A Certification Body of atsec information security AB
under the EUCC scheme

Certification Report - Blancco File Eraser

Certification ID EUCC-3089-2026-001

Certification Body ID 3089

Version 1.0

Author David Hedberg

atsec information security AB
Svärdvägen 23
SE-182 33 Danderyd
Phone: +46 8 55 110 400
www.atsec.com

The objective of the certification report is to provide detailed and practical security information about the ICT product or protection profile for any interested parties. The report does not contain any protected information. This report is based on the Evaluation Technical Report/s.

Disclaimer: The certification or certificate is entirely related to the cybersecurity certification requirements of the product at the moment of issuance of the certificate. It is not related to the product itself.

The certification is not an endorsement of the product, the package or anything else related to the product. It only expresses that the cybersecurity related material and information of the product meets the requirements of this certification related information. There are no warranties about fit for purpose or merchantability, absence of defects, errors, accuracy, non-infringement of intellectual property rights, consumer rights and any other related rights. The issuer of the certification or the cybersecurity certification scheme owner are under no circumstances liable for any direct, indirect, material, technical and IT functionality related or moral damages of any kind arising out of the product for non-use, or use.

Neither will any loss of goodwill, work stoppage, computer failure or malfunction, loss or damages, amendments, misuse, abuse, alteration, destruction, theft, ransom or any other form of unauthorised access to data or any commercial damage generate liability to the issuer of the certificate or the designer of the certification scheme or any other organisation that recognises or gives effect to this certificate, except for gross negligence or wilful misconduct caused by natural persons working under these institutions.

Table of Contents

1 Executive Summary

The TOE that is the subject of this Certification Report is Blancco File Eraser. Blancco File Eraser comes in three editions –

- Blancco File Eraser (Home Edition)
- Blancco File Eraser (Enterprise Edition)
- Blancco File Eraser (Data Center Edition)

All editions run the same software version, 8.7.1.

The developer of the TOE is Blancco Technology Group IP Oy.

Blancco File Eraser (BFE) enables the secure deletion of selective data on PCs, servers and virtual machines. It is also optimized for erasure of selected files and folders in a corporate network. It can be used to erase specified paths or commanded with automated tasks using various rules. Detailed information of each erasure performed by BFE is stored in an erasure report. This report provides proof that the erasure has been performed successfully. BFE is a software application running on Windows. The software is operated via a graphical user interface (GUI) or by using a Command Line Interface (CLI).

The TOE is software only and consists of the respective executables, along with user documentation. The physical scope of the TOE is:

• Software executable (BlanccoFileEraser.exe or BlanccoFileEraserCmd.exe)

• Blancco File Eraser, User Manual for version 8.7.1

• Blancco File Eraser, Administrator's manual for version 8.7.1

• Blancco File Eraser, Common Criteria Supplement for version 8.7.1

The evaluation was performed by atsec information security AB, located at Svärdvägen 23, 182 33 Danderyd, Stockholm, Sweden. atsec information security AB is accredited according to ISO/IEC 17025 by the Swedish accreditation body Swedac with accreditation number 1937.

The evaluation has been completed on EAL2, augmented with ALC_FLR.2. This corresponds to [EUCC] level "Substantial", as AVA_VAN.2 has been applied. See a description of the evaluation in chapter 8 of this report, along with a summary of the results of the evaluation in chapter 9.

The [ST] does not claim conformance to any Protection Profile.

The [ST] has identified four assumptions. The TOE relies on these assumptions to properly counter the one defined threat and to fulfil the OSP that has also been defined. See chapter 5 of this report for further information regarding the specific assumptions, threat, and OSP.

The evaluation was completed in June, 2026. The evaluation was conducted in accordance with the Common Methodology for Information Technology Security Evaluation, CEM:2022, revision 1 [CEM], and corresponding Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, parts 1-5 [CC].

After reviewing the work of the evaluator, the Certification Body has issued the initial certificate for Blancco File Eraser version 8.7.1 on the 26th of June, 2026. The validity period is 5 years, and the certificate is therefore valid until 25th of June, 2031. The unique identifier of the certificate is **EUCC-3089-2026-001**.

The certification procedures were conducted in line with the provisions and requirements of the [EUCC].

2 Identification of the ICT Product

The TOE for this certification is Blancco File Eraser (BFE) version 8.7.1.

The following components make up the TOE:

Type	Reference	Version
Software	Blancco File Eraser (Home Edition)	8.7.1
Software	Blancco File Eraser (Enterprise Edition)	8.7.1
Software	Blancco File Eraser (Data Center Edition)	8.7.1

Table 1: Components

Along with the TOE, a set of guidance documents is provided.

See section 7 of this report for more information regarding the Supplementary Cybersecurity Information, as required by the [CSA].

2.1 System Requirements

The TOE is a Windows based solution, both 32- and 64-bit systems are supported. BFE works on single machines or in a network. It can erase selected files on both clients and servers, with the note that only the Data Center Edition can run on servers.

The following versions are included in the evaluation:

- Windows 10, 11 all versions
- Windows Server 2016, 2019, 2022 all versions (if you have licensed the Data Center Edition)
- .NET Framework 4.0 or later

BFE supports the following file systems: NTFS, FAT32 and exFAT. Note that the erasure of NTFS compressed files and /or volumes is not supported.

2.2 Contact Information

2.2.1 Holder of Certificate

Developer Name	Blancco Technology Group IP Oy
Address	Länsikatu 15 80110 Joensuu, Finland
Contact	support@blancco.com
Website link for Supplementary Cybersecurity Information	https://support.blancco.com/space/KB/11632706

2.2.2 Certification Body

Name	atsec information security AB
Address	Svärdvägen 23 182 33 Danderyd Sweden
Contact	cb@atsec.com
ITSEF	atsec information security AB
NCCA	Swedish Defence Material Administration (FMV)

3 Security Policy

The TOEs Security Policy contains the following:

- Security Audit
- User Data Protection

3.1 Security Audit

Reports that are designed to meet requirements for an audit of erased data are generated every time a file or drive free space is erased. The TOE receives a reliable date and time stamp, which is taken from the Windows Operating System.

The report contains the date and time that the actions were performed along with an indication of success or failure for the erasure events taking place.

3.2 User Data Protection

The TOE erases the data that constitutes a file or the unallocated space (Free Disc Space Erasure) on a target storage device by overwriting it with the selected overwrite pattern. A file erasure operation consists of a series of steps to access a file, get its size, overwrite the content and finally delete it from file system.

4 Vulnerability handling and Assurance Continuity

The following policy regarding vulnerability handling has been identified as applicable to the TOE:

Blancco File Eraser - Life-cycle Support (Security Flaw Remediation) v4.0-ALC_FLR

4.1 Assurance Continuity

This is an initial certification, and an assurance continuity policy was not provided.

4.2 Patch Management

Patch Management is not applicable to this certification.

5 Assumptions and Clarification of Scope

The [ST] contains four assumptions, one threat, and one OSP.

The assumptions are not covered by the TOE itself, but instead require Security Objectives to be fulfilled by the Operational Environment.

5.1 Usage Assumptions

The [ST] makes one assumption for usage of the TOE.

Assumption	Description
A.Users	Personnel using the TOE must have been trained, competent and follow all applicable guidance documentation.

5.2 Environment Assumptions

The [ST] makes three assumptions on the operational environment of the TOE.

Assumption	Description
A.Platform	The underlying hardware, firmware and the operating system functions needed by the TOE to guarantee secure operation, are working correctly and have no undocumented security critical side effect on the functions of the TOE.
A.Time	The platform must provide a time stamp and ensure that the time is correctly set.
A.Repository	The operational environment must provide storage to retain reports generated by the TOE in order to use them later for auditing/erasure proof requirements.

5.3 Threats

The [ST] outlines on threat to the TOE.

Threat	Description
T.Recovery	A threat agent gains access to a storage device after sensitive data files on that storage device have been erased by the TOE and is able to recover the contents of the file(s) using software or hardware tools.

The threat, as outlined in the [ST], is countered by the TOE. The evaluation did not uncover any threats to the TOE that the TOE does not counter.

As such, there are no threats to the ICT product not countered by the evaluated security functions of the product according to the intended use.

5.4 Organisational Security Policies (OSP)

The [ST] outlines one Organisational Security Policy (OSP):

OSP	Description
P.Report	The security objective O.Report ensures that information of the erasure process, consisting of erasure success or failure, the date erasure was performed, the erasure standard used and information about the content that was erased will be reported to the user and audited.

6 Architectural Information

The TOE is software only and consists of executables. The software can be downloaded from the developer's website.

There are three named editions of Blancco File Eraser:

- Blancco File Eraser (Home Edition)
- Blancco File Eraser (Enterprise Edition)
- Blancco File Eraser (Data Center Edition)

All the editions are operable via the use of a GUI. Enterprise Edition and Data Center Edition also include an additional application to operate the tool via a CLI.

Only the Data Center Edition may be installed on server versions of Windows.

While the core functionality and security functionality (i.e. erasing files and reporting) is the same for all the editions, there are slight differences as outlined by the [ST] as below:

Feature	Home Edition	Enterprise Edition	Data Center Edition
Installation on PCs?	Yes	Yes	Yes
Installation on servers?	No	No	Yes
Installation by .exe and .msi?	Yes	Yes	Yes
Graphical user interface?	Yes	Yes	Yes
Command line interface?	No	Yes	Yes
Scripting / Automating?	No	No	Yes
Local report saving?	Yes	Yes	Yes
Management console (BMP) compatible?	Yes	Yes	Yes
Windows event logging?	No	Yes	Yes
Group policy control?	No	Yes	Yes
Network erasures?	No	No	Yes

7 Supplementary Cybersecurity Information

The following website(s) were supplied by the developer for their supplementary cybersecurity information, according to Article 55 in [CSA]:

Information	Website
Documentation and TOE information	https://support.blancco.com/space/KB/11632706
Vulnerability reporting and publishing	https://support.blancco.com/space/KB/11632672
Support lifecycle	https://support.blancco.com/space/KB/11634250

On above mentioned support website(s), users can find:

Information regarding the guidance documentation which accompanies Blancco File Eraser,

the period in which Blancco File Eraser will receive support,

contact information for reporting any potential vulnerabilities,

and the online repository in which any vulnerability related to Blancco File Eraser would be published.

7.1 Documentation

The following documentation is provided along with the TOE:

- Blancco File Eraser, User Manual for version 8.7.1
- Blancco File Eraser, Administrator’s manual for version 8.7.1
- Blancco File Eraser, Common Criteria Supplement for version 8.7.1

8 ICT Product Evaluation

8.1 Assurance Components

The assurance components used for the evaluation of the TOE are the ones included in EAL2, augmented by ALC_FLR.2, as defined in [CC] and [CEM]. See chapter 9 for a full summary of all components included in the package.

8.2 State-of-the-Art Documents and Evaluation Criteria

No specific State-of-the-Art document was used in this evaluation.

No further Evaluation Criteria applicable.

No Protection Profile was applied during this evaluation.

8.3 Evaluated Configuration

For testing, the Data Center edition version 8.7.1 was used.

For the evaluation, the following erasure algorithms are in scope:

Algorithm Name	Document Title and Version
HMG Infosec Standard 5, Lower standard (DEFAULT)	HMG Infosec Standards No. 5, Secure Sanitisation of Protectively Marked or Sensitive Information, September 2007
HMG Infosec Standard 5, Higher standard	
U.S Department of Defense Sanitizing (DoD 5220.22-M)	1. DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM), February 28, 2006 2. DSS Clearing and Sanitization Matrix, June 28, 2007
NSA 130-1	1. NSA/CSS Manual 130-1, Information System Security Training Requirements, September 2001 2. Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, 31 March 2001, Revision 2
NIST 800-88 Clear	NIST Special Publication 800-88, Guidelines for Media Sanitization, Revision 1, December 2014
Aperiodic random overwrite	N/A

As a platform, the TOE utilizes the Windows Operating Systems. The following versions are in scope of the evaluation:

- Windows 10, 11
- Windows Server 2016, 2019, 2022 (Only Data Center Edition)

8.4 Developer Testing

The developer testing is constituted of both manual and automated tests. The evaluators examined the testing conducted by the developer (coverage and functional testing) to ensure that the developers have fulfilled their responsibilities and covered all requirements.

Developer testing included both automatic and manual testing with coverage of all SFRs, and all applicable overwrite patterns.

The developer conducted testing on all applicable versions of Windows.

8.5 Evaluator Testing

The evaluator repeated a sample of the tests conducted by the developer.

Along with this, the evaluator devised additional control tests and independent tests. The purpose of the control tests was to establish a baseline for normal behavior of the environment and the suitability of the tools used for testing.

For the independent testing, the evaluator devised new test cases to supplement the testing done by the developer and the repetition of developer test cases. Evaluator testing was conducted on the Data Center Edition of the TOE (to get access to the full set of functionalities) on a Windows 10 Professional Operating System.

The evaluator testing covered all supported file system types (NTFS, FAT32, ExFAT), all types of data that the TOE may erase (e.g. files, empty disk space), and all algorithms mentioned in chapter 8.3 of this document. Since some of the algorithms go through multiple rounds, it was also verified that these were implemented properly.

All evaluator testing was conducted within the premises of the ITSEF.

8.6 Penetration Testing

A public search for vulnerabilities was conducted according to a compiled list of terms related to the TOE and the environment used by the TOE.

Penetration testing was conducted according to a number of tests, which were devised by searching through the accompanying documentation of the TOE. These tests included, among others, interruption of the erasure procedure in different ways and deleting small (less than 4 kB) or large (4 GB) files.

All penetration testing was conducted on the same setup as the independent testing.

All penetration testing activities were conducted at the premises of the ITSEF.

9 Results of the Evaluation

9.1 Summary

Development		**Result**
Security Architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.2	Pass
TOE design	ADV_TDS.1	Pass
Guidance documents		
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life-cycle support		
CM capabilities	ALC_CMC.2	Pass
CM scope	ALC_CMS.2	Pass
Delivery	ALC_DEL.1	Pass
Flaw remediation	ALC_FLR.2	Pass
ST evaluation		
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
Security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Tests		
Coverage	ATE_COV.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass
Vulnerability assessment		
Vulnerability analysis	AVA_VAN.2	Pass

9.2 Result

As defined in chapter 8.1, the evaluation was based on the EAL2 package augmented with ALC_FLR.2. This corresponds to a certificate on “Substantial” as defined in [EUCC].

The [ST] did not claim conformance to any PP.

Based on the above, the evaluation results from the ITSEF concluded that Blancco File Eraser version 8.7.1 **is conformant with Part 2 and Part 3 of [CC].**

10 Certificate Information

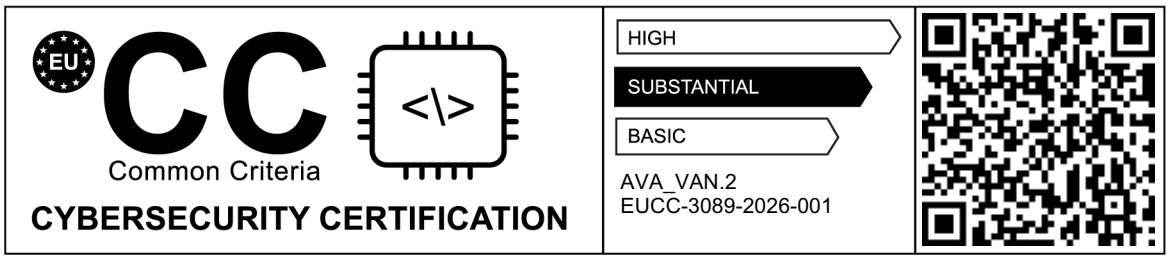
A certificate has been issued following the conclusion of the evaluation.

Unique identifier for certificate: **EUCC-3089-2026-001**

Initial certificate issued: **2026-06-26**

Valid for: **5 years**

Expiration date: **2031-06-26**



11 Comments and Recommendations

None.

12 Reference to the Security Target

The Blancco File Eraser Security Target [ST] is provided as a separate document alongside this Certification Report.

13 Glossary

If applicable, this section is used to increase the readability of the report by providing definitions of acronyms or terms of which the meanings may not be readily apparent.

BFE	Blancco File Eraser
TOE	Target of Evaluation
GUI	Graphical User Interface
CLI	Command-Line Interface
ITSEF	IT Security Evaluation Facility
FMV	The Swedish Defence Material Administration
Swedac	The Swedish National Accreditation Body

14 Bibliography

[CC] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Parts 1 – 5

[CEM] Common Methodology for Information Technology Security Evaluation, CEM:2022, revision 1, November 2022 — Evaluation methodology

[ETR] Final Evaluation Technical Report, atsec information security AB, version 3.0, 2026-06-22

[ST] Blancco File Eraser v8.7.1 Security Target, Blancco Technology Group, version 7.0, 2026-05-22

[CCS] Blancco File Eraser 8.7.1 Common Criteria Supplement, Blancco Technology Group

[ADM] Blancco File Eraser Administrator Manual for Version 8.7.1, Blancco Technology Group, 2026-04-27

[USM] Blancco File Eraser User Manual for Version 8.7.1, Blancco Technology Group, 2026-04-27

[FLR] Blancco File Eraser - Life-cycle Support: Flaw Remediation, Blancco Technology Group, version 4.0, 2026-05-29

[EUCC] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024, amended by Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 and Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025

[CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019