Ärendetyp: 6 Diarienummer: 19FMV6202-28:1

Certification ID CSEC2019023

CSEC

Swedish Certification Body for IT Security

Certification Report - Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.4.R11

Issue: 1.0, 2021-Feb-17

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a network switch comprised of hardware and firmware. The TOE provides Layer-2 switching, Layer-3 routing, and traffic filtering.

The TOE is Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.4.R11.

The following measures that are applied by the developer to maintain security during TOE delivery:

- The TOE hardware:
  - The hardware is boxed using sealing tape with "Alcatel Lucent Enterprise" and logo.
  - The hardware is packaged in electrostatic discharge (ESD) bags and sealed with an ESD warning label.
  - The hardware is only delivered by reputable couriers.
- The TOE software/firmware and guidance documentation:
  - The ALE support website (Business Portal) for downloading the TOE software and guidance documentation uses HTTPS (TLS 1.2) for security. Also, the TOE software and guidance downloads include SHA-256 checksums.

No PP claims are being made.

There are seven assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the nine threats and comply with the two organisational security policies (OSPs) in the ST. The assumptions, threats and OSPs are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden. The evaluation was completed on 2021-02-04. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 2 augmented by ALC_FLR.2.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2019023
Name and version of the certified IT product	Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.4.R11
Security Target Identification	Alcatel-Lucent Enterprise OmniSwitch with AOS 8.6.R11 Security Target for EAL2, ALE USA Inc., 2021-02-03, document version 3.2
EAL	EAL 2 + ALC_FLR.2
Sponsor	ALE USA Inc.
Developer	ALE USA Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.24.1
Scheme Notes Release	17.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2021-02-17

3 Security Policy

- Audit
- Administrator Identification and Authentication
- End user and device authentication
- Management of the TOE
- Cryptographic support
- Traffic Mediation
- Protection of the TSF
- Trusted path/channels

3.1 Audit

The TOE generates audit records. The audit records can be displayed on the serial console as they are generated in a scrolling format.

The TOE writes audit records to a text file stored in the systems flash memory for permanent storage. These entries are tagged with the AOS Application ID that created them. The TOE also provides the ability to send the audit records to an external syslog server using a secure channel.

The TOE provides to security administrators the ability to modify the maximum size allowed for the audit files. Once the files are full the oldest entries are overwritten.

3.2 Administrator Identification and Authentication

The TOE requires identification and authentication of administrators of the TOE prior to access any of the management functionality in all possible scenarios, which are as follows:

- TOE administrators accessing (either locally or remotely) the Command Line Interface (CLI) via a serial console or a Secure Shell (SSH) session.
- TOE administrators accessing TOE storage using SFTP via an SSH session.
- A SNMP Management Station accessing the TOE through the SNMP management interface.

The TOE displays to the administrator a configurable banner after the administrator successfully logs onto the TOE (either serial console, SSH, or SFTP). The TOE also provides the ability to lock the administrator after a configurable number of unsuccessful attempts, and terminate the logon session after a configurable period of inactivity.

The TOE provides administrator configurable password settings to enforce password complexity when a password is created or modified.

The TOE provides support for the following Identification and Authentication mechanisms:

- Identification and Authentication made by the TOE using credentials stored in the local file system;
- Identification and Authentication made by the TOE using credentials stored in a Lightweight Directory Access Protocol (LDAP) server, which is part of the operational environment; or
- Identification and Authentication made by an external authentication server, which is part of the operational environment.

The only external authentication server supported by the TOE for administrator authentication in the evaluated configuration is Remote Authentication Dial In User Service (RADIUS).

Communications with RADIUS servers, LDAP servers and SNMP Management stations are protected with the Transport Layer Security (TLS) protocol. Communication with SSH and SFTP clients are protected with the Secure Shell (SSH) protocol.

3.3 End user and device authentication

Authentication of end users or devices is used to dynamically assign network devices to a VLAN domain and enforcing the VLAN and Traffic Filtering policies. Authentication is performed by verifying the credentials of the end user or the device. The TOE supports two types of authentication: Media Access Control (MAC) based authentication (for devices) and IEEE 802.1X authentication (for end users). The sections below describe the supported mechanisms.

3.4 Management of the TOE

The TOE provides a Command-Line Interface (CLI) for security management. TOE administrators connect to the TOE via either a serial console or a remote session using Secure Shell (SSHv2). In either case, administrators are required to identify and authenticate against the TOE before getting access to the CLI.

The TOE provides an SNMPv3 management interface for security management functionality. An SNMP Management Station authenticates to the TOE and can send request commands to get and set configuration information.

The TOE also provides a Flash file system used for storing configuration files/directories. TOE administrators connect to the TOE via the Secure File Transfer Protocol (SFTP), providing their credentials to identify and authenticate against the TOE before any action.

The TOE provides the administrator the ability to create, modify & delete policies that meditate traffic flow as implemented by the Traffic Filter SFP or Virtual Local Area Network (VLAN) SFP.

3.5 Cryptographic support

The TOE requires cryptography for supporting the following functionality.

- Establishment of secure channels using the SSHv2, TLSv1.1 and TLSv1.2 protocols.
- X.509 certificate generation and validation.
- Storage of passwords.
- Self-tests of the cryptographic algorithms.
- Verification of the integrity of the TOE firmware.

The TOE provides cryptographic support using the OpenSSL and OpenSSH software packages, which are bundled in the TOE.

3.6 Traffic Mediation

The TOE provides filtering of network traffic through two mechanisms: Virtual Local Area Network (VLAN) configuration and traffic filtering based on Access Control Lists (ACLs).

3.7 Protection of the TSF

The TOE protects itself by requiring administrators to identify and authenticate themselves prior to performing any actions and by defining the access allowed by each administrator. The TOE uses the filesystem access control to protect access to sensible data like cryptographic keys and credentials.

The TOE ensures that manual updates of the TOE firmware are done using trusted updates by verifying the integrity of the new version of the TOE firmware.

The TOE also implements self-tests to ensure the correct operation of cryptographic services.

The TOE also provides a reliable date and time that is used for audit record timestamps, certificate verification and session timing.

3.8 Trusted path/channels

The TOE provides the following secure channels to ensure the integrity and confidentiality of the information exchanged between the TOE and external IT entities in the operational environment.

- Transport Layer Security (TLS) versions 1.1 and 1.2 are used to protect communication with authentication servers (RADIUS), LDAP servers, SNMP Management stations, and audit servers (syslog).
- Secure Shell version 2 (SSHv2) is used to protect communication with SSH and SFTP clients and servers.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes seven assumptions on the usage of the TOE.

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

A.PHYSICAL_PROTECTION

The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

A.SERVICES_RELIABLE

All network services in the Operational Environment provide reliable information and responses to the TOE. In case the TSF does not provide a secure channel for the network service, it is assumed that the Operational Environment protects the communication between the network service and the TOE from loss of integrity, either by physical or logical means.

4.2 Clarification of Scope

The Security Target contains nine threats, which have been considered during the evaluation.

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle of the critical network traffic, and potentially could lead to a compromise of the network device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints (e.g. a shared password that is guessable or transported as plaintext). The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

T.PASSWORD_CRACKING

Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other network devices.

T.INFORMATION_FLOW_POLICY_VIOLATION

An unauthorized individual or an IT external entity may send messages through the TOE, which violates the permissible information flow rules enforced by the TOE.

The Security Target contains two Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.ACCESS_BANNER

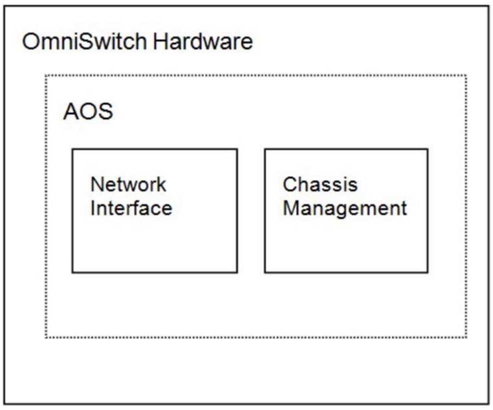
The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

P.SELF_TESTS

The TOE shall ensure the reliability of the cryptographic functionality used in the TOE security functionality by performing self-tests at start-up and during operation.

5 Architectural Information

The following diagram shows the basic components that comprise the TOE.



The term Chassis Management Module (CMM) is used to describe the logical management functionality of the TOE providing the following services.

- Console, Universal Serial Bus (USB), and Ethernet management port connections. The console port that is used to connect a serial console to initialize and configure the TOE via a Command Line Interface (CLI). Depending on the TOE model the physical interface can be an USB or an RJ-45 connector.
- Software and configuration management, including the CLI.
- Power distribution.
- Diagnostics.
- Cryptographic functionality.
- Important availability features, including failover (when used in conjunction with another CMM), software rollback, temperature management, and power management.

Network Interface (NI) modules provides the connectivity to the network through different physical ports, connector types and speed. The NI modules are categorized into Gigabit Ethernet Network Interface (GNI), 10-Gigabit Ethernet Network Interface (XNI) and 40-Gigabit Ethernet Network Interface (QNI) modules. GNI modules provide 1000 Mbps (1 Gbps) connections. GNI modules can be used for backbone connections in networks where Gigabit Ethernet is used as the backbone media. XNI modules provide up to six 10000 Mbps (10 Gbps) connections per module and can be used in networks where 10-gigabit Ethernet is used as the backbone media. Finally, QNI modules provide 40000 Mbps (40 Gbps) connections per module.

The main distinction between models are the form factor (either chassis or stacks), the processor used, the number of physical ports, the port speeds, the connector types, and the amount of physical RAM installed.

The OS6465, OS6560, OS6860, OS6865 series products are packaged in a single PCB with an embedded CPU Cortex ARM 9 processor. The CMM and NI functions execute on this processor, and communicate via a socket based protocol running over TCP/IP.

The OS6900 series products are packaged in a single PCB with a NXP MPC8572, NXP QorIQ P2040 or Intel Atom C2538 processor, depending on the model. The CMM and NI functions execute on this processor, and communicate via a socket based protocol running over TCP/IP.

The OS9900 is a chassis based product including a CMM with an Intel Atom C2518 processor. The CMM functions execute on this processor and communicate with the NIs via a socket based protocol running over TCP/IP. This product can support up to six NI cards containing an Intel Atom C2338 processor, where the NI functions execute.

An Omniswitch can operate in two different modes: Standalone and Virtual Chassis (VC). A virtual chassis is a group of switches managed through a single management IP address that operates as a single bridge and router. Virtual chassis connects two or more physical stackable switches through Virtual Fabric Links (VFL) and has a specific protocol to communicate between switches.

Virtual Chassis mode is not allowed in the evaluated configuration. The TOE must always operate in Standalone mode.

6 Documentation

The following documentation comprises the TOE guidance:

- Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 8.6.R11 [AOS8-CCGUIDE]
- AOS Release 8.6.R01 Release Notes [AOS8-RN]
- OmniSwitch AOS Release 8 Switch Management Guide [AOS8-SM]
- OmniSwitch AOS Release 8 CLI Reference Guide [AOS8-CLI]
- OmniSwitch AOS Release 8 Network Configuration Guide [AOS8-NC]
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide [AOS8-ARC]
- OmniSwitch AOS Release 8 Transceivers Guide [AOS8-TCV]
- OmniSwitch AOS Release 8 Data Center Switching Guide [AOS8-DCS]
- OmniSwitch 6465 Hardware Users Guide [OS6465-HWUG]
- OmniSwitch 6560 Hardware Users Guide [OS6560-HWUG]
- OmniSwitch 6860 Hardware Users Guide [OS6860-HWUG]
- OmniSwitch 6865 Hardware Users Guide [OS6865-HWUG]
- OmniSwitch 6900 Hardware Users Guide [OS6900-HWUG]
- OmniSwitch 9900 Hardware Users Guide [OS9900-HWUG]

7 IT Product Testing

7.1 Developer Testing

The developer performed manual functional tests to verify that the claimed security functionality worked as intended. The tests that were performed by the developer provide full test coverage.

The developer reported that all tests were completed successfully.

7.2 Evaluator Testing

The evaluator re-run a number of developer tests on two TOE models from different hardware families: 6860 and 6900, and analyse some of the developer tests in more detail.

The execution and analysis of the developer tests were performed by the evaluator successfully. All tests were performed successfully - expected and actual results were consistent.

7.3 Penetration Testing

Vulnerability testing was performed against the TOE interfaces that are accessible to a potential attacker. I.e., the IPv4/IPv6 TCP and UDP ports of the TOE. The evaluator also executed a command against SSH that was identified during the public vulnerability search.

None of the performed penetration tests revealed any exploitable vulnerability in the TOE.

8 Evaluated Configuration

The intended TOE environment is a secure data center that protects the TOE from unauthorized physical access. Only security administrators are to have access to connect to the serial console, or gain physical access to the hardware storing log data. Appropriate administrator security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

- If the TOE is part of a network where network addresses are assigned dynamically, a Dynamic Host Configuration Protocol (DHCP) server is required in the operational environment. Communication between the TOE and the DHCP server must be reliable and protected from loss of integrity by physical or logical means.
- Versions 1.1 and 1.2 of the TLS protocol are the only versions allowed in the evaluated configuration. Usage of other protocol versions usually supported in SSL and TLS (SSLv2.0, SSLv3.0 or TLSv1.0) are prohibited.
- If the TOE is configured to use a RADIUS authentication server, or an LDAP server for credential storage, the TOE is dependent upon this external server in the operational environment for authentication.
- If the TOE is configured to use an LDAP server for credential storage, then a TLSv1.1 or TLSv1.2 capable LDAP server is required in the operational environment.
- If the TOE is configured to use a RADIUS external server for credential storage, then a TLSv1.1 or TLSv1.2 capable RADIUS server is required in the operational environment.
- If the TOE is configured to perform IEEE 802.1X authentication, then the TOE is dependent upon an IEEE 802.1X client to be on the end user device attached to the LAN port in the TOE operating environment. This client is built into most standard current operating systems.
- In addition, if 802.1X is enabled, the TOE is dependent upon a RADIUS authentication server in the TOE operational environment.
- If the TOE is configured to use SNMP, only SNMPv3 can be used and protected with the Transport Security Model (TSM) ("snmp security tsm enable" setting); In addition, a TLSv1.1 or TLSv1.2 capable SNMP Network Management Station is required in the operational environment.
- If the TOE is configured to send logging output files (syslog files) to a remote IP address, a TLSv1.1 or TLSv1.2 capable syslog server is required in the operational environment.
- If the domain name is used as an identifier in the Subject Alternative Names (SAN) of external servers' certificates (LDAP, SNMP, Syslog, Radius), then the Domain Name Server (DNS) must be configured to support reverse DNS so server certificates can be validated during the TLS session establishment.
- A serial console connected to the appliance must be available for installation and initial configuration. Once installation and configuration is completed, access to the TOE can be performed via the serial console as well as a remote console.
- If remote console is used, the Operational Environment must include an SSHv2 client.
- File transfers between the TOE and external servers, when the TOE is acting either as a client or a server, must be only performed using SFTP. FTP and Trivial File Transfer Protocol (TFTP) are forbidden. In this case, the Operational Environment must include an SFTP client or server.

The following features interfere with the TOE security functionality claims and must be disabled or not configured for use in the evaluated configuration:

- Virtual Chassis mode
- Captive Portal
- Terminal Access Controller Access-Control System Plus (TACACS+)
- Internetwork Packet Exchange (IPX) forwarding (routing)
- Port Mobility Rules
- FTP access to the TOE
- Telnet access to the TOE
- Webview
- SNMP versions 1 and 2
- HTTP and HTTPs
- Cryptographic algorithms: The MD5 algorithm
- The use of NTP to synchronize the time with an external time source.
- IPSec

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class/Family	*Component*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Flaw Remediation	ALC_FLR.2	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

ACL	Access control List
ALE	Alcatel-Lucent Enterprise
AOS	Alcatel-Lucent Operating System
ARM	Advanced RISC Machine
CEM	Common Methodology for Information Technology Security
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
GigE	Gigabit Ethernet
GNI	Gigabit Ethernet Network Interface
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITSEF	IT Security Evaluation Facility
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
PCB	Printer Circuit Board
QNI	40-Gigabit Ethernet Network Interface
RADIUS	Remote Authentication Dial In User Service
SAN	Subject Alternative Name
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSHv2	Secure Shell version 2
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TSM	Transport Security Model
TOE	Target of Evaluation
UDP	User Datagram Protocol
USB	Universal Serial BUS
VC	Virtual Chassis
VFL	Virtual Fabric Link
VLAN	Virtual LAN
XNI	10-Gigabit Ethernet Network Interface

12 Bibliography

ST Alcatel-Lucent Enterprise OmniSwitch with AOS 8.6.R11 Security Target for EAL2, ALE USA Inc., 2021-02-03, document version 3.2

AOS8-ARC OmniSwitch AOS Release 8 Advanced Routing Configuration Guide, Rev. A, July 2019

AOS8-CCGUIDE Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS Release 8.6.R11, December 2020

AOS8-CLI OmniSwitch AOS Release 8 CLI Reference Guide, Rev. A, July 2019

AOS8-DCS OmniSwitch AOS Release 8 Data Center Switching Guide, Rev. A, July 2019

AOS8-NC OmniSwitch AOS Release 8 Network Configuration Guide, Rev. A, July 2019

AOS8-RN Release Notes - OmniSwitch 6465/6560/9900/6900/6860(E)/6865, Rev. A, July 2019

AOS8-SM OmniSwitch AOS Release 8 Switch Management Guide, Rev. A, July 2019

AOS8-TCV OmniSwitch AOS Release 8 Transceivers Guide, Rev. A, July 2019

OS6465-HWUG OmniSwitch 6465 Hardware Users Guide, Rev E, July 2019

OS6560-HWUG OmniSwitch 6560 Hardware Users Guide, Rev F, July 2019

OS6860-HWUG OmniSwitch 6860/6860E Hardware Users Guide, Rev H, July 2019

OS6865-HWUG OmniSwitch 6865 Hardware Users Guide, Rev L, July 2019

OS6900-HWUG OmniSwitch 6900 Hardware Users Guide, Rev. P, March 2019

OS9900-HWUG OmniSwitch 9900 Series Hardware Users Guide, Rev H, July 2019

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC CCpart1 + CCpart2 + CCpart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

SP-002 SP-002 Evaluation and Certification, CSEC, 2020-11-30, document version 32.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.23 valid from 2019-10-14

QMS 1.23.1 valid from 2020-03-06

QMS 1.23.2 valid from 2020-05-11

QMS 1.24 valid from 2020-11-19

QMS 1.24.1 valid from 2020-12-03

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.24.1”. The certifier concluded that, from QMS 1.23 to the current QMS 1.24.1, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 28 - Updated procedures for application, evaluation and certification