Certification Report

Youwipe Erasure Tool 4 with WipeCenter 4

Sponsor and developer:	***AllWipe Ltd*** **Pyväntölahdentie 4** **81120 Katajaranta** **Finland**
Evaluation facility:	***Secura B.V.*** **Karspeldreef 8** **1101 CJ AMSTERDAM** **The Netherlands**
Report number:	**NSCIB-CC-0114526-CR**
Report version:	**1**
Project number:	**0114526**
Author(s):	**Denise Cater**
Date:	**12 August 2020**
Number of pages:	**11**
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Youwipe Erasure Tool 4 with WipeCenter 4. The developer of the Youwipe Erasure Tool 4 with WipeCenter 4 is AllWipe Ltd located in Katajaranta, Finland and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE consists of two main components Youwipe Data Erasure Tool (further referred to as Youwipe tool) and WipeCenter report management application (further referred to as WipeCenter application).

The Youwipe tool is performing the secure erasure actions (in line with the selected standard), as well as verification of erasure results and issuing of the erasure report. The Youwipe tool includes all the tools and drivers needed for its interaction with other hardware elements on the host machine.

The WipeCenter application is responsible for regulating the access to the generated erasure reports. The application allows users to read or delete erasure reports stored on a local server.

The TOE has been evaluated by Secura B.V. located in Amsterdam, The Netherlands. The evaluation was completed on 12 August 2020 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Youwipe Erasure Tool 4 with WipeCenter 4, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Youwipe Erasure Tool 4 with WipeCenter 4 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provides sufficient evidence that the TOE meets the EAL3 augmented (EAL3+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Youwipe Erasure Tool 4 with WipeCenter 4 from AllWipe Ltd located in Katajaranta, Finland.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Youwipe	4.1.48
	WipeCenter	4.0.43

To ensure secure usage a set of guidance documents is provided together with the Youwipe Erasure Tool 4 with WipeCenter 4. Details can be found in section 2.5 of this report.

2.2 Security Policy

The Youwipe tool is responsible for:

- Generation of the random numbers used in the data erasure process;
- Data erasing of the target device, based on the selected erasure standard or methodology;
- Data erasure verification on the target device;
- Audit data collection for the generation of the erasure report;
- Erasure report generation and delivery (including saving the report on either an USB drive or the local server, as well as hashing the report to ensure its integrity).

The erasure standards chosen for evaluation are:

- EXT. HMG Infosec High for HDD, SDD, Flash drives, SD cards;
- Infosec High for Android devices;
- Cryptographic Erasure for iOS devices.

The WipeCenter application is responsible for:

- Enforcing authentication for the access of erasure reports generated by the Erasure Engine of Youwipe, while at the same time collecting information about modifications to existing users and failed authentication attempts;
- Ensuring role separation in the access of erasure report (separation between read-only rights and read-only + delete rights);
- Retrieving the erasure report from the local server and verifying its integrity;
- Deleting erasure reports from the local server;
- Generating new passwords for existing users.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 3.4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The following security features are not included in the TOE:

- Booting of the Youwipe solution;
- Booting of the WipeCenter application.
- The only erasure standards included in the evaluation are:
  - EXT. HMG Infosec High for HDD, SDD, Flash drives, SD cards;
  - Infosec High for Android devices;
  - Cryptographic Erasure for iOS devices

2.4 Architectural Information

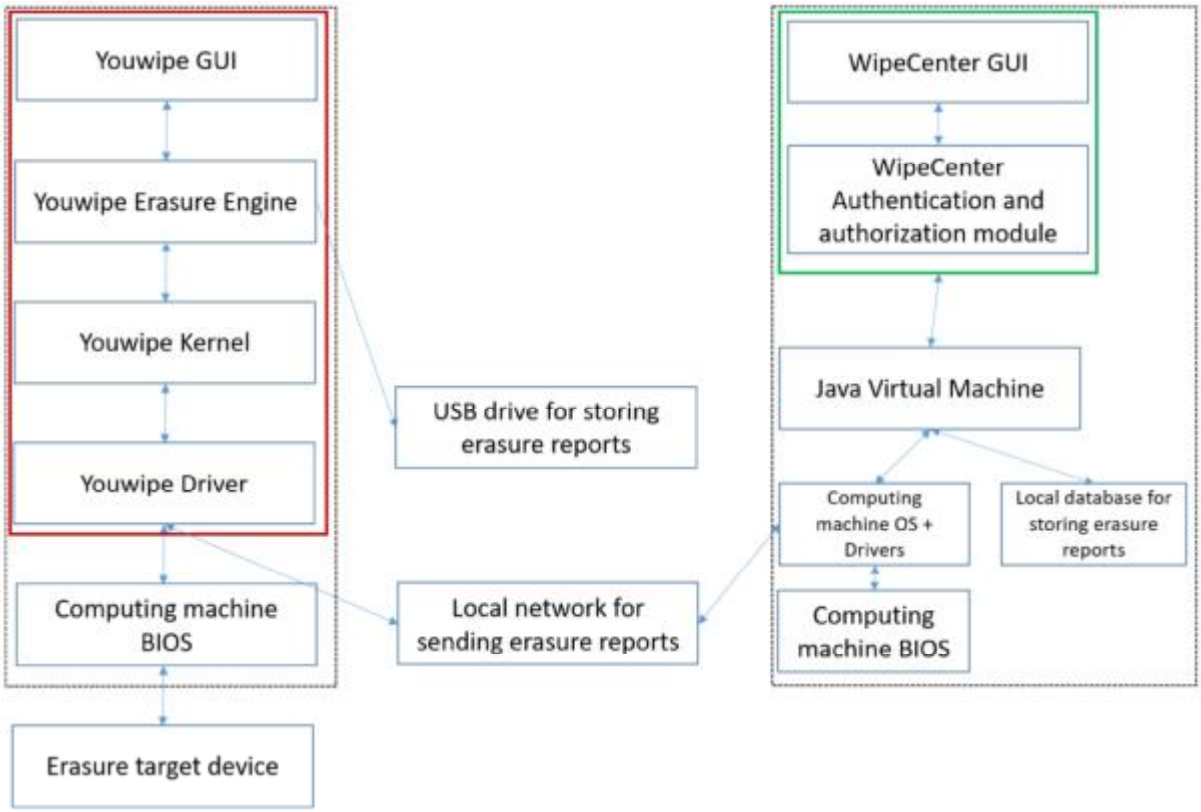
The Youwipe tool interacts with the other environmental components as follows:

- The Youwipe tool interacts (via the driver) with the target media for erasure;
- The Youwipe tool interacts (via the driver) with the BIOS of the host machine;
- The Youwipe tool interacts with the external USB drive or server in order to save the generated erasure report.

The WipeCenter application with the other environmental components as follows:

- The WipeCenter application interacts with the Java Virtual Machine on the host machine in order to access the local machine BIOS, database or network connection (for importing erasure reports).

The interactions between TOE components and the environmental components are defined in the diagram below. The TOE components are marked in the red (Youwipe) and green (WipeCenter) boxes.



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Youwipe Erasure Tool User Manual	2.0.6
WipeCenter User Manual	2.0.5

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed testing against the functional specification, covering all TSFI and (implicitly) all subsystems. The developer testing included both positive and negative test cases.

For the testing performed by the evaluators, the developer has provided a test environment. The evaluators have reproduced a selection of (14) the developer tests, selected based on the following criteria:

- Criticality of the tests;
- Depth of provided test evidence.

The evaluator designed (5) additional test cases to further investigate some areas of functionality.

2.6.2 Independent Penetration Testing

AVA testing was performed in the following steps:

- Analysis of publicly known vulnerabilities (initial research with Google for each of the components of the TOE, followed by research within the CVE database and research within the web-site of the component's developer);
- Attempting to exploit identified applicable publicly known vulnerabilities;
- Performing additional independent testing based on the developed test plan of (18) penetration test cases.

A total of 32 days testing effort was applied to the logical testing, of which 25 days were spent on penetration testing.

2.6.3 Test Configuration

The test configuration used was in accordance with the evaluated configuration, using the following components:

- Data Eraser Tool;
- PC Hard drive x2
- SSD
- USB
- Android phone – Samsung A10
- iPHONE 5S

All tests were performed on the initially supplied versions (WipeCenter version 4.0.32, YouWipe version 4.1.41), with as exceptions:

- Tests which resulted in an update being issued were repeated on the updated version to verify correctness and sufficiency of the patch;

- Tests that cover TSFI that may unwillingly be impacted by changes made to other components in order to address (seemingly unrelated) issues in the TOE.

In addition to basic Ubuntu system utilities (grep, strings, awk, base64, curl, tar, openssl, nc, etc.), a number of specialised tools were used throughout the technical part of this evaluation, including forensic, web application assessment, network assessment and reverse engineering tools.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Re-used evaluation results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Youwipe Erasure Tool 4 with WipeCenter 4.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references a ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Youwipe Erasure Tool 4 with WipeCenter 4, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

3 Security Target

The Common Criteria Security Target for YouWipe Erasure Tool 4 with WipeCenter 4, version 6.0, 30 July 2020 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Evaluation Technical Report Youwipe Erasure Tool 4 with WipeCenter 4, Version 1.3, 05 August 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST] Common Criteria Security Target for YouWipe Erasure Tool 4 with WipeCenter 4, version 6.0, 30 July 2020.

(This is the end of this report).