Certification Report

YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0

Sponsor and developer: ***AllWipe Oy Ltd.***
Pyväntölahdentie 4
81120 Katajaranta
Finland

Evaluation facility: ***Secura B.V.***
Herikerbergweg 15
1101 CN Amsterdam
The Netherlands

Report number:	**NSCIB-CC-2500035-01-CR**
Report version:	**1**
Project number:	**NSCIB-2500035-01**
Author(s):	**Brian Smithson**
Date:	**08 September 2025**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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, TrustCB 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 TrustCB 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 TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence 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, TrustCB 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, 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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

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

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0. The developer of the YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0 is AllWipe Oy 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 Console report management application (further referred to as WipeCenter application).

The Youwipe tool performs secure erasure actions in accordance 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 2025-09-08 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 Data Erasure Tool 5.0 and WipeCenter Console 5.0, 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 Data Erasure Tool 5.0 and WipeCenter Console 5.0 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 provide 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 (Basic Flaw Remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM:2022 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 *[CC]*.

TrustCB 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. Note that the certification results apply only 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 available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0 from AllWipe Oy Ltd. located in Katajaranta, Finland.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Software	YouWipe	5.0
Software	WipeCenter	5.0

To ensure secure usage a set of guidance documents is provided, together with the YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0. For details, see section 2.5 “Documentation” 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 drivers, SD cards;
- Infosec High for Android devices;
- Cryptographic Erasure for iOS devices.

The WipeCenter console 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.

The following security features are not included in the TOE:

- Booting of the Youwipe solution;
- Booting of the WipeCenter application.

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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see 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

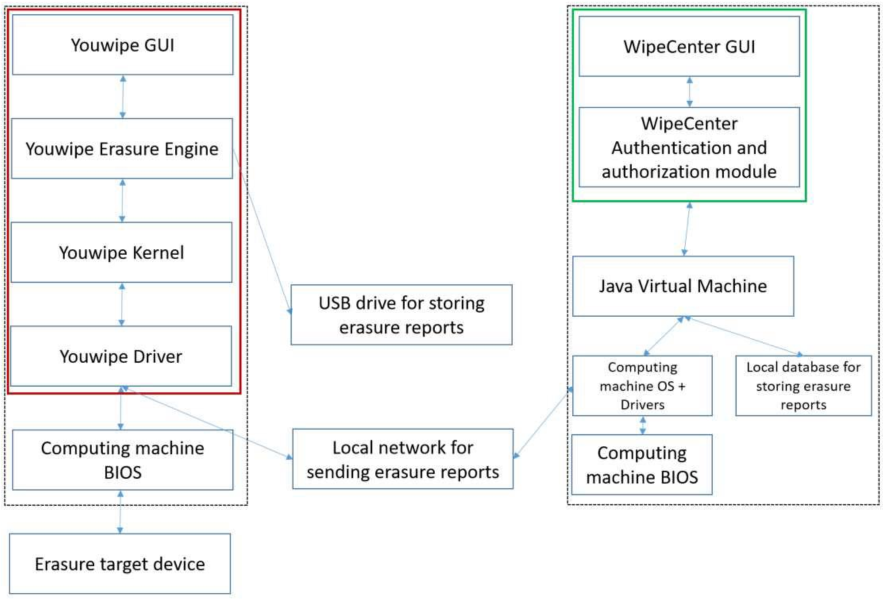
The Youwipe tool interacts with the other environmental components as follows:

- 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.


Youwipe GUI
Youwipe Erasure Engine
Youwipe Kernel
Youwipe Driver
Computing machine BIOS
Erasure target device
USB drive for storing erasure reports
Local network for sending erasure reports
WipeCenter GUI
WipeCenter Authentication and authorization module
Java Virtual Machine
Computing machine OS + Drivers
Local database for storing erasure reports
Computing machine BIOS

2.5 Documentation

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

Identifier	Version
Youwipe Erasure Tool & WipeCenter Version 5.0 User Manual	V2.0.0

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

For ATE testing the following test approach was implemented:

- Several developer tests were repeated];
- Additional tests developed by the evaluator were performed.

The repeated tests were selected based on the following criteria

- Criticality of the tests;

Depth of provided test evidence.

2.6.2 Independent penetration testing

AVA testing was performed in the following steps:

- Analysis of publicly known vulnerabilities;
- Attempting to exploit identified applicable publicly known vulnerabilities;
- Performing additional independent testing based on the developed test plan presented in [7].

The following approach was implemented for the research of publicly known vulnerabilities:

- Initial research with Google for each of the components of the TOE;
- Research within the CVE database;

Research within the web-site of the component's developer

2.6.3 Test configuration

Since no direct physical hardware interfacing is required for the TOE (DET part) to operate (e.g. low-level USB functions are not used), it allows for virtualization of the test setup in VMware.

Virtualized setup was used throughout this evaluation to maximize effective testing (memory analysis, snapshot management, virtual networking, portability). Virtualized setup validated functionally with the physical setup considering expected operation of 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.

2.6.4 Test 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 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an 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 Data Erasure Tool 5.0 and WipeCenter Console 5.0, to be **CC Part 2 conformant, 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 “Documentation” 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 must 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. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <**none**>, which are out of scope as there are no security claims relating to these.

3 Security Target

The Common Criteria Security Target for YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0, v7.0, 26 February 2025 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

CM	Configuration Management
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerability Enumeration
DET	Data Erature Tool
GUI	Graphical User Interface
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
PXE	Preboot Execution Environment
RNG	Random Number Generator
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 1 to 5, CC:2022 Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[ETR]	EVALUATION TECHNICAL REPORT YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0, v1.0, 18 August 2025
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Common Criteria Security Target for YouWipe Data Erasure Tool 5.0 and WipeCenter Console 5.0, v7.0, 26 February 2025

(This is the end of this report.)