Swedish Certification Body for IT Security

Certification Report ALE OmniAccess Stellar

Issue: 1.0, 2021-okt-29

Authorisation: Ulf Noring, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is several hardware models of wireless local area network access points running a specific firmware. The TOE is used to securely connect wireless clients to a wired network. It enforces Wi-Fi Protected Access 2 (WPA2) to authenticate wireless clients and to protect the confidentiality and integrity of wireless traffic.

The TOE models are:

Alcatel-Lucent OmniAccess Stellar AP series AP1201, AP1201H/HL/L, AP1220, AP1230, AP1251, AP1320 and AP1360 with AWOS 4.0.1 (build number 504) firmware.

The TOE provides the following security functions:

• Security audit

• Cryptographic support for WPA2, IEEE 802.1X, TLS, and secure storage of passwords and keys

• Identification and authentication of administrators and wireless clients

• Security management

• Protection of the TSF including firmware, sensitive data and system time

• TOE access control based on inactivity time and time/day

• Trusted path/channels for remote administration and wireless communication

Alcatel-Lucent Enterprise orders for the Common Criteria evaluated TOE are delivered using reputable couriers for shipping. Hardware is packaged in electrostatic discharge (ESD) bags and sealed with an ESD warning label. It is then boxed in the factory using tape.

The evaluated firmware must be loaded by the customer after receiving the hardware in order to ensure correct configuration. The firmware on the shipped OmniAccess Stellar AP is not guaranteed to be the same version as evaluated. The evaluated firmware can be obtained from the Alcatel-Lucent Enterprise Business Portal (https://businessportal2.alcatel-lucent.com). The TOE guidance can be downloaded from the same portal. In order to access the Business Portal, the user must have a support contract in place.

The security target [ST] claims conformance to the EAL2 package of security assurance requirements, augmented with ALC_FLR.1. It does not claim conformance to any Protection Profile (PP).

Twelve threats, one OSP and four assumptions are specified in chapter three in the security target [ST].

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden. The evaluation was completed on 2021-10-01. 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 Crite-ria 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.1. 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.

2 Identification

Certification Identification	
Certification ID	CSEC2020006
Name and version of the certified IT product	Alcatel-Lucent OmniAccess Stellar AP series AP1201, AP1201H/HL/L, AP1220, AP1230, AP1251, AP1320 and AP1360 with AWOS 4.0.1 (build number 504) firmware. See the list below for the exact hardware models covered by the certification.
Security Target Identification	Alcatel-Lucent OmniAccess Stellar AP Security Target, Alcatel-Lucent, 2021-10-06, document version 1.0
EAL	EAL 2 + ALC_FLR.1
Sponsor	ALE USA Inc.
Developer	ALE USA Inc. Hardware design: HAN Networks or Sercomm Corporation (depending on hardware model) Software design: HAN Networks
ITSEF	atsec information security AB
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	1.25
Scheme Notes Release	18.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2021-10-29

The certified models of the TOE are:

OAW-AP1201-RW, rev. D01
OAW-AP1201-US, rev.
OAW-AP1201-ME, rev. A01
OAW-AP1201H-RW, rev. F01
OAW-AP1201H-US, rev. B01
OAW-AP1201H-ME, rev. B01
OAW-AP1201HL-RW, rev. A
OAW-AP1201L-RW, rev. A
OAW-AP1221-RW, rev. E
OAW-AP1221-US, rev. B
OAW-AP1221-ME, rev. B01
OAW-AP1222-RW, rev. E
OAW-AP1222-US, rev. B

OAW-AP1222-ME, rev. B01
OAW-AP1231-RW, rev. B01
OAW-AP1231-US, rev. B04
OAW-AP1232-RW, rev. B01
OAW-AP1232-US, rev. B03
OAW-AP1251-RW, rev. E
OAW-AP1251-US, rev. C
OAW-AP1251-ME, rev. B
OAW-AP1321-RW, rev. A
OAW-AP1321-US, rev. A
OAW-AP1321-ME, rev. A
OAW-AP1322-RW, rev. A
OAW-AP1322-US, rev. A
OAW-AP1322-ME, rev. A
OAW-AP1361-RW, rev. A
OAW-AP1361-US, rev. A
OAW-AP1361-ME, rev. A
OAW-AP1361D-RW, rev. A
OAW-AP1361D-US, rev. A
OAW-AP1361D-ME, rev. A
OAW-AP1362-RW, rev. A
OAW-AP1362-US, rev. A
OAW-AP1362-ME, rev. A

3 Security Policy

The TOE provides the following security functionality:

- Security audit
- Cryptographic support for WPA2, IEEE 802.1X, TLS, and secure storage of passwords and keys
- Identification and authentication of administrators and wireless clients
- Security management
- Management of cryptographic keys
- Configuration of login banner, authentication failure parameters, session timeout
- Manual update of TOE firmware
- Start and stop WLAN service
- Protection of the TSF including firmware, sensitive data and system time
- TOE access control based on inactivity time and time/day
- Trusted path/channels for remote administration and wireless communication

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 a computing platform for general purpose applications (unrelated to networking functionality).

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.

A.PRESHARED_KEY

For pre-shared key based authentication of wireless clients, it is assumed that the pre-shared key is provided only to trusted users

4.2 Environmental Assumptions

The Security Target [ST] makes one assumption 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.

4.3 Clarification of Scope

The Security Target contains twelve 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 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. NETWORK_DISCLOSURE

Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.

T. NETWORK_ACCESS

Unauthorized access may be achieved to services on a protected network from outside that network.

T. DATA_INTEGRITY

A malicious party attempts to change the data being sent - resulting in loss of integrity.

T. REPLAY_ATTACK

If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.

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 TOE encompasses the entire device, including both the hardware and firmware. The TOE hardware platforms (chipset and CPU) are described in the table below. The next table after that specifies the firmware, physical interfaces and features of the different TOE models. All models run the same firmware, AWOS 4.0.1 build 504.

TOE Models	Chipset (Qualcomm)	CPU (integrated in main chip)	Linux Kernel
OAW-AP1201	IPQ4018	Quad-core ARM Cortex-A7 at 600 MHz	3.14.77-ARM
OAW-AP1201H, OAWAP1201HL, OAWAP1201L	QCA9563 + QCA9886	MIPS 74Kc at 775Mhz	3.14.77-MIPS
OAW-AP1221, OAWAP1222	IPQ4029 + QCA9994	Quad-core ARM Cortex-A7 at 717MHz	3.14.77-ARM
OAW-AP1231, OAWAP1232	IPQ8065 + QCA9994	Dual-core SMP Krait CPU (ARMv7-compliant) at 1.7GHz	3.14.77-ARM
OAW-AP1251	IPQ4029	Quad-core ARM Cortex-A7 at 717MHz	3.14.77-ARM
OAW-AP1321, OAWAP1322	IPQ8071A	Quad ARM Cortex A53s, 1.0GHz	4.4.60-ARM
OAW-AP1361, OAWAP1361D, OAW-AP1362	IPQ8071A	Quad ARM Cortex A53s, 1.0GHz	4.4.60-ARM

TOE Models	Hardware Description
OAW-AP1201	The 802.11ac AP1201 access point supports a maximum concurrent data rate of 1.2 Gb/s (867 Mb/s in 5 GHz and 400 Mb/s in 2.4 GHz), 80 MHz channels (VHT80), multi-user MIMO (MU-MIMO) and two spatial streams (2SS) per radio. Antenna: Built-in 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz, BLE antenna. Interfaces: • 1× 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1x Bluetooth Low Energy (BLE) 5.0 radio, integrated antenna. Hardware ready for Zigbee. • 1× management console port (RJ-45) • Reset button: Factory reset • DC48V power jack • Kensington security slot
OAW-AP1201H, OAWAP1201HL, OAWAP1201L	The 802.11ac AP1201H access point supports a maximum concurrent data rate of 1.2 Gb/s (867 Mb/s in 5 GHz and 300 Mb/s in 2.4 GHz), MUMIMO and two spatial streams (2SS). Antenna: Built-in 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz. Interfaces: • Uplink: 1× 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE)

	• Downlink: o AP1201H: 1× 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE-PSE) 802.3af compliant; 2×10/100/1000Base-T autosensing (RJ-45) port o AP1201HL: 3× 10/100/1000Base-T autosensing (RJ-45) port • AP1201H and AP1201HL: Passive Pass through one pair, back and bottom • AP1201H and AP1201HL: 1× USB 2.0 (Type A) • AP1201L: 1× management console port (RJ-45) • Reset button: Factory reset • DC48V power jack
OAW-AP1221, OAWAP1222	The 802.11ac AP1220 series supports a maximum concurrent data rate of 2.1 Gb/s (1733 Mb/s in 5 GHz and 400 Mb/s in 2.4 GHz), 160 MHz channels (VHT160*), multi-user MIMO (MUMIMO) and four spatial streams (4SS). Antenna: • AP1221: Built-in 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • AP1222: External 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • Optional external antenna (sold separately) Interfaces: • 1x 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1x USB 2.0 (Type A connector) • 1x management console port (RJ-45) • Reset button: Factory reset • DC48V power jack • Kensington security slot • AP1222: 4x RP-SMA antenna connectors
OAW-AP1231, OAWAP1232	The 802.11ac AP1230 series supports a maximum concurrent data rate of 4.266 Gb/s (dual 1733 Mb/s in 5 GHz and 800 Mb/s in 2.4 GHz), dual uplinks with 2.5 GbE and 1 GbE, 160 MHz channels (VHT160*), multi- user MIMO (MUMIMO) and four spatial streams (4SS). Antenna: • AP1231: Built-in 4×4:4 @ 2.4 GHz, dual 4x4:4 @ 5 GHz • AP1232: External 4×4:4 @ 2.4 GHz, dual 4x4:4 @ 5 GHz 8 RP-SMA connectors for external dual band antennas. • Optional external antenna (sold separately) Interfaces: • 1x 100/1000/2500Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1x 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1x Bluetooth Low Energy (BLE) radio, integrated antenna • 1x USB 2.0 (Type A connector) • 1x management console port (RJ-45) • Reset button: Factory reset • DC48V power jack • Kensington security slot • AP1232: 8x RP-SMA antenna connectors
OAW-AP1251	The AP1251 supports the IP67 standard for harsh outdoor environments, such as exposure to high and low temperatures, persis-

	tent moisture and precipitation, and electrical interfaces include industrial strength surge protection. The AP1251 supports a maximum concurrent data rate of 1.267 Gb/s (867 Mb/s in 5 GHz and 400 Mb/s in 2.4 GHz), and dual Gigabit Ethernet links, integrated omni-directional antennas, the AP1251 is ideal for medium density outdoor environments. Antenna: Built-in 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz. Interfaces: • 1× 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1× 10/100/1000Base-T autosensing (RJ-45) port • 1x management console port (Micro-USB) • Reset button: Factory reset
OAW-AP1321, OAWAP1322	The OmniAccess Stellar AP1320 series supports a maximum aggregate data rate of 3Gbps (2.4Gbps in 5 GHz and 573Mbps in GHz). To support this higher capacity the access point is powered by a Multigig Ethernet uplink. Antenna: • AP1321: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • AP1322: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz Interfaces: • 1x 10BASE-Te/100BASE-TX/1000BASET/2500BASE-T IEEE 802.3 compliant autosensing (RJ-45) port, ENET0, Power over Ethernet (PoE) 802.3at compliant • 1x 10/100/1000 BASE-T IEEE 802.3 compliant auto-sensing (RJ-45) port, ENET1, Power over Ethernet (PoE) 802.3at compliant • 1x BLE/ZigBee radio • 1x USB 2.0 Type A (5V, 500mA) • 1x management console port (RJ-45) • Reset button: Factory reset • DC48V power jack • AP1322: 4x RP-SMA female external antenna connectors
OAW-AP1361, OAWAP1361D, OAW-AP1362	The OmniAccess Stellar AP1320 series supports a maximum aggregate data rate of 3Gbps (2.4Gbps in 5 GHz and 573Mbps in GHz). To support this higher capacity the access point is powered by a Multigig Ethernet uplink. Antenna: • AP1361: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • AP1361D: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • AP1362: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz Interfaces: • 1x 10/100/1000/2500 Mbps IEEE 802.3 compliant autosensing (RJ-45) uplink port, ENET0, Power over Ethernet (PoE) 802.3at/bt compliant • 1x 10/100/1000 Mbps IEEE 802.3 compliant auto-sensing (RJ-45) downlink port, ENET1, PoE output up to 802.1at power dependent on input PoE • 1x SFP port • 1x BLE/ZigBee radio • 1x USB 2.0 Type C • 1x management console port (Micro-USB) • Reset button: Factory reset

	• AP1362: 6x N-type external antenna connectors, integrated 6KA lightning protection, not require additional lighting arrester

6 Documentation

The following documentation comprises the TOE guidance and is available on the Alcatel-Lucent Enterprise Service and Support website:

• OmniAccess Stellar AP User Guide [APGUIDE]

• Common Criteria Evaluated Configuration Guide for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points [CCECG]

7 IT Product Testing

7.1 Developer Testing

The developer has performed testing against all TSFIs, covering functionality related to every claimed SFR by at least one test. Since the TOE includes different AP models, the developer has performed testing against a set of TOE models covering every hardware chipset:

- AP1201
- AP1201H
- AP1221
- AP1231
- AP1321

The developer has executed a total of 78 test cases for each tested TOE model. The test cases specify both negative and positive testing. The developer has provided the results of all test cases that were performed. All tests were successful.

7.2 Evaluator Testing

The evaluator did not identify any gaps in the coverage of the developer's testing to TSF or TSFIs. The evaluator expanded two developer test cases to increase the depth of testing for the two sensitive cryptographic TSFIs:

- ETC#1: Extended TLS testing
- ETC#2: Extended WPA2 testing

The evaluator also re-executed a sample of the developer's test cases, which consisted of 7 manual tests. These tests were selected to cover all TSFIs and every applicable SFR class. As SFR classes denominate separate security functions, the evaluator used these to attempt to cover different areas of the TOE implementation. While the developer had tested all relevant TOE models, the evaluator selected AP1221 and AP1201H. All evaluator tests were executed against both models. All evaluator tests, both the test sample and test subset, were completed successfully.

7.3 Penetration Testing

Penetration testing was conducted against a set of potential vulnerabilities within the TOE, as identified during the public search for vulnerabilities and during the search of vulnerabilities through the developer's evidence. For each identified attack surface and potential vulnerability, a penetration test was devised to verify that no actual vulnerability was present. A port scanner was used to scan for undocumented network ports. An automated TLS scanner was used to verify the setup of the TLS service. Finally, for a number of unused services, various tools were used to attempt to establish a connection and extract any kind of data. The testing was conducted using negative tests, i.e. that output was not expected in the case that no vulnerability was present. To confirm the whether the identified potential vulnerabilities were applicable to the TOE, only simple tests were necessary, e.g. to attempt to connect to a service and confirm that the attempt was unsuccessful. However, at least one test was devised for each potential vulnerability. None of the performed penetration tests revealed any applicable vulnerability in the TOE.

8 Evaluated Configuration

The TOE is intended to operate in a secure enterprise environment that protects the TOE from unauthorized physical access. Appropriate security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

The TOE environment requires an administrator workstation is also needed to configure the TOE. For 802.1X authentication, a RADIUS server is needed. A syslog server can be provided for additional log storage.

The following items need to be adhered to in the evaluated configuration:

• 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 (SSLv1.0, SSLv2.0, SSLv3.0 or TLSv1.0) are prohibited.

• The console interface shall not be used to perform any management functions on the TOE

• FTP/TFTP access to the AP must be disabled for security reasons.

• Secure Shell (SSH) is used only for diagnostics and must be disabled in the CC evaluated configuration.

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

• The use of captive portal for guest WLAN access must be disabled in the CC evaluated configuration.

For more information on the evaluated configuration, please see the Common Criteria Evaluated Configuration Guide for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points [CCECG] which is available on the Alcatel-Lucent Enterprise Service and Support website.

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 Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
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
Derived security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Life-cycle support	ALC	PASS
Use of a CM system	ALC_CMC.2	PASS
Parts of the TOE CM Coverage	ALC_CMS.2	PASS
Delivery procedures	ALC_DEL.1	PASS
Flaw reporting procedures	ALC_FLR.1	PASS
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.2	PASS
Basic design	ADV_TDS.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

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
TOE	Target of Evaluation
AP	Access Point
WLAN	Wireless Local Area Network

12 Bibliography

12.1 General

CC Combination of CCp1, CCp2, CCp3, and CEM (see below)

CCp1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCp2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCp3 Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 5, April 2017, CCMB-2017-04-003

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

ST Alcatel-Lucent OmniAccess Stellar AP Security Target, ALE USA Inc., 2021-10-06, document version 1.0

SP-002 SP-002 Evaluation and Certification, CSEC, 2021-06-04, document version 33.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2021-06-07, document version 11.0

12.2 Documentation

APGUIDE Alcatel-Lucent Enterprise OmniAccess Stellar AP User Guide - AWOS 4.0.1, ALE USA Inc., 2020-10-21, version 033517-10 Rev. B

CCECG Common Criteria Evaluated Configuration Guide for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points, Bojie Xie, 2021-05-31, version 0.12

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

Version	Introduced	Impact of changes
1.25	2021-06-17	None
1.24.1	2020-12-03	None
1.24	2020-11-19	None
1.23.2	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	3.0	Demonstration of test coverage	Clarify demonstration of test coverage at EAL2.
SN-18	3.0	Highlighted Requirements on the Security Target	Clarifications on the content of the ST.
SN-22	3.0	Vulnerability Assessment	Vulnerability assessment needs to be redone if 30 days or more has passed between AVA and the final version of the final evaluation report.
SN-27	1.0	ST Requirements at the Time of Application for Certification	Expectations on the quality of the Security Target at the time of application for certification
SN-28	1.0	Updated procedures application, evaluation and certification	Evaluator reports should be received in two batches.