CSEC

Swedish Certification Body for IT Security

Certification Report - ALE Omniswitch

Issue: 1.0, 2017-Oct-17

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary 3

2 Identification 4

3 Security Policy 5

3.1 Audit 5

3.2 Administrator Identification and Authentication 5

3.3 End user and device authentication 6

3.4 Management of the TOE 6

3.5 Cryptographic support 6

3.6 Traffic Mediation 6

3.7 Protection of the TSF 6

4 Assumptions and Clarification of Scope 8

4.1 Usage Assumptions 8

4.2 Environmental Assumptions 8

4.3 Clarification of Scope 9

5 Architectural Information 11

6 Documentation 13

7 IT Product Testing 14

7.1 Evaluator Testing 14

7.2 Penetration Testing 14

8 Evaluated Configuration 15

9 Results of the Evaluation 17

10 Evaluator Comments and Recommendations 18

11 Glossary 19

12 Bibliography 20

Appendix A Scheme Versions 22

A.1 Scheme/Quality Management System 22

A.2 Scheme Notes 22

1 Executive Summary

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

The evaluation covers two groups of models:

- ALE Omniswitch 6250, 6350, and 6450 with the AOS 6.7.1.79.R04 firmware, which is based on the VxWorks version 5.5.1 operating system.
- ALE Omniswitch 6860, 6865, 6900, 9900, and 10K with the AOS 8.3.1.348.R01 firmware, which is based on the Linux version 3.10.34 operating system.

The Security Target claims exact conformance to Collaborative Protection Profile for Network Devices (NDcPP) v1.0 (NDcPP).

There are six 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 single organisational security policy (OSP) in the ST. The assumptions, threats and the OSP 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, and in their foreign location in Austin, USA.

The evaluation was completed in 2017-09-28. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 revision 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 Evaluation Activities for Network Device cPP v1.0 (EA NDcPP), and the Security Target (ST). The certifier has also determined that the requirements of EAL 1 augmented by ASE_SPD have been met.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by atsec information security AB.

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	CSEC2016007
Name and version of the certified IT product	ALE Omniswitch 6250, 6350, and 6450, with the AOS 6.7.1.79.R04 firmware, and ALE Omniswitch 6860, 6865, 6900, 9900, and 10K, with the AOS 8.3.1.348.R01 firmware
Security Target Identification	Alcatel-Lucent Enterprise OmniSwitches with AOS 6.7.1.R04 and AOS 8.3.1.R01 Security Target
Assurance claims	Evaluation Activities for Network Device cPP v1.0
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	1.20.5
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2017-10-17

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

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 logs to a text file stored in the systems flash memory for permanent storage. These audit log entries are tagged with the AOS Application that created them. The TOE also provides the ability to send switch logging information 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 log files (the default value and allowed ranges for this value depends on the AOS version). Once the files are full the oldest entries are overwritten.

3.2 Administrator Identification and Authentication

Security Management is performed by administrators that must identify and authenticate to the TOE before any action. Whether through serial console or Secure Shell (SSH), the TOE requires the administrator to identify and authenticate to the TOE prior to accessing any of the management functionality. 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 the RADIUS and LDAP servers can be protected with the Transport Layer Security (TLS) protocol.

The TOE provides administrator configurable password settings to enforce local password complexity when a password is created or modified. The TOE also displays to the user a configurable banner before a session starts, and provides the ability to terminate a session after a configurable period of inactivity.

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).

3.4 Management of the TOE

The TOE provides the CLI for the TOE's security management functionality. The TOE also provides a Flash file system for storing configuration files/directories. Files can be transferred to the Flash file system via Secure File Transfer Protocol (SFTP).

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

The Simple Network Management Protocol (SNMP) is supported by the TOE but is not allowed in the evaluated configuration.

3.5 Cryptographic support

The TOE requires cryptography for supporting the following functionality.

- Establishment of secure channels using the SSHv2 and TLS v1.1 and v1.2 protocols
- X.509 certificate generation and validation
- Storage of passwords
- IPsec protocol (for AOS 8.3.1.R01 only)

The TOE provides cryptographic support using the OpenSSL and OpenSSH software packages. For the IPsec protocol, the TOE uses cryptographic functionality provided by the crypto library that is part of AOS 8.3.1.R01

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 key and credentials.

The TOE also implements self-tests to ensure the correct operation of cryptographic services, as well as integrity tests on software updates to ensure that software updates to the TOE can be trusted.

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, audit servers (syslog).

- Secure Shell version 2 (SSHv2) is used to protect communication with SSH and SFTP clients and servers.

The TOE also supports IPsec in AOS 8.3.1.R01 for protecting IPv6 communications; Internet Protocol Security (IPsec) is a suite of protocols for securing IP traffic and the exchange of route information with external routers.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes three 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 computing platform for general purpose applications (unrelated to networking functionality).

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.

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.

4.2 Environmental Assumptions

The Security Target [ST] makes three assumptions on the operational environment of the TOE.

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.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.NO_THRU_TRAFFIC_PROTECTION

A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity is not covered by theNetwork Device collaborative Protection Profile. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g. firewall).

4.3 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 tunneling 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 attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity 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 include 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.SECURITY_FUNCTIONALITY_FAILURE

A component of the network device may fail during start-up or during operations causing a compromise or faiure in the security functionality of the network device, leaving the device susceptible to attackers.

The Security Target contains one Organisational Security Policy (OSP), which has 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.

5 Architectural Information

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

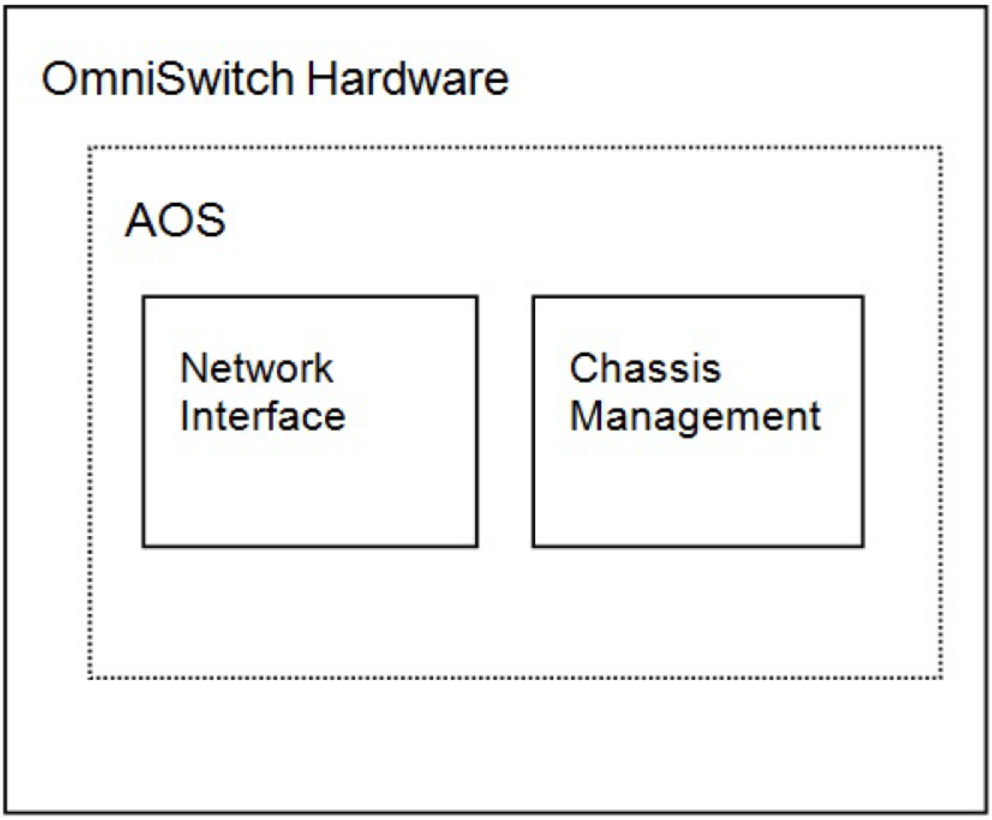

Figure 1: TOE Architecture

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 to the switch. 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
- Switch diagnostics
- 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 10000 Mbps (10 Gbps) connections 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.

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

6 Documentation

The following guidance documents are included in the scope of the TOE:

● OmniSwitch models with AOS 6.7.1.79.R04:

- Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 6.7.1.R04
- AOS Release 6.7.1 Release Notes
- OmniSwitch AOS Release 6250/6350/6450 Switch Management Guide
- OmniSwitch AOS Release 6250/6350/6450 CLI Reference Guide
- OmniSwitch AOS Release 6250/6350/6450 Network Configuration Guide
- OmniSwitch 6250/6350/6450 Transceivers Guide
- OmniSwitch 6250 Hardware Users Guide
- OmniSwitch 6350 Hardware Users Guide
- OmniSwitch 6450 Hardware Users Guide

● OmniSwitch models with AOS 8.3.1.348.R01:

- Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 8.3.1.R01
- AOS Release 8.3.1 Release Notes
- OmniSwitch AOS Release 8 Switch Management Guide
- OmniSwitch AOS Release 8 CLI Reference Guide
- OmniSwitch AOS Release 8 Network Configuration Guide
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide
- OmniSwitch AOS Release 8 Transceivers Guide
- OmniSwitch AOS Release 8 Data Center Switching Guide
- OmniSwitch 6860 Hardware Users Guide
- OmniSwitch 6865 Hardware Users Guide
- OmniSwitch 6900 Hardware Users Guide
- OmniSwitch 9900 Hardware Users Guide
- OmniSwitch 10K Hardware Users Guide
- OmniSwitch 10K Getting Started Guide

7 IT Product Testing

7.1 Evaluator Testing

The evaluator performed complete testing of the ALE Omniswitch 6350, 6900 and 10K models, covering both firmwares, and partial testing of ALE Omniswitch 6250, 6450, 6860, and 9900 to establish confidence that all variations of the TOE hardware behaves similarly.

All tests showed that the TOE behaves as expected.

7.2 Penetration Testing

The evaluators identified many third party components, for each of which several public vulnerability databases were searched. The vulnerability testing was performed using the ALE Omniswitch 6350, and 6900 models. Toolbased IP v4 TCP and UDP portscans and testing of a potential SSH vulnerability from the database search was performed. No exploitable vulnerabilities were found.

8 Evaluated Configuration

During installation and setup, the user is expected to follow the guidance, in particular “Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 6.7.1.R04” or “Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 8.3.1.R01” depending on model.

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

Authenticated VLAN

(feature provided only in AOS 6.7.1.R04)

An authenticated VLAN grants end-users access to one or more VLANs after successful authentication at the switch port. Authenticated VLAN permissions are granted to end-users (not devices) leveraging external RADIUS, or LDAP directory servers, an authenticated VLAN grants end-users access to one or more VLANs after successful authentication at the switch port. Authenticated VLAN permissions are granted to end-users (not devices) leveraging external RADIUS, or LDAP directory servers.

This feature is superseded by Captive Portal and has been kept in the product for backwards compatibility reasons.

- Alcatel-Lucent-proprietary authentication client for VLAN-authentication
- Telnet authentication client for VLAN-authentication

Captive Portal

This feature allows web-based authentication of end-users.

Terminal Access Controller Access-Control System Plus (TACACS+)

Authentication using an external TACACS+ server is not allowed in the CC evaluated configuration.

Internetwork Packet Exchange (IPX) forwarding (routing)

(feature provided only in AOS 6.7.1.R04)

This feature has been kept in the product for backwards compatibility reasons.

Port Mobility Rules

Port mobility allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic.

This feature is superseded by User network profiles and has been kept in the product for backwards compatibility reasons.

FTP access to the switch

FTP traffic is not secured so the FTP service must be disabled for security reasons

Telnet access to the switch

Telnet traffic is not secured so the Telnet service must be disabled for security reasons.

Webview

This web-based interface used for switch management must be disabled.

Simple Network Management Protocol (SNMP)

SNMP must be disabled in the CC evaluated configuration.

Hypertext Transfer Protocol (HTTP)

HTTP and HTTPs must be disabled in the CC evaluated configuration.

Cryptographic algorithms

The MD5 algorithm cannot be used.

Network Time Protocol (NTP)

The use of NTP to synchronize the time with an external time source must be disabled in the CC evaluated configuration.

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 evaluators also performed all evaluation activities in Evaluation Activities for Network Device cPP v1.0.

The certifier reviewed the work of the evaluator 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
	Functional Specification	ADV_FSP.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.1	PASS
	CM Scope	ALC_CMS.1	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.1	PASS
	Extended Components Definition	ASE_ECD.1	PASS
	Security Requirements	ASE_REQ.1	PASS
	TOE Summary Specification	ASE_TSS.1	PASS
Tests		ATE	PASS
	Independent Testing	ATE_IND.1	PASS
Vulnerability Assessment		AVA	PASS
	Vulnerability Analysis	AVA_VAN.1	PASS
Evaluation Activities for NDcPP			PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria for Information Technology Security, a set of three documents describing different aspects of Common Criteria evaluations
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
PP	Protection Profile,
SFR	Security Functional Requirement, a requirement included in the ST, on the TOE
TOE	Target of Evaluation, the (part of a) product that is evaluated
TSF	TOE Security Function(s), the part of TOE that implements security mechanisms, as defined in the ST

12 Bibliography

ST	Alcatel-Lucent Enterprise OmniSwitches with AOS 6.7.1.R04 and AOS 8.3.1.R01 Security Target, ALE-USA Inc, 2017-09-29, document version 1.0
CCGuide6	Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 6.7.1.R04, ALE-USA Inc, June 2017, document version 060471-00 Rev A
RN6	AOS Release 6.7.1 Release Notes, ALE-USA Inc, February 2017, document version 033169-10 Rev A
SMG6	OmniSwitch AOS Release 6250/6350/6450 Switch Management Guide, ALE-USA Inc, October 2016, document version 060438-10 Rev A
CLI6	OmniSwitch AOS Release 6250/6350/6450 CLI Reference Guide, ALE-USA Inc, October 2017, document version 060440-10 Rev A
NET6	OmniSwitch AOS Release 6250/6350/6450 Network Configuration Guide, ALE-USA Inc, October 2016, document version 060439-10 Rev A
TG6	OmniSwitch 6250/6350/6450 Transceivers Guide, ALE-USA Inc, October 2016, document version 060441-10 Rev A
HW6250	OmniSwitch 6250 Hardware Users Guide, ALE-USA Inc, October 2016, document version 060303-10 Rev G
HW6350	OmniSwitch 6350 Hardware Users Guide, ALE-USA Inc, February 2017, document version 060406-10 Rev D
HW6450	OmniSwitch 6450 Hardware Users Guide, ALE-USA Inc, October 2016, document version 060351-10 Rev K
CCGuide8	Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 8.3.1.R01, ALE-USA Inc, June 2017, document version 060472-00 Rev A
RN8	AOS Release 8.3.1 Release Notes, ALE-USA Inc, February 2017, document version 033168-10 Rev A
SMG8	OmniSwitch AOS Release 8 Switch Management Guide, ALE-USA Inc, September 2016, document version 060411-10 Rev A
CLI8	OmniSwitch AOS Release 8 CLI Reference Guide, ALE-USA Inc, February 2017, document version 060415-10 Rev B
NET8	OmniSwitch AOS Release 8 Network Configuration Guide, ALE-USA Inc, September 2016, document version 060412-10 Rev A
ARG8	OmniSwitch AOS Release 8 Advanced Routing Configuration Guide, ALE-USA Inc, September 2016, document version 060413-10 Rev A
TG8	OmniSwitch AOS Release 8 Transceivers Guide, ALE-USA Inc, September 2016, document version 060416-10 RevA
DCSG8	OmniSwitch AOS Release 8 Data Center Switching Guide, ALE-USA Inc, September 2016, document version 060414-10 Rev A

HW6860	OmniSwitch 6860 Hardware Users Guide, ALE-USA Inc, September 2016, document version 060390-10 Rev D
HW6865	OmniSwitch 6865 Hardware Users Guide, ALE-USA Inc, January 2017, document version 060435-10 Rev C
HW6900	OmniSwitch 6900 Hardware Users Guide, ALE-USA Inc, September 2016, document version 060334-10 Rev L
HW9900	OmniSwitch 9900 Hardware Users Guide, ALE-USA Inc, February 2017, document version 060409-10 Rev C
HW10K	OmniSwitch 10K Hardware Users Guide, ALE-USA Inc, September 2016, document version 060310-10 Rev J
START10K	OmniSwitch 10K Getting Started Guide, ALE-USA Inc, October 2016, document version 060309-10 Rev A
CC	Common Criteria for Information Technology Security Evaluation, CCMB-2017-04-001 through 003, document versions 3.1 revision 4
CEM	Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, document version 3.1 revision 5
NDcPP	Collaborative Protection Profile for Network Devices (NDcPP) v1.0, 2015-02-27
EA NDcPP	Evaluation Activities for Network Device cPP v1.0, 2017-02-27

Appendix A Scheme Versions

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

A.1 Scheme/Quality Management System

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used:

Version	**Introduced**	**Impact of changes**
1.20.5	2017-06-28	*None*
1.20.4	2017-05-11	*None*
1.20.3	2017-04-24	*None*
1.20.2	2017-02-27	*None*
1.20.1	2017-01-12	*None*
1.20	2016-10-20	*None*
1.19.3	Application	Initial version

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 QMS 1.20”.
The certifier concluded that, from QMS 1.19.3 to the current QMS 1.20.5, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target