Certification Dossier Code:	2020-4
Certification Report Creation Date:	31st July 2023
Certification Report Code:	2020-4-REP-58 (internal) 2020-4-REP-92 (public)
NASK RWA code:	OSiC.8711.4.2021

Certification Report

[2020-4] Certification Report on WIPERAPP EP EAL4 + ALC_FLR.1

COMMON CRITERIA

CERTIFICATE

NASK

Certification Identification: **2020-4** | Type of Product: **Other Devices and Systems**
Product Name and Version: **WIPERAPP EP WIPERAPP_CORE, software, version 3.4.0**

Target of Evaluation:

WIPERAPP EP WIPERAPP_CORE, software, version 3.4.0

Product Manufacturer: **WIPERAPP sp. z o.o., Wrocław, Poland** | Assurance Package: **EAL4 + ALC_FLR.1**

Name of Certification Body:

NASK National Research Institute, Standardisation and Certification Centre, Kolska 12, 01-045 Warsaw, Poland

Certification Report Identifier: **2020-4-REP-58**

PCA
POLSKIE CENTRUM AKREDYTACJI
CERTYFIKACJA WYROBÓW
AC 223

The IT Product identified in this certificate has been evaluated at an Evaluation Facility accredited and approved under the rules of the Polish IT Security Evaluation and Certification Scheme (PC1) using the Common Methodology for IT Security Evaluation, April 2017 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, April 2017 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and conjunction with the complete Certification Report. The evaluation has been conducted following the provisions of the IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by the NASK National Research Institute or any other organisation that recognises or gives effect to this certificate. No warranty of the IT Product by NASK National Research Institute or any other organisation that recognises or gives effect to this certificate is expressed or implied. The validity of the certificate may change over time. For information regarding the current status of the certificate, please contact NASK National Research Institute (Certification Body) or look at the NASK's website.

Certificate Identifier:
1/PC1/AC223/2023

Certificate issue date: 02.08.2023

Certificate expiry date: 02.08.2028

Signature:
Signed by / Podpisano przez: Paweł Krzysztof Kostkiewicz
Date / Data: 2023-08-02 22:42

NASK National Research Institute
Certification Body Manager

Podpisany elektronicznie przez
NASK - PIB
11.06.2025
10:14:12 +02'00'

Table of content

1. Introduction

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been tested at an approved Laboratory (IT Security Evaluation Facility) – on the basis of the IT Security Evaluation and Certification Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. This certification report, and its associated certificate, applies only to the identified version and release of the product in its tested and evaluated configuration. The evaluation has been conducted in accordance with the provisions of the IT Security Evaluation and Certification Scheme - PC1, and the conclusions of the Laboratory in the technical evaluation report are consistent with the evidence. This report, and its associated certificate, are not an endorsement of the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration.

2. Certification overview

The NASK's "IT Security Evaluation and Certification Scheme" provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by an approved Laboratory under the oversight of the Certification Body, which is managed by the NASK National Research Institute. Laboratory is a commercial facility that has been approved by the Certification Body to perform Common Criteria based cybersecurity evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2018- The General Requirements for the Competence of Testing and Calibration Laboratories. By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. **The consumer of certified IT products should review the Security Target, in addition to this Certification Report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the Laboratory**. The Certification Report, Product Certificate and Security Target are posted to the Certified Products List for the IT Security Evaluation and Certification Scheme published by NASK National Research Institute.

Recognition of the certificate

European Recognition of 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 up to EAL4. A higher recognition levels are provided for IT-Products related to certain SOGIS Technical Domains only.

The current list of signatory nations and approved certification schemes can be found on https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. This certificate is recognized under SOGIS-MRA up to EAL4.

International Recognition of CC Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the Common Criteria (Common Criteria Recognition Arrangement, CCRA-2014) became effective in September 2014. It covers Common Criteria certificates based on: collaborative Protection Profiles, assurance components up to EAL2 augmented by ALC_FLR and certificates for PP and cPP.

The current list of signatory nations and of collaborative Protection Profiles can be found on https://www.commoncriteriaportal.org .

The CCRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition. This certificate is recognized under CCRA-2014 up to EAL2 augmented by ALC_FLR.

Executive Summary

This document constitutes the Certification Report for the certification file of the product: **WIPERAPP EP WIPERAPP_CORE**

TOE Version:	3.4.0
Developer:	WIPERAPP sp. z o.o.
Sponsor:	Project co-financed from the NCBiR national programme „Cybersecurity and e-Identity" in other words the KSO3C project
Security Target:	SECURITY TARGET LITE FOR WIPERAPP_CORE, version 1.1, date of issue 2025-06-02
Protection Profile:	None
Laboratory/ITSEF:	Sieć Badawcza Łukasiewicz - Instytut Technik Innowacyjnych EMAG

Evaluation Level:	Common Criteria version 3.1 release 5, Evaluation Assurance Level EAL4+ALC_FLR.1
Evaluation end date:	March 2023 (Final ETR ver. 2.1, issue date 31.03.2023)
Expiration Date:	02/08/2028

All the assurance components required by the evaluation level EAL4+ALC_FLR.1 of Common Criteria standard have been evaluated and obtained a "PASS" verdict. Consequently, the laboratory assigned the "PASS" VERDICT to the whole evaluation due to the fact that all the evaluation requirements are satisfied for the EAL4+ALC_FLR.1, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5. Considering the Developer's evidence submitted during the Certification Process of the product WIPERAPP EP WIPERAPP_CORE, version 3.4.0 and ITSEF's reports validated by the CB, a positive resolution by Certification Body is proposed.

Documentation available for users

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

[EXT-1055] [EVD-ST_PUB-V1.8.1]	**Security Target for WIPERAPP EP WIPERAPP_CORE version 3.4.0, v1.8.1, issue date 07.07.2023 (confidential document)**
[EXT-950] [EVD-AGD_OPE-V1.8]	**User's Manual, v. 1.8, issue date 05.05.2022 (confidential document)**
[EXT-949] [EVD-AGD_PRE-V1.8]	**Installation manual, v. 1.8, issue date 05.05.2022 (confidential document)**
[EXT-926] [EVD-UG-V1.3]	**Wiperbox User Manual, Rev. 1.3, issue date 31.01.2023**

Security Target

Along with this certification report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

WIPERAPP_CORE Security Target, version 1.8.1, issue date 07.07.2022

The public version of this document is the same as complete Security Target described above and it is published along with this certification report on the Certification Body website.

3. TOE Summary

TOE Overview

The Target of Evaluation (TOE) is the WIPERAPP_CORE software (part of WIPERAPP solution) together with the WIPERAPP_CONF configuration file necessary for the correct operation of WIPERAPP_CORE.

The TOE is not available to the end user as a separate, stand-alone program. The TOE is part of the WIPERAPP application (set of modules) and the only possible contact and interaction of the end-user with the TOE may be through the WIPERAPP application only. WIPERAPP is a software solution for permanent and irreversible erasure of data from data drives.

The main goal of the application is to protect data against unauthorized access and against the disclosure of data saved on drives which are to change their intended use.

WIPERAPP_CORE, which is the Target of Evaluation (TOE), is responsible for the following:

- identifying the specifications of the device on which it was launched,
- identifying data drives connected to the device in order to delete data from them,
- wiping information from the data drives according to the wiping algorithm selected by the user-operator,
- basic verification of the accuracy of the process of erasing data from the drives,
- Creation, collection, cryptographic protection and export of data, which are indispensable to generate a report (certificate) confirming that the data have been erased.

The TOE is composed of four modules:

- DETECT - the function of the detection module is to identify the device on which the TOE was launched to which the drives whose data are to be erased were connected. The following data of the device are identified: manufacturer, model, serial number, capacity of RAM memory, processor type.
- WIPE - module for data erasure from drives. This allows to gain access to the whole user-accessible space of the drive detected in the DETECT module.
- VERIFY - the TOE has a function that ensures basic verification of the data erasure process accuracy. The verification process lies in reading the whole space of the drive and comparing the contents of all read sectors with expected values that should be placed in the drive sectors after the data are deleted.
- REPORTER – module for generating report data. These data are used to generating WIPE REPORT (WIPE CERTIFICATE) document.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4+ ALC_FLR.1, according to Common Criteria v3.1 Revision 5.

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC.FLR.1 Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definitione
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definitione
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Security Functional Requirements

Functional requirement	Description
FCS: Cryptographic support	FCS_COP.1 Cryptographic operation
FDP: User Data Protection	FDP_RIP.1 Subset residual information protection
FAU: Security audit	FAU_GEN.1 Audit data generation
	FAU_SAA.1 Potential violation analysis
	FAU_ARP.1 Security alarms
FPT: Trusted path/channels	FPT_TST.1 TSF testing

Functional requirement	Description
	FPT_ITI.1 Inter-TSF detection of modification

Identification

Product: WIPERAPP EP WIPERAPP_CORE, software, version 3.4.0

Security Target: WIPERAPP_CORE Security Target, version 1.8.1, issue date 07.07.2022

Security Policy

Security audit

The TOE implements the mechanism to collect and report the audit records of the data wiping process, which are indispensable to generate a report (certificate) confirming that the data have been erased.

Cryptographic Support

The TOE is performing the cryptographic hash function using SHA-512 algorithm to protect the audit data generated during the wiping process which finally exported outside the TOE.

User Data Protection

The TOE provides the residual information protection providing the mechanism ensuring that the storage information is unavailable on the devices being the subject of the successful erasure process. The data erasure is performed using the data erasure algorithms which are listed in the Table 5 of the Security Target.

Trusted Path/Channels

The TOE runs a suite of self-tests after completion the erasure process to demonstrate the correct operation of the wiping process. Additionally, the TOE provides the capability to detect modification of the data transferred outside of the TOE. It is realized by SHA512 hash generation which is attached to the information collected during erasure process. This mechanism allows to verify the integrity of the transmitted data.

4. Assumptions and Clarification of Scope

The assumptions are constraints to the conditions used to assure the security properties and functionalities introduced by the Security Target. All assumptions are to be taken into consideration when calculating the attack potential and affect the vulnerability of the product (mostly in terms of reduction). In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its usage and 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. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

Usage Assumptions

The Security Target contains two assumptions related to the usage of the TOE:

A.USERS: The administrator and users-operators of the system shall be competent people, i.e. they have been trained to use the WIPERAPP application in the ranges corresponding to the functions (roles) they have in the process of data erasure by means of this application.

A.NOEVIL: The administrator and users-operators shall not be irresponsible people who would deliberately cause negligence.

Environmental Assumptions

The Security Target makes six assumption on the operational environment of the TOE:

A.TIME: The TOE environment shall provide reliable timestamps that will be used by the TOE for its operation and reporting.

A.BIOS_SETTINGS: The BIOS settings of the clients in which the TOE will run shall be properly configured so that they allow the correct recognition and wiping data from the media intended for data erase. The device in which the TOE will run shall support booting from LAN (booting from a PXE server.

A.LOCATION: Both, the client in which the TOE runs and the WIPERBOX shall be located in secure facilities with controlled access so that no access rights are given to unauthorized or accidental users or persons.

A.KERNEL: All operating system kernel modules and libraries used by the TOE to communicate with data wiping media shall be from official authorized repositories (sources), stable, and will be included in accordance with the TOE addition or replacement procedure.

A.COMMUNICATION: It is assumed that the connection between the WIPERBOX and the client where the TOE runs is protected so that no attackers can access to it and try to

disclose or modify the flow of information. In addition, the communication shall be done using cryptographic protected protocols.

A.RELIABLE_MEDIUM_BEHAVIOUR: Customer organization ensure that disk identifiers and technical parameters are protected against their counter fight before their wiping by applying the procedural means.

Clarification of Scope

Threats

The Security Target defines four threats which have been taken into consideration during the evaluation process.

T.DISK_IDENTITY: The serial number of the device to be wiped is not correct due to either an intentional modification made by S.ATTACKER or to natural damage (e.g. wearing out of the magnetic surface or semiconductor structure) which makes the TOE performing an incorrect identification of the device.

If the TOE does not detect the modification of the serial number, it may lead to the generation of an incorrect report confirming the wiping and D.PROTECTED_DATA may remain partially or completely unwiped, which may result in unauthorized and uncontrolled disclosure.

T.BAD_SECTOR: "Bad sector" flags are set in the device by either S.ATTACKER or due to normal medium operation (e.g. wearing out of the magnetic surface or semiconductor structure) which makes the TOE identify them as bad sectors and not securely wipe them.

If the TOE does not detect the modification made by S.ATTACKER, it may lead to the generation of an incorrect report confirming the wiping and D.PROTECTED_DATA may remain partially or completely unwiped (in particular the information contained in the marked bad sectors), which may result in unauthorized disclosure.

T.CONNECTION: Any subject impersonates the WIPERBOX server and/or: (1) makes the client in which the TOE is supposed to run boot a non-legit OS with a non-legit TOE without detection. The user of the TOE would be under the impression that the data wiping of the storage device was correctly finished, which may result in unauthorized disclosure (2) modifies the data sent to the WIPERBOX from the TOE after a wiping process without being detected

T.BAD_USE: S.USER or S.ADMIN perform a bad use of the TOE, forcing it to work incorrectly by generating fake reports.

OSPs

Additionally The Security Target contains three Organisational Security Policies (OSPs).

OSP.WIPE: The TOE must wipe the data contained in the target storage device using any of the algorithms included in "Table 5 Data erasure algorithms available in WIPERAPP_CORE"

OSP.REPORT: The TOE must collect all audit data of the wipe process, encapsulate it, and generate a SHA-512 digest of it in order to transmit them to third IT entities for its integrity verification and report generation. Timestamps of wipe process, generated by TOE, must be reliable.

OSP.VERIFICATION: The TOE must verify the data written in the storage media after a wiping process for confirming that the erasure algorithm has worked properly.

5. Architectural Information

Physical scope

The Target of Evaluation (TOE) is a software called WIPERAPP_CORE together with the WIPERAPP_CONF configuration file necessary for the correct operation of WIPERAPP_CORE.

It is a software designed to securely and irreversibly erase data from storage devices such as HDDs, SSDs, USB drives, and memory cards. The TOE includes four main security modules: DETECT (device/media identification), WIPE (data erasure), VERIFY (verification of erasure), and REPORTER (audit and reporting). The TOE runs in a dedicated Linux-based environment provided by WIPERBOX.

A WIPERBOX device is delivered to the customer along with a short user manual printed (the full version of the user manual is available via the website in HTML web format). The WIPERBOX device is a minimum requirement computer acting as a server that hosts the WIPERAPP application image of which the TOE (WIPERAPP_CORE) is part.

WIPERAPP_CORE and WIPERAPP_CONF are loaded together with the WIPERAPP application (TOE environment element), from the server - WIPERBOX device (TOE environment element), via the LAN network interface to RAM memory of the device (TOE environment element), to which the data mediums to be erasure are connected. The application then runs on that device from RAM.

Logical scope

The TOE is WIPERAPP_CORE, software designed to securely and irreversibly erase data from storage devices such as HDDs, SSDs, USB drives, and memory cards. The TOE includes four main security modules: DETECT (device/media identification), WIPE (data erasure), VERIFY (verification of erasure), and REPORTER (audit and reporting). The TOE runs in a dedicated Linux-based environment provided by WIPERBOX. Proprietary technical details of implementation and configuration files are not included in this version.

The logical scheme of the WIPERAPP_CORE is presented in Figure 1.

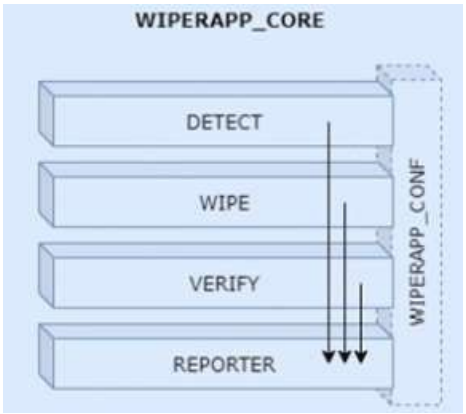

Figure 1. Logical scheme of WIPERAPP_CORE

6. Product Documentation

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

[EXT-1055]	**Security Target for WIPERAPP EP WIPERAPP_CORE version 3.4.0, v1.8.1, issue date 07.07.2023 (confidential document – LITE version available)**
[EXT-950]	**User's Manual, v. 1.8, issue date 05.05.2022**
[EXT-949]	**Installation manual, v. 1.8, issue date 05.05.2022**
[EXT-926]	**Wiperbox User Manual, Rev. 1.3, issue date 31.01.2023**

Security Target

Along with this Certification Report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

WIPERAPP_CORE Security Target, version 1.8.1, issue date 07.07.2022

The public version of this document is a sanitized subversion of complete Security Target described above and it is published along with this Certification Report on the Certification Body website.

7. IT security evaluation

Evaluated Configuration

The WIPERBOX device works with a target computer in the following architecture: Wiperapp server (WIPERBOX) – Client network (computer with data erasure media) is presented in figure 2.

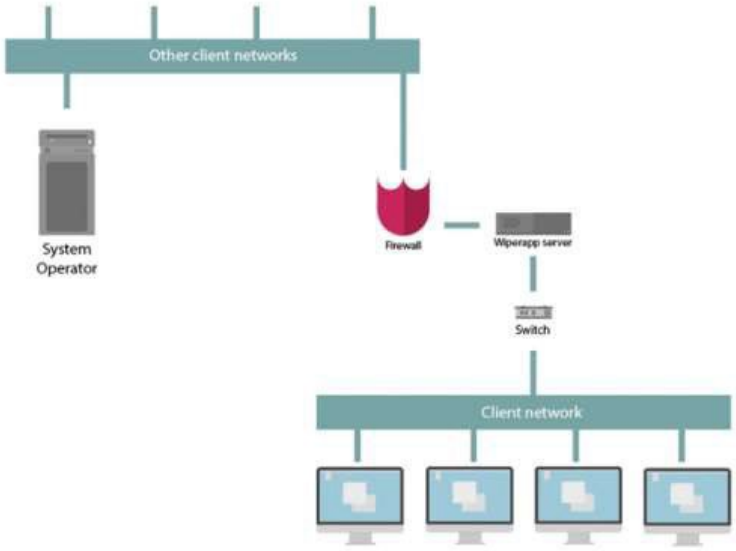

Figure 2. The topology of network connections.

The WIPERBOX device operates as a server and provides distribution of the software packages which are uploaded and installed in the RAM memory of the target computer (client). The package consists of elements which constitute the TOE environment elements (WIPERAPP application and Debian 10 Buster operating system with the required libraries necessary for the operation of WIPERAPP application) as well as the WIPERAPP_CORE (the TOE itself) which is the part of the WIPERAPP application, The constitute only the environment of the TOE. The data storage devices (intended for the data erasure) connected to the target computer, are not either part not part of the TOE nor its environment. The specification of the minimum requirements for the TOE environment could be found in the paragraph 1.3.3 of the Security Target.

The test configuration used by the ITSEF to perform the tests is presented on the figure 3.

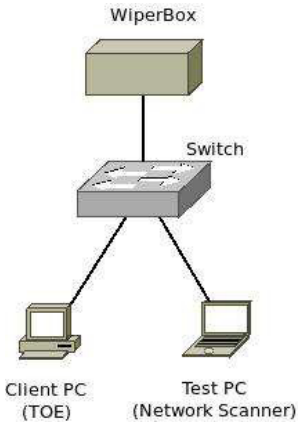

Figure 3. The test bed

The configuration of the test bed used by the Evaluators consists of the following elements:

1. Client computer - HP Compaq 6200 PRO MT PC (as client machine):
   - Processor: Intel(R) Core i3-2100 3.10GHz
   - RAM memory: 4096 MB DDR3 / 1333MHz
   - Graphical card – integrated
2. WIPERBOX Server,
3. Laptop DELL Latitude 3490 as client machine,
4. Laptop DELL Vostro 3360 as testing tool (network scanner),
5. smart-phone Xiaomi Mi 11 Lite 5G as wireless blue-tooth scanner.

To provide the erasure tests the following set of the storage devices was used by the Evaluators:

- HDD Seagate 7200.7 80 GB, model: ST380011A,
- HDD Western Digital Raport 80 GB, model: WD800ADFS-75SLR2,
- HDD Western Digital Caviar 80 GB, model: WD800JB-00FMA0,
- HDD Seagate 200GB, model:ST9200423AS,
- SSD Lite-On 128 GB,
- HDD Western Digital 120 GB, model: WD1200BEVT-75ZCT2,
- SSD Samsung 128 GB, model: SM481N,
- HDD Seagate 80 GB model: ST380815AS.

Functional testing

The Evaluation Assurance Level EAL 4 requires the Developer to devise and conduct the complete set of tests covering all TSFIs and interactions between subsystems of the TOE. The Evaluator's task is divided int two activities. The Evaluators shall confirm the Developer's tests results using the sampling strategy described in details by the Common Criteria methodology. Additionally, the Evaluator's task is to devise and perform their own subset of tests which are intended to be the supplementary for the tests prepared by the Developer.

Developer testing

The Developer's testing covers all TSFIs and their security functional behaviour. As the TOE consists of the only one subsystem the interactions between subsystems were not the subject of tests.

The Developer prepared 43 tests which are divided into two groups: 11 unit tests dedicated for testing TOE interfaces and 32 functional tests are connected with the usage of the TOE.

All the 43 test cases have obtained a PASS verdict.

Evaluator testing

The Evaluator decided to repeat all functional tests delivered by the Developer. The positive results of the Developer's tests were confirmed by the Evaluators.

Additionally the Evaluators independently devised and conducted 16 test cases.

The main objective of the tests performed by the Evaluators was to check that the security functional requirements are implemented as expected and that the TSFIs definitions are consistent with the TOE. The Evaluator's independent test plan was SFR oriented, and the functionality of each SFR included at the Security Target has been considered. The independent tests plan covered the whole TOE functionality: all the SFRs have been tested through their TSFIs.

All the 16 test cases have obtained a PASS verdict.

Penetration testing

The attack potential used for this evaluation is consistent with AVA_VAN.3: Enhanced-Basic attack potential. The developed test plan was based on vulnerability survey of the evaluation evidence as well as the information available in the public domain is performed by the Evaluator to ascertain potential vulnerabilities that may be easily found by an attacker. TOE configuration used to execute the penetration test plan was consistent with the evaluated configuration according to the Security Target. The intention of the vulnerability analysis is to determinate if there are faults or weaknesses of the TOE that can be exploited in the operational environment. The vulnerability analysis focus in following points of interest break the auto protection of TSF using tampering, break the isolation of TSF domain mean direct attack or monitoring direct attacks or TSF monitoring and TSF bypass.

The evaluation of documentation analysis as well as the public vulnerability research resulted in the identification of 6 potential vulnerabilities not mitigated by the assumptions for the

environment and having attack potential corresponding to the TOE evaluation level (EAL4). All of these vulnerabilities were considered for penetration tests.

The penetration tests resulted with FAIL verdict, which is the proof for the resilience of the product and fulfilment of the assumptions of the Security Problem Definition.

After providing all planned tests the Evaluator concluded that there were not exploitable vulnerabilities according to the scope of this evaluation.

Evaluation verdicts

The Evaluators applied each work unit of the Common Methodology [CEM31] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target for an attack potential Enhanced-Basic.

The Certifier reviewed the work of the Evaluator and determined that the evaluation was conducted in accordance with the Common Criteria.

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

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Validation
ADV: Development	ADV_ARC.1 Security architecture description	PASS	CONFORMANT
	ADV_FSP.4 Complete functional specification	PASS	CONFORMANT
	ADV_IMP.1 Implementation representation of the TSF	PASS	CONFORMANT
	ADV_TDS.3 Basic modular design	PASS	CONFORMANT
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS	CONFORMANT
	AGD_PRE.1 Preparative procedures	PASS	CONFORMANT
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	PASS	CONFORMANT
	ALC_CMS.4 Problem tracking CM coverage	PASS	CONFORMANT
	ALC_DEL.1 Delivery procedures	PASS	CONFORMANT
	ALC_DVS.1 Identification of security measures	PASS	CONFORMANT
	ALC_LCD.1 Developer defined life-cycle model	PASS	CONFORMANT
	ALC_TAT.1 Well-defined development tools	PASS	CONFORMANT
	ALC.FLR.1 Basic flaw remediation	PASS	CONFORMANT
ASE: Security	ASE_CCL.1 Conformance claims	PASS	CONFORMANT

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Validation
Target evaluation	ASE_ECD.1 Extended components definition	PASS	CONFORMANT
	ASE_INT.1 ST introduction	PASS	CONFORMANT
	ASE_OBJ.2 Security objectives	PASS	CONFORMANT
	ASE_REQ.2 Derived security requirements	PASS	CONFORMANT
	ASE_SPD.1 Security problem definition	PASS	CONFORMANT
	ASE_TSS.1 TOE summary specification	PASS	CONFORMANT
ATE: Tests	ATE_COV.2 Analysis of coverage	PASS	CONFORMANT
	ATE_DPT.1 Testing: basic design	PASS	CONFORMANT
	ATE_FUN.1 Functional testing	PASS	CONFORMANT
	ATE_IND.2 Independent testing - sample	PASS	CONFORMANT
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis	PASS	CONFORMANT

Evaluator Comments/Recommendations

Recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and shall to be considered when using the product.

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the Security Target.

8. Certifier Recommendations

All the assurance components required by the evaluation level EAL4+ALC_FLR.1 of Common Criteria standard have been evaluated and obtained a “PASS” verdict. Consequently, the laboratory assigned the “PASS” VERDICT to the whole evaluation due to the fact that all the evaluation requirements are satisfied for the EAL4+ALC_FLR.1, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5.

Considering the Developer's evidence submitted during the Certification Process of the product WIPERAPP EP WIPERAPP_CORE, version 3.4.0 and ITSEF's reports validated by the CB, **a positive resolution is proposed by the Certifier**.

9. Acronyms

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
CB	Certification Body
TOE	Target Of Evaluation

10. Bibliography

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

1. [CC31p1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5
2. [CC31p2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5
3. [CC31p3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5
4. [CEM31] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology, Version 3.1 Revision 5

References

List of normative documents:

SOG-IS MRA Mutual Recognition Agreement of Information Technology Security Evaluation Certificates

CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security

CC Common Criteria for Information Technology Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security

ISO/IEC 17025 General requirements for competence of calibration and testing laboratories

ISO/IEC 17065 Conformity assessment – Requirements for bodies certifying products, processes and services

ISO/IEC 18045 Information technology – Security techniques – Methodology for IT security evaluation

ISO/IEC 19790 Information Technology – Security Techniques – Security requirements for cryptographic modules

ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements

PC1 IT Security Evaluation and Certification Scheme

List of related documents

[EXT-928] [FIN-ETR-V2.1]	**Final Evaluation Technical Report for WIPERAPP EP WIPERAPP_CORE, v2.1, issue date 31.03.2023 (ITSEF confidential document)**
[EXT-1055] [EVD-ST_PUB-V1.8.1]	**Security Target for WIPERAPP EP WIPERAPP_CORE version 3.4.0, v1.8.1, issue date 07.07.2023 (confidential document)**
[EXT-1350] [EVD-ST-LITE-V1.1]	**Security Target Lite for WIPERAPP EP WIPERAPP_CORE version 3.4.0, v1.1, issue date 02.06.2025**
[EXT-929] [TR-ATE_IND-V1.5]	**WIPERAPP EP WIPERAPP_CORE Independent Test Plan and Report, v. 1.5, issue date 09.02.2023 (ITSEF confidential document)**