FIPS 140-2 Non-Proprietary Security Policy
for
Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 Cryptographic Module




Module Version No: 8.3.1.R01
FIPS Security Level: 1
Document Version: 1.0
Date: May 9, 2017

Prepared For:

ALE USA Inc.
26801 West Agoura Road
Calabasas, CA
USA 91301
www.enterprise.alcatel-lucent.com

Prepared By:

EWA-Canada, Ltd.
1223 Michael Street, Suite 200
Ottawa, Ontario
Canada K1J 7T2
www.ewa-canada.com

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 Cryptographic Module Cryptographic Module by Alcatel-Lucent Enterprise describes how the module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode of operation.

This document was prepared as part of the Level 1 FIPS 140-2 validation of the module. The following table lists the module's FIPS 140-2 security level for each section.

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1
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 Communications Security Establishment Canada (CSE) 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 Altacel Lucent Enterprise website:

http://enterprise.alcatel-lucent.com/

1.3 Document Organization

This non-proprietary Security Policy is part of the Alcatel-Lucent Enterprise OmniSwitch AOS 8.3.1.R01 Cryptographic Module 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 Cryptographic Module is also referred to in this document as the AOS Cryptographic Module, cryptographic module, or the module.

1.4 Module Platforms

The module has been tested on the following hardware platforms:

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
9900	9900

Table 2 - FIPS 140-2 Tested Platforms

1.5 Platform Series Overview

1.5.1 OmniSwitch 6860

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.

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.

1.5.4 OmniSwitch 9900

The Alcatel-Lucent OmniSwitch® 9900 series Modular LAN chassis platform is a high-capacity, high-performance modular Ethernet LAN switch that is field-proven in enterprise, service provider and data center environments. As the OmniSwitch 9900 series runs on the Alcatel- Lucent Operating System (AOS), a state-of-the-art programmable operating system designed for Software-Defined Networking (SDN), it delivers uninterrupted network uptime with non-stop Layer-2 and Layer-3 forwarding.

The OmniSwitch 9900 is a high density, multi Terabit modular platform. The platform can linearly scale switching capacity with virtual chassis technology providing tens of Terabit of aggregate switching capacity. In particular its modular design provides investment protection allowing for scaling out in the future with inline upgrades offering high density 25G/40G/50G/100G interfaces.

The OmniSwitch 9900 series is ideally suited for enterprise core, aggregation and edge environments. Its resilient platform architecture providing control plane and data plane redundancy together with unparalleled scalability helps meet demanding resiliency and throughput requirements for evolving enterprises of all sizes.

The OmniSwitch 9900 series offers a broad range of modules supporting 1 GigE, 10 GigE and 40 GigE ports in an 11-RU chassis form factor, and it offers highest 1 GigE/10GigE port density in its class. The platform is also ready to support 100 GigE.

The OmniSwitch 9900 offers the highest density of Power over Ethernet (PoE) in its class, scaling up to 10080 W of inline PoE power. The gigabit PoE line card supports 8 ports of HPoE (75 W) and 40 ports of 802.3at PoE (30 W). All PoE-enabled ports are IEEE 802.3af/at compliant. The OmniSwitch 9900 leverages an energy-efficient model with leading low power consumption, making it an efficient and versatile switch.

The Alcatel-Lucent Enterprise Intelligent Fabric technology is also enabled on the OmniSwitch 9900 Modular LAN chassis. The technology brings true network flexibility ensuring business agility. It not only delivers a resilient, high-capacity infrastructure, but it also delivers automated deployment and self-healing network capabilities to reduce overhead in IT operations. The technology platform is built upon standard IEEE protocols and key innovations such as Shortest Path Bridging (802.1aq/SPB-M) for bridged and routed services, Multiple VLAN Registration Protocol (MVRP), dynamic Virtual Network Profiles (vNP), 802.3ad/802.1AX (LACP) and Auto-Fabric for automatic protocol and topology discovery.

2 Module Overview

The OmniSwitch AOS 8.3.1.R01 Cryptographic Module is a software module which provides cryptographic functionality to Alcatel-Lucent software applications present on the Alcatel-Lucent OmniSwitch series of routers. For the purposes of FIPS 140-2, the module is classified as a software module with a multi-chip standalone embodiment.

2.1 Cryptographic Module Specification

The physical boundary of the module is the OmniSwitch chassis enclosure on which the module is running. The logical cryptographic boundary contains the AOS Cryptographic Module which provides cryptographic functionality for calling applications, and is denoted in the below figure by a dashed line. The physical and logical boundaries is depicted in the figure below.

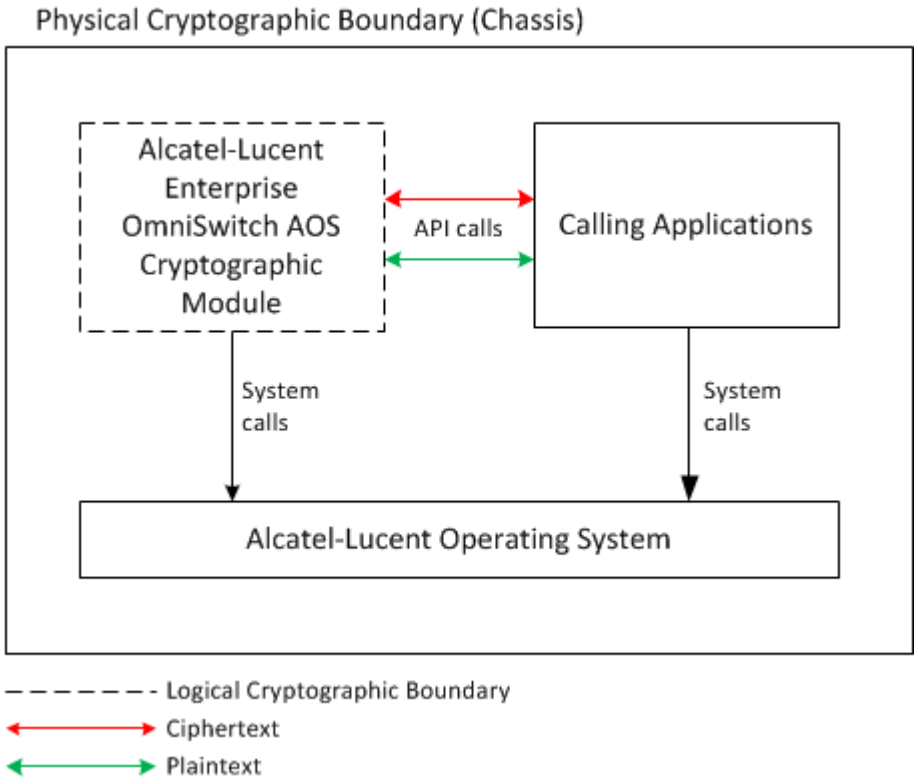

Figure 1 - Block Diagram

2.2 Cryptographic Module Ports and Interfaces

The module's physical ports and interfaces are those of the hardware on which the module is operating. For the OmniSwitch series of routers, the physical ports and interfaces would be as follows:

- Ethernet, RJ-45, USB, SFP, SFP+, QSFP+
- LEDs
- Power supplies

Being a software module, the logical interfaces are defined by API function calls and their associated input and output parameters (including return codes). Table 3 below shows how OmniSwitch physical ports and interface map to the logical interfaces of the module as defined in FIPS 140-2:

FIPS 140-2 Interface	Physical Interface	Module Interface
Data Input	Ethernet, SFP, SFP+, QSFP+	API Input Parameters
Data Output	Ethernet, SFP, SFP+, QSFP+	API Output Parameters
Control Input	USB, RJ-45, Ethernet, SFP, SFP+, QSFP+	API Function Calls
Status Output	USB, RJ-45, Ethernet, SFP, SFP+, QSFP+, LEDs	API Output Parameters and Return Codes
Power Input	Hardware Power Connector, Ethernet (PoE)	N/A

Table 3 - Module Interface Mappings

2.3 Roles & Services

2.3.1 Roles

The module has two operator roles: Crypto Officer and User. The roles are assumed implicitly upon the invocation of the module services. The Crypto Officer is an administrative role that initializes the module and uses cryptographic services provided by the module, while the Users are the calling applications that utilize the cryptographic functions.

The module does not support concurrent operators.

2.3.2 Services

Table 4 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 API call to perform the service, and Write means the CSP is generated, modified or deleted by the API call.

Service	Operator	Description	Input	Output	Key/CSP	CSP Access
Encryption	User	Encrypts plaintext data	Plaintext data, Initialization vector, Key	Encrypted data	AES-CBC Key, Triple-DES-CBC Key	Execute
Decryption	User	Decrypts encrypted data	Encrypted data, Initialization vector, Key	Plaintext data	AES-CBC Key, Triple-DES-CBC Key	Execute
Generate Random Number	User	Generates random bits	Seed value	Random bits	DRBG Entropy, DRBG Seed	Read/Execute
Generate Symmetric Key	User	Generate symmetric key	Key size	Key	AES-ECB Key, AES-CBC Key, AES-GCM Key, Triple-DES-CBC Key, TLS Session Encryption Key, SSH Session Key	Execute/Write
Generate Asymmetric Key	User	Generates asymmetric key pair	Key size	Asymmetric key pair	EC Diffie-Hellman Private Key, EC Diffie-Hellman Public Key, ECDSA Public Key, ECDSA Private Key, RSA Public Key, RSA Private Key, SSH RSA private key	Read/Write/Execute
Hash	User	Calculates a hash using SHA	Plaintext data	Hashed data	N/A	N/A
Keyed Hash	User	Calculates a hash using HMAC-SHA	HMAC key and Plaintext data	Hashed data	HMAC key	Read/Write/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 on behalf of calling process. Not used to establish keys into the module	EC DH public key and private Key	EC DH agreement key	EC Diffie-Hellman Private Key, EC Diffie-Hellman Public Key	Read/Write/Execute

Service	Operator	Description	Input	Output	Key/CSP	CSP Access
Key Transport	User	Encrypt or Decrypt a key value on behalf of the calling process	Encrypt: key value, RSA Key Transport Key Decrypt: Encrypted Key value, RSA Key Transport Key	Encrypt: Encrypted key value Decrypt: key value	RSA Public Key, RSA Private Key	Read/Write/Execute
Self-Test	User/Crypto Officer	Performs self-tests	N/A	Pass or fail return code	N/A	Execute/Read
Show Status	User/ Crypto Officer	Displays module status and version	N/A	Module status	N/A	Execute
Signature Sign	User	Generates a digital signature	Signing key; plaintext	Digital signature	ECDSA Public Key, ECDSA Private Key, RSA Public Key, RSA Private Key	Execute
Signature Verify	User	Verifies a digital signature	Digital signature; Public Key,	Result of verification	ECDSA Public Key, ECDSA Private Key, RSA Public Key, RSA Private Key	Execute
Zeroize	User/Crypto Officer	Zeroize CSPs	N/A	N/A	All except Integrity key	Write

Table 4 - Services

2.4 Authentication Mechanisms

The module does not support authentication.

2.5 Physical Security

The module is a software module and does not implement any physical security.

2.6 Operational Environment

The AOS Cryptographic Module was tested on the following OmniSwitch platforms:

Series	Model	OS & Version
6860	6860-24 6860-P24 6860-48 6860-P48 6860E-24 6860E-P24 6860E-48 6860E-P48 6860E-U28	Alcatel-Lucent Operating System (AOS) 8.3.1.R01
6865	6865-P16X	
6900	6900-X20 6900-X40 6900-T20 6900-T40 6900-Q32 6900-X72	
9900	9900	

Table 5 - Operational Environments

The AOS cryptographic module is invoked and functions entirely within the logical process space of the calling application. The tested operating systems segregates user processes into separate process spaces.

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 6.

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or	Use
#4285 #4286 #4287 #4288	AES	FIPS 197, SP800-38A	CBC	128/192/256 bits	Data Encryption and Decryption
#4440 #4441 #4443 #4444	AES	FIPS 197, SP800-38A	ECB	128/256 bits	Data Encryption and Decryption
#4440 #4441 #4443 #4444	AES	SP800-38D	GCM	128/256 bits	Data Encryption and Decryption
#1184 #1185 #1186 #1187	CVL TLS 1.0/1.1, TLS 1.2, SSH	SP 800-135	-	-	Key Derivation
#1345 #1346 #1347 #1348	DRBG	SP800-90A	Hash_DRBG HMAC_DRBG CTR_DRBG	-	Deterministic Random Bit Generation
#1078 #1079 #1081 #1082	ECDSA	FIPS 186-4	PKG, SigGen, SigVer	P-256 P-384 P-521	Digital Signature Generation and Verification
#2821 #2822 #2823 #2824	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-1-96[1] HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	512/1024 bits	Message Authentication
#2306 #2307 #2308 #2309	RSA	FIPS 186-4	-	2048 bits	Key Generation

[1] 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.

#2306 #2307 #2308 #2309	RSA	FIPS 186-4	SHA-1 SHA-256 SHA-384 SHA-512 (ANSI X9.31, PKCS1 v1.5, SSA-PSS)	2048 bits	Digital Signature Generation and Verification
#3523 #3524 #3525 #3526	SHS	FIPS 180-4	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	-	Message Digest
#2386 #2387 #2388 #2389	Triple-DES	FIPS 46-3, SP 800-67	TCBC	192 bits	Data Encryption and Decryption

Table 6 - 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 7.

Algorithm	Caveat	Use
Diffie-Hellman	Provides 112 bits of encryption strength.	Key establishment
EC Diffie-Hellman Suport 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.[2]

Table 7 - Non-Approved but Allowed Algorithm Implementations

[2] The estimated amount of entropy provided by the NDRNG is 0.99 per 1 bit of data.

2.7.1.3 Non-Approved Algorithms

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

Algorithm	Use
MD5	Hashing Algorithm
SHA-1	Signature Generation

Table 8 - Non-Approved Algorithm Implementations

2.7.2 Key Management Overview

Key or CSP	Usage	Storage	Storage Method	Input	Output	Zeroization	Access
AES-CBC Key (128/192/256 bit)	TLSv1.1, TLSv1.2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
AES-CBC Key (128/192/256 bit)	IPsec	RAM	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
AES-ECB Key (128/256 bit)	TLSv1.1, TLSv1.2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
AES-GCM Key[3] (128/256 bit)	TLSv1.1, TLSv1.2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
DRBG Entropy	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
DRBG "Key" Value	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
DRBG Seed	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
DRBG "V" Value	Key Generation	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
EC Diffie-Hellman Private Key	EC DH (All NIST defined B, K and P curves) private key agreement key	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
EC Diffie-Hellman Public Key	EC DH (All NIST defined B, K and P curves) public key agreement key	Flash Memory	Plaintext	None	None	Power-Off / API Command	CO: Z User: RWZ
ECDSA Public Key	TLSv1.1, TLSv1.2, SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
ECDSA Private Key	TLSv1.1, TLSv1.2, SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ

[3] 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.

Key or CSP	Usage	Storage	Storage Method	Input	Output	Zeroization	Access
HMAC-SHA-1 Integrity Key	Module Integrity	Module Binary	Plaintext	None	None	None	CO: R User: R
HMAC-SHA-1	SSHv2, MAC-based end-user and device authentication	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-1-96	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-224	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-256	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-384	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
HMAC-SHA-512	SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
RSA Public Key	TLSv1.1, TLSv1.2, SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
RSA Private Key	TLSv1.1, TLSv1.2, SSHv2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ
IPSec session Authentication Key	Exchanged using the IPsec protocol. Used to authenticate IPSec traffic.	RAM	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
IPSec Session Encryption Key	Exchanged using the IPsec protocol. Used to encrypt IPSec traffic.	RAM	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
TLS Pre-master Secret	Shared secret used in TLS exchange for TLS sessions.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
TLS Master Secret	Shared secret used in TLS exchange for TLS sessions.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ

Key or CSP	Usage	Storage	Storage Method	Input	Output	Zeroization	Access
TLS Session Authentication Key	Used to authenticate TLS traffic.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
TLS Session Encrypton Key	Used to encrypt TLS traffic.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
SSH Session Authentication Key	Used by SSH for data integrity.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
SSH Session Key	Used by SSH for session encryption.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
SSH RSA private key	The RSA private key used for SSH authentication.	Flash Memory	Plaintext	API call parameter	None	Power-Off API Command Terminate Session	CO: Z User: RWZ
Triple-DES-CBC Key (192 bit)	TLSv1.1, TLSv1.2	Flash Memory	Plaintext	API call parameter	None	Power-Off / API Command	CO: Z User: RWZ

Table 9 - Cryptographic Keys, Key Components, and CSPs

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

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

2.7.3 Key Generation & Input

The module implements SP 800-90A compliant DRBG services for creation of symmetric keys, and for generation of ECDSA and RSA keys as shown in Tables 5 and 8. Resulting symmetric keys are an unmodified output from an Approved DRBG.

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. CSPs are passed to the module in plaintext as API parameters. Private and secret keys as well as seed and entropy are also provided to the module by the calling application.

2.7.4 Key Output

The module does not output CSPs, other than the explicit results of key generation requests.

2.7.5 Storage

Keys are provided to the module by the calling process and are destroyed when released by the appropriate API function call or during a power cycle. The module does not perform the persistent storage of keys or CSPs. Generated data will always be associated with the relevant calling process. The module code ensures that no data can be associated with calling daemons beyond the relevant caller. The implementation of the zeroization process leaves no traces of data left for successive calls of the same or other services.

2.7.6 Zeroization

Zeroization of sensitive data is performed automatically by an API function call for temporarily stored CSPs. There are also functions provided to explicitly destroy CSPs related to random number generation services.The calling application is responsible for parameters passed in and out of the module. Private and secret keys as well as seed and entropy are destroyed when the API function calls return. No key information is output through the data output interface when the module zeroizes keys.

2.8 Electromagnetic Interference / Electromagnetic Compatibility

The AOS Cryptographic Module runs on the OmniSwitch series of routers that 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 module performs the following tests automatically upon power up:

Algorithm	Type	Description
AES	KAT[4]	Encryption and decryption are tested separately, ECB 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[5]	KAT	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
HMAC	KAT	HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512

[4] KAT: Known Answer Test
[5] SHA KATs are tested as part of HMAC KATs

ECDSA	PCT[6]	Keygen, sign and verify using P-224, K-233 and SHA512.
Module Integrity	KAT	HMAC-SHA1
RSA	KAT	Signature generation and verification are tested separately using 2048 bit key, SHA-256, PKCS#1
Triple-DES	KAT	Encryption and decryption are tested separately, CBC mode, 192 bit length

Table 10 - 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 module enters an error state and all data output is inhibited. During self-tests, cryptographic functions 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 reloading the module.

2.9.2 Conditional Self Tests

The module performs the following conditional self tests:

Algorithm	Modes and Key Sizes

DRBG	• Continuous Random Number Generation Test
	• SP 800-90B 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 11 - 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 module is 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 module does not claim to mitigate any attacks outside the requirements of FIPS 140-2.

[6] PCT: Pairwise Consistency Test

3 Secure Operation

The AOS Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in FIPS-Approved mode of operation.

When the FIPS enable command is entered on OmniSwitch, FIPS 140-2 compliant encryption is used by the OmniSwitch devices in the various management interfaces such as SFTP, HTTPS, SSH and SSL.

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 mode on an OmniSwitch using the following command:
```
-> system fips admin-state enable
WARNING: FIPS Admin State only becomes Operational after write
memory and reload
```

2. **Write the changes to the boot configuration**
```
-> 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 system fips** to view the configured and running status of the FIPS mode on the Switch.
```
-> show system fips
Admin State: Enabled
Oper State: Enabled
```

5. Disable insecure management interfaces such as Telnet/ FTP/SNMP[7] manually after FIPS mode is enabled to achieve a complete secure device.

   Disabling management interfaces can be performed by invoking the command:
   no aaa authentication [console | telnet | ftp | http | snmp | ssh | default]

[7] The SNMP KDF has not been validated by the CAVP. Per IG D.11, the SNMP KDF shall not be used in the Approved Mode of Operation. Furthermore, keys that are generated by the SNMP KDF in the Non-Approved mode of Operation are not permitted for use in the Approved Mode of Operation.

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/SFTP/SSL 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 in the OpenSSL module to verify the FIPS compliance of the certificate/keys in the flash.

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

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

3.3 User Guidance

The User role is assumed by non-CO operators, calling applications, or the OS. The following requirement is imposed on the User role needed to operate the module securely in accordance with Implementation Guidance A.13:

- Per SP800-67 rev1, the user is responsible for ensuring the module’s limit to 2^{32} encryptions with the same Triple-DES key while being used in the TLS protocol.

4 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AOS	Alcatel-Lucent Operating System
CA	Certificate Authority
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSEC	Communications Security Establishment Canada
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 12 - Acronym Definitions