FIPS 140-2 Non-Proprietary Security Policy for

# OmniSwitch AOS Cryptographic Module

Module Software Version No:
8.6.R11 FIPS Security Level: 1

Document P/N: 015882-00

Document Version: 1.3
Date: November 17, 2022

# Table of Contents

# List of Tables

# List of Figures

# 1 Introduction

## 1.1 Purpose

This non-proprietary Security Policy for the OmniSwitch AOS Cryptographic Module by Alcatel- Lucent Enterprise (ALE USA Inc.) 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 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/

## 1.3 Document Organization

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

## 1.4 Module Platforms

The module has been tested on the following hardware platforms:

| Series | OmniSwitch Model | Processor |
|---|---|---|
| OS6465 | 6465-P6<br>6465-P12<br>6465-P28<br>6465T-12<br>6465T-P12 | ARM Cortex-A9 |
| OS6560 | 6560-24X4<br>6560-24Z8<br>6560-24Z24<br>6560-48X4<br>6560-P24X4<br>6560-P24Z8<br>6560-P24Z24<br>6560-P48X4<br>6560-P48Z16<br>6560-PXZ24<br>6560-X10 | ARM Cortex-A9 |
| OS6860 | 6860-24<br>6860-48<br>6860-P24<br>6860-P48<br>6860E-24<br>6860E-48<br>6860E-P24<br>6860E-P24Z8<br>6860E-P48<br>6860E-U28 | ARM Cortex-A9 |
| OS6865 | 6865-P16X<br>6865-U12X<br>6865-U28X | ARM Cortex-A9 |
| OS6900 | 6900-C32<br>6900-V72 | Intel Atom C2538 |
| | 6900-Q32<br>6900-T20<br>6900-T40<br>6900-X72 | NXP QorIQ P2040 |
| | 6900-X20<br>6900-X40 | NXP MPC8572 |
| OS9900 | 9907 | Intel Atom C2518 |

*Table 2 - FIPS 140-2- Tested Platforms*

## 1.5 Platform Series Overview

### 1.5.1 OmniSwitch 6465

OS6465 switches are a family of hardened, compact, fan-less gigabit Ethernet switches that have been designed specifically for industrial applications and OmniSwitch 6465T switches that offer extended temperature and are ideal for residential/metro Ethernet triple play applications. The switches run on the widely deployed and field proven Alcatel-Lucent Operating system that offers high security, reliability, performance, and easy management. The hardened switches are designed to operate in extended temperatures, offer higher EMI/EMC tolerance, a flexible range in power inputs options and high surge protection.

The OS6465 series offers HPoE (60W PoE) providing power to a range of new age devices from PTZ IP cameras on toll booths, LED lights and building management gateways in smart buildings to industrial control systems. These switches are easy to deploy and offer out-of-the-box plug-and-play, Zero-touch provisioning, network automation and disaster recovery options. These switches support IEEE 1588v2 PTP for the nanosecond-level precision timing requirements of industrial devices and applications. With support for MACSec on all ports, OS6465 enables end-to-end encrypted networks. The OS6465 family offers advanced system and network level resiliency features and convergence through standardized protocols in a space efficient form factor.

### 1.5.2 OmniSwitch 6560

The Alcatel-Lucent OmniSwitch™ 6560 Stackable Gigabit and Multi-Gigabit Ethernet LAN value switch family is an industry leading campus access solution for enterprise networks. With multi-gigabit ports for high-speed IEEE 802.11ac devices, 10 GigE uplinks and 20 GigE stacking, the OmniSwitch 6560 is the right solution for your next generation network.

Offering a design optimized for flexibility and scalability as well as low power consumption, the OmniSwitch 6560 is an outstanding edge solution. It uses the field-proven Alcatel-Lucent Operating System (AOS) to deliver highly available, secure, self-protective, easily managed and eco-friendly networks.

The Alcatel-Lucent OmniSwitch 6560 family is embedded with the latest technology innovations and offers maximum investment protection. Deployments benefiting from the OmniSwitch 6560 family are:

□ Edge of small-to-mid-sized networks
□ Branch office enterprise and campus workgroups
□ Residential and commercially managed services applications

### 1.5.3 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 suchas 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

### 1.5.4 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.

### 1.5.5 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.

### 1.5.6 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 and40 GigE ports in an 11-RU chassis form factor, and it offers highest 1 GigE/10GigE port density inits 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 Cryptographic Module version 8.6.R11 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 OmniSwitch AOS Cryptographic Module that provides cryptographic functionality for calling applications and is denoted in the figure below by a dashed line. The physical and logical boundaries are depicted in the figure below.

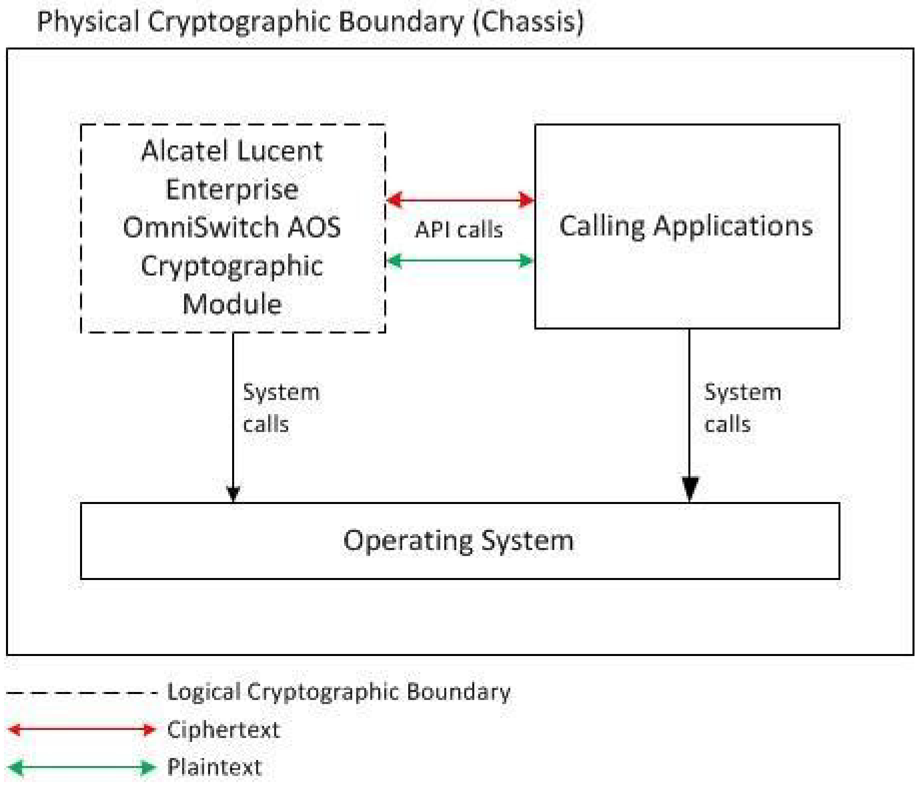
Physical Cryptographic Boundary (Chassis)
Alcatel Lucent Enterprise OmniSwitch AOS Cryptographic Module
API calls
Calling Applications
System calls
System calls
Operating System
Logical Cryptographic Boundary
Ciphertext
Plaintext

*Figure 1 - Block Diagram*

## 2.2 Cryptographic Module Ports and Interfaces

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 | Module Interface |
|---|---|
| Data Input | API Input Parameters |
| Data Output | API Output Parameters |
| Control Input | API Function Calls |
| Status Output | API Output Parameters and Return Codes |
| Power Input | 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 | CSP | CSP Access |
|---|---|---|---|---|
| Encryption | User | Encrypts plaintext data | AES key | Execute |
| Decryption | User | Decrypts encrypted data | AES key | Execute |
| Generate Random Number | User | Generates random bits | DRBG Entropy, DRBG Seed, DRBG State | Read/Execute |
| Generate Symmetric Key | User | Generate symmetric key | AES key | Execute/Write |
| Generate Asymmetric Key | User | Generates asymmetric key pair | RSA, ECDSA keys | Read/Write/Execute |
| Hash | User | Calculates a hash using SHA | N/A | N/A |
| Keyed Hash | User | Calculates a hash using HMAC- SHA | HMAC key | Read/Write/Execute |
| Installation, Uninstallation, and Initialization | Crypto Officer | Install, initialize, configure, uninstall | N/A | N/A |
| Key Agreement | User | Perform key agreement on behalf of calling process. Not used to establish keys into the module | DH and EC DH keys, Shared Secret | Read/Write/Execute |
| Key Derivation | User | Perform key derivation per SSH or TLS | TLS pre-master secret, TLS master secret, Shared Secret | Read/Write/Execute |
| Key Transport | User | Encrypt or Decrypt a key value on behalf of the calling process | RSA keys | Read/Write/Execute |
| Self-Test | User/Crypto Officer | Performs self-tests | N/A | Execute/Read |
| Show Status | User | Displays module status and version | N/A | Execute |
| Signature Sign | User | Generates a digital signature | ECDSA, RSA keys | Execute |
| Signature Verify | User | Verifies a digital signature | ECDSA, RSA keys | Execute |
| Zeroize | User/Crypto Officer | Zeroize CSPs | All except HMAC-SHA-1 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 OmniSwitch AOS Cryptographic Module was tested on the OmniSwitch platforms listed in Table 2 above running on AOS version 8.6.R11.

The OmniSwitch 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. The module does not support a software loading service or capability. The module conforms with IG 6.1, whereby the module is implemented in a client/server architecture to be used on both the client and the server. The cryptographic module will be used to provide cryptographic functions to the client and server applications. The cryptographic module is implemented in a server environment and the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the cryptographic module.

## 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 5.

| CAVP Cert | Algorithm | Standard | Mode/ Method | Key Lengths, Curves | Use |
|---|---|---|---|---|---|
| C1692<br>C1693<br>C1694<br>C1695<br>C1696<br>C1697<br>C1698<br>C1699 | AES | FIPS 197,<br>SP800-38A,<br>SP800-38D | CBC, CTR,<br>GCM[1] | 128/256<br>bits | Data Encryption and Decryption |

[1] The IV shall be generated internally in its entirety randomly using the Approved DRBG that is internal to the module's boundary. The IV length is at least 96-bits in alignment with IG A.5, Scenario 2.

| | | | | | |
|---|---|---|---|---|---|
| VA | CKG | SP800-133 | Section 4, 6.1, and 6.2.2 | - | Cryptographic Key Generation |
| C1692<br>C1693<br>C1694<br>C1695<br>C1696<br>C1697<br>C1698<br>C1699 | CVL TLS 1.0/1.1, TLS 1.2, SSH[2] KDFs | SP 800-135 | - | - | Key Derivation |
| C1692<br>C1693<br>C1694<br>C1695<br>C1696<br>C1697<br>C1698<br>C1699 | DRBG | SP800- 90A | Hash_DRBG, HMAC_DRBG, CTR_DRBG | Hash_DRBG (SHA-1, SHA-256, SHA-384, SHA-512),<br>HMAC_DRBG (SHA-1, SHA-256, SHA-384, SHA-512),<br>CTR_DRBG (AES-256) | Deterministic Random Bit Generation |
| C1692<br>C1693<br>C1694<br>C1695<br>C1696<br>C1697<br>C1698<br>C1699 | ECDSA | FIPS 186-4 | PKG, SigGen, SigVer, KeyVer | P-256<br>P-384<br>P-521 | Digital Signature Generation and Verification, Key Generation and Verification |
| C1692<br>C1693<br>C1694<br>C1695<br>C1696<br>C1697<br>C1698<br>C1699 | HMAC | FIPS 198-1 | HMAC-SHA-1<br>HMAC SHA-1-96[3]<br>HMAC-SHA-256<br>HMAC-SHA-384<br>HMAC-SHA-512 | Minimum 112 bits | Message Authentication. HMAC-SHA-1-96 used in the SSHv2 protocol. The truncated form of an HMAC is approved if the HMAC is truncated to its ‘$\lambda$’ leftmost bits where $\lambda \geq 32$. |

[2] No parts of the TLS or SSH protocol, other than the KDFs, have been tested by the CAVP and CMVP

[3] Conformant to IG A.8

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| A1774 | KAS-ECC-SSC | SP800-56A-rev3 | Ephemeral Unified | P-224, P-256, P-384, P-521 | Key Agreement |
|  | KAS-FFC-SSC | SP800-56A-rev3 | DH Ephemeral | DPG: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 | Key Agreement, Safe Primes Key Generation, Safe Primes Key Verification |
| C1692<br>C1693<br>C1694<br>C1695<br>C1696<br>C1697<br>C1698<br>C1699 | RSA | FIPS 186-4 | - | 2048/3072 bits | Key Generation |
| C1692<br>C1693<br>C1694<br>C1695<br>C1696<br>C1697<br>C1698<br>C1699 | RSA | FIPS 186-4 | SHA-1[4]<br>SHA-256<br>SHA-384<br>SHA-512<br>(PKCS1 v1.5,<br>PKCS PSS) | 2048/3072 bits | Digital Signature Generation and Verification |
| C1692<br>C1693<br>C1694<br>C1695<br>C1696<br>C1697<br>C1698<br>C1699 | SHS | FIPS 180-4 | SHA-1 SHA-256 SHA-384 SHA-512 | - | Message Digest |

*Table 5 - FIPS-Approved Algorithm Implementations*

[4] SHA-1 is for Digital Signature Verification Only

#### 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 6.

| Algorithm | Caveat | Use |
|---|---|---|
| MD5 | Allowed per IG 1.23 | Used in the TLS 1.0/1.1 KDF. |
| RSA Key Wrapping | Provides 112 bits of encryption strength. | Non-SP800-56B conformant using the PKCS#1-v1.5 padding scheme and 2048-bit keys. Allowed until December 31, 2023 per IG D.9. |

*Table 6 - Non-Approved but Allowed Algorithm Implementations*

#### 2.7.1.3 Non-Approved Algorithms

A list of non-Approved algorithms implemented by the module can be found in Table 7.
These algorithms are never to be used in the Approved mode of operation. Invoking any of the algorithms specified in Table 7 will result in a non-Approved configuration.

| Algorithm | Use |
|---|---|
| AES 128/192/256 CFB, ECB, OFB, CFB 1, CFB 8, CFB 128, CCM, XTS | Data encryption and decryption |
| AES 192 CBC, CTR, GCM | Data encryption and decryption |
| Blowfish | Data encryption and decryption |
| Camellia | Data encryption and decryption |
| CAST | Data encryption and decryption |
| CMAC (AES and TDES) | Message Authentication |
| DES | Data encryption and decryption |
| DSA | Digital signature |
| Dual EC DRBG | Random Number Generation |
| ECDSA (P-224, B-curves, K-curves, and FIPS186-2 functions) | Digital signature |
| HMAC-SHA-224 | Message authentication |
| IDEA | Data encryption and decryption |
| MD5 | Hashing Algorithm |
| RC2 | Hashing Algorithm |
| RC4 | Hashing Algorithm |
| RIPEMD160 | Hashing Algorithm |
| RSA (1024-bit, greater than 3072-bit, and FIPS 186-2 functions) | Digital signature |

| | |
|---|---|
| SEED | Data encryption and decryption |
| SHA-1 | Signature Generation |
| SHA-224 | Hashing Algorithm |
| Triple-DES | Data encryption and decryption |
| Whirlpool | Hashing Algorithm |
| X9.31 RNG | Pseudorandom Number Generation |

*Table 7 - Non-Approved Algorithm Implementations*

### 2.7.2 Key Management Overview

| Key or CSP | Usage | Storage | Storage Method | Input | Output | Zeroization | Access |
|---|---|---|---|---|---|---|---|
| AES Key | 128/256-bit CTR, CBC, or GCM Key<br>Encrypt/Decrypt | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| DRBG Entropy | Key Generation | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| DRBG Seed | Key Generation | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| DRBG State | V, C, and/or Key depending on the DRBG<br>Key Generation | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| Diffie-Hellman Private Key | Key agreement | RAM | Plaintext | None | None | Power-Off/ API Command | CO: Z<br>User: RWZ |
| Diffie-Hellman Public Key | Key agreement | RAM | Plaintext | None | None | Power-Off/ API Command | CO: Z<br>User: RWZ |
| EC Diffie-Hellman Private Key | EC DH (All NIST defined P curves) private key agreement key | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User:RWZ |
| EC Diffie-Hellman Public Key | EC DH (All NIST defined P curves) public key agreement key | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| ECDSA Public Key | Digital Signature Verification | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| ECDSA Private Key | Digital Signature Generation | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| HMAC-SHA-1 Integrity Key | Module Integrity | Module Binary | Plaintext | None | None | None | CO: R<br>User: R |

| Key or CSP | Usage | Storage | Storage Method | Input | Output | Zeroization | Access |
|---|---|---|---|---|---|---|---|
| HMAC-Key | Message Integrity | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| RSA Public Key | Digital Signature Verification | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| RSA Private Key | Digital Signature Generation | RAM | Plaintext | None | None | Power-Off / API Command | CO: Z<br>User: RWZ |
| TLS pre-master secret | Shared secret used in TLS exchange for TLS sessions. | RAM | Plaintext | None | None | Power-Off<br>API Command<br>Terminate Session | CO: Z<br>User: RWZ |
| TLS master secret | Shared secret used in TLS exchange for TLS sessions. | RAM | Plaintext | None | None | Power-Off<br>API Command<br>Terminate Session | CO: Z<br>User: RWZ |
| Shared Secret | Shared secret calculated from KAS-SSC (ECC or FFC) | RAM | Plaintext | None | None | Power-Off<br>API Command<br>Terminate Session | CO: Z<br>User: RWZ |

*Table 8 - Cryptographic Keys and CSPs*

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

### 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.

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 a named pipe. 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.

While using ECDH algorithm, the calling application should validate the domain parameters and security strength of the elliptic curve before EC key generation to ensure that the selected elliptic curve meets the security requirements of the application.

### 2.7.4 Key Output

The module does not output CSPs.

### 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 control 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 OmniSwitch 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 implements numerous self-tests, but only those associated with a conformance claim for FIPS 140-2 are listed below. The module performs the following tests automatically upon power up:

| Algorithm | Type | Description |
|---|---|---|
| AES GCM | KAT | Encryption and decryption are tested separately, 256-bit key length |
| DRBG (CTR_DRBG) | KAT | AES, 256-bit with and without derivation function |
| DRBG (Hash_DRBG) | KAT | SHA-256 |
| DRBG (HMAC_DRBG) | KAT | HMAC-SHA-256 |
| ECDSA | PCT | Keygen, sign and verify using P-256 |
| HMAC | KAT | HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512 |
| KAS_FFC_SSC | KAT | Shared Secret Calculation using 2048-bit keys. |
| KAS_ECC_SSC | KAT | Shared Secret Calculation using P-256 |
| KDF | KAT | SP 800-135 TLS 1.0/1.1, TLS 1.2, and SSH |
| RSA | KAT | Signature generation and verification are tested separately using 2048 bit key, SHA-256, PKCS#1<br>This test also satisfies the KAT requirements for RSA Key Wrapping per IG D.9 |
| SHS[3] | KAT | SHA-1 SHA-512 |
| Module Integrity | KAT | HMAC-SHA1 |

*Table 9 - Power-On Self-Tests*

[3] SHA-2 KATs are tested as part of HMAC KATs

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<br>□ SP 800-90A DRBG Health Tests<br>o Instantiate<br>o Reseed<br>o Generate<br>o Uninstantiate |
| ECDSA | Pairwise consistency test for Sign/Verify |
| KAS | Public Key Validation Tests |
| RSA | Pairwise consistency test for both Sign/Verify and Encrypt/Decrypt |

*Table 10 - 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.

# 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 module 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, HTTP, 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. This prevents any form of hijacking/hacking or attack on the device through the secure mode of communication.

When configured according to the instructions below in Sections 3.1 and 3.2, the module will operate in the Approved 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 (Note: This will effectively invoke “fips mode set = 1” on the module itself:

```
-> 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, a confirmation message is displayed. Type “Y” to confirm reload.

```
-> reload from working no rollback-timeout
-> Confirm Activate (Y/N): y
```

**4.** Use “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.** Do not employ any algorithms from Table 7.

**6.** The AES-GCM IV must be generated internally in its entirety randomly using the Approved DRBG that is internal to the module’s boundary.

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

The following procedure must be performed whenever exiting the FIPS mode on the switch:

1. Power cycle the device to zeroize all secrets.

## 3.2 Crypto Officer Guidance

The Crypto-Officer (CO) is responsible for initializing and configuring the module into the FIPS- Approved mode of operation per the instructions provided in “Initialization and Configuration.”

## 3.3 User Guidance

The User role is assumed by non-CO operators, calling applications, or the OS. There are no requirements imposed on the User role that are needed to operate the module securely.

# 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 |
| VA | Vendor Affirmed |

*Table 11 – Acronyms and Definitions*