens, management sessions with the old Primary will be disconnected. Users will have to reconnect to the new Primary.

• In order to operate in the Approved Mode of Operation, tamper evident seals shall be applied to the modules as indicated in Section 2.5 “Physical Security”.

Additional information and guidance is available in the “OmniSwitch AOS Release 8 Switch Management Guide”.

3.2.1 Receipt of the Module

During deliver of a module, it is packaged in ESD (Electro-Static Discharge) bags and sealed with an ESD warning label. It is then boxed in the factory using sealing tape written with "Alcatel Lucent Enterprise". If the box is opened during transit, the tape seal will break or show signs of tamper.

A tracking number is generated when the package is shipped, which allows Alcatel-Lucent Entreprise to track the shipment to the authorized operator. When the authorized operator receives the module, they must sign for the package.

3.3 User Guidance

The User role is assumed by non-CO operators.

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AOS	Alcatel-Lucent Operating System
CA	Certificate Authority
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
EFP	Environmental Failure Protection
EMI/EMC	Electromagnetic Interference / Electromagnetic Compatibility
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
HMAC	(Keyed-) Hash Message Authentication Code
KAS	Key Agreement Scheme
KAT	Known Answer Test
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
NDRNG	Non-Deterministic Random Number Generator
NVM	Non-Volatile Memory
PoE	Power Over Ethernet
QVGA	Quarter Video Graphics Array
ROM	Read Only Memory
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
Triple-DES	Triple Data Encryption Standard
USB	Universal Serial Bus

Table 13 - Acronym Definitions

© ALE USA, Inc., 2018
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.