Reference: 2022-51-INF-4313- v1
Target: Pública
Date: 27.05.2025

Created by: CERT13
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2022-51**
TOE	**ZEN-D v1.2.14.15 + OpenVPN v2.4.4**
Applicant	**B99051385 - GRUPO SALLEN TECH SLU**
References	

[EXT-8143] 2022-11-29_2022-51_solicitud_certificacion

[EXT-8971] 2024-03-25_2022-51_ETR_v1.3

Certification report of the product ZEN-D v1.2.14.15 + OpenVPN v2.4.4, as requested in [EXT-8143] dated 29/11/2022, and evaluated by jtsec Beyond IT Security, S.L., as detailed in the Evaluation Technical Report [EXT-8143] received on 25/03/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product ZEN-D v1.2.14.15 + OpenVPN v2.4.4.

ZEN-D is cash deposit handling software, designed to give control over Sallén's cash deposit devices. Together with OpenVPN, ZEN-D provide customers with a secure remote management interface. The purpose of the TOE is to offer the user the possibility of making cash deposits in a secure manner. OpenVPN provides ZEN-D with the required implementations to deploy a secure VPN between the TOE and its management endpoints.

Developer/manufacturer: GRUPO SALLEN TECH SLU

Sponsor: GRUPO SALLEN TECH SLU.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: jtsec Beyond IT Security, S.L.

Protection Profile: none.

Evaluation Level: Common Criteria v3.1 R5 EAL2.

Evaluation end date: 23/04/2025

Expiration Date[1]: 23/05/2030

All the assurance components required by the evaluation level EAL2 have been assigned a “PASS” verdict. Consequently, the laboratory jtsec Beyond IT Security, S.L. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product ZEN-D v1.2.14.15 + OpenVPN v2.4.4, a positive resolution is proposed.

TOE SUMMARY

The TOE is composed of the modular software called ZEN-D and the OS service OpenVPNv2.4.4, which are embedded in the ARM board inside a safe manufactured by Sallén. ZEN-D is composed of a backend-frontend application and a set of drivers in charge of orchestrating the Sallén box

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

peripherals. These drivers are also embedded in the ARM board and are considered part of the ZEN-D application.

The OpenVPN service from the Operating System where ZEN-D software runs is considered a TOE component as it is in charge of providing the secure communication functionality. It communicates with CashControl Server and the remote users accessing by Remote Access functionality, in order to remotely manage the safe box by the ZEN-D software.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

- Security Audit:
  - FAU_GEN.1

  - FAU_GEN.2
  - FAU_SAR.1
  - FAU_SAR.3
  - FAU_STG.1
- User Data Protection:
  - FDP_ACC.1
  - FDP_ACF.1
- Identification and Authentication:
  - FIA_ATD.1
  - FIA_UAU.2
  - FIA_UID.2
- Security Management:
  - FMT_MOF.1/Modification
  - FMT_MOF.1/Determination
  - FMT_MSA.1
  - FMT_MSA.3
  - FMT_MTD.1
  - FMT_SMF.1
  - FMT_SMR.1
- TOE Access:
  - FTA_SSL.3
  - FTA_SSL.4
- Trusted Path/Channels:
  - FTP_ITC.1
  - FTP_TRP.1

IDENTIFICATION

Product: ZEN-D v1.2.14.15 + OpenVPN v2.4.4

Security Target: ZEN-D Security Target version 0.9 2024/02/06.

Protection Profile: none.

Evaluation Level: Common Criteria v3.1 R5, EAL2.

SECURITY POLICIES

The use of the product ZEN-D v1.2.14.15 + OpenVPN v2.4.4 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.4 Organizational Security Policies.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.5 Assumptions.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product ZEN-D v1.2.14.15 + OpenVPN v2.4.4, although the agents implementing attacks have the attack potential according to the Basic of EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.3 Threat Agents").

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 Security Objectives for the Operational Environment.

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE includes several security features. Each of the security features identified above consists of several security functionalities and are considered TOE Security Functionalities, as identified below.

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access
- Trusted Path/Channels

PHYSICAL ARCHITECTURE

The Target of Evaluation (TOE) includes the following components:

Delivery Item	Type	Description	Version	Delivery Method	Format
ZEN-D	Software	Software that is embedded in the ARM board, which is located inside the safe.	1.2.14.15	Is distributed as an application on the OS that comes on the ARM board. The board is distributed with the safe box and shipped by Courier delivery.	Embedded
SR120 Driver	Software	Driver used to operate the safe with peripherals, it is located inside	0.0.0.1	Is distributed as a binary file on the OS that comes on the ARM board.	Embedded

		the safe.		The board is distributed with the safe box and shipped by Courier delivery.	
OpenVPN	Software	OS service part of the TOE that implements the secure communication channels by OpenVPN protocol.	2.4.4	Is distributed as a binary file on the OS that comes on the ARM board. The board is distributed with the safe box and shipped by Courier delivery.	Embedded
Preparative Procedures	Preparative Documentation	Documents for the safe acceptance of the TOE and the installation and configuration process.	0.9	Microsoft SharePoint	PDF
Operational User Guidance	Guidance Documentation	Documents describing the safe use of the TOE.	0.8	Microsoft SharePoint	PDF

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- Preparative Procedures v0.9: documents for the safe acceptance of the TOE and the installation and configuration process.

- Operational User Guidance v0.8: Documents describing the safe use of the TOE.
- VPN configuration files.
- OS update package.
- Credentials for CashControl server.
- Document with SHA-256 digests of each document distributed.

PRODUCT TESTING

The independent testing approach has been testing all the SFRs declared in the Security Target, all the TSFIs declared in the Functional Specification and all the subsystems declared in the TOE Design.

Regarding the repetition of the developer's functional tests, the 54% of the tests have been repeated. The developer's functional tests are broken into three types corresponding to the interface tested: Touchscreen, Remote Access and CashControl. The evaluator has repeated all tests for Touchscreen and CashControl interfaces. The tests related to Remote Access interface was not repeated because the functionality provided is the same than the provided by Touchscreen interface, excluding the cash-related functionality that cannot be tested through Remote Access interface, and they only can be tested through the Touchscreen interface.

On the other hand, the vulnerability analysis approach has been based in:

- Search of public vulnerabilities for the TOE components and the third-party libraries used by the TOE.
- Search of public vulnerabilities for the OS where the TOE runs and for the SSH server of the OS where the TOE runs.
- Identification of possible vulnerabilities in the Security Target, Guidance documentation, Functional Specification, TOE Design and Security Architecture evidences.

Based on the vulnerabilities found, the evaluator calculated the attack potential and designed a test for each vulnerability with Basic attack potential.

EVALUATED CONFIGURATION

The TOE evaluated version is ZEN-D v1.2.14.15 + OpenVPN v2.4.4, and the evaluated configuration is:

- NTP is used to synchronize date and time through an external server. It is configured by default by the manufacturer.

- Login mode is set to default, which requires a user ID as mandatory. Through the security guidelines, a password is required for administrators.
- User roles have assigned the privileges that the application awards them by default.
- Disable firewall functionality is disabled (firewall is activated).
- Lock type is set to Smart Password, which requires an extra security code for performing CIT Collection.
- *Deposit inactivity time* is set by default to 120 (seconds).
- Machine *inactivity time* is set by default to 30 (seconds).
- Keep Alive period is set to 30 (seconds).
- Auto Cash Code is set to Manual.
- Transaction ID Format is set to Location ID + User + Timestamp.
- OpenVPN is correctly configured to connect with the remote management server.
- DOVE protocol is selected as the Cloud management protocol.
- *Downgrade application*, *Set new MAC* and *Reset Serial NO* functionalities are not allowed.
- Workflow modification is not allowed.

EVALUATION RESULTS

The product ZEN-D v1.2.14.15 + OpenVPN v2.4.4 has been evaluated against the Security Target ZEN-D Security Target version 0.9 2024/02/06.

All the assurance components required by the evaluation level EAL2 have been assigned a "PASS" verdict. Consequently, the laboratory jtsec Beyond IT Security, S.L. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The evaluation team makes the following security recommendations:

- To follow the security guidance's of the TOE strictly
- To keep the TOE under personal control and set all other security measures available from the environment.
- To periodically review the status of the certification of the underlying platform.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product ZEN-D v1.2.14.15 + OpenVPN v2.4.4, a positive resolution is proposed.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- **Target:** ZEN-D Security Target version 0.9 2024/02/06.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-

2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components selected.