Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) v.3.1 rel. 5

Certificato n. *(Certificate No.)*	02/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/12/2022/RC, v1.0
Decorrenza *(Date of 1st Issue)*	6 febbraio 2024
Nome e Versione del Prodotto *(Product Name and Version)*	Tresorit Core Interface v5.0
Sviluppatore *(Developer)*	Tresorit Kft.
Tipo di Prodotto *(Type of Product)*	Protezione dati
Livello di Garanzia *(Assurance Level)*	EAL4+ (AVA_VAN.5) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto conforme a CC Parte 2

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 6 febbraio 2024

p. il Direttore Generale
dell'ACN

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) 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 Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Tresorit Core Interface v5.0

OCSI/CERT/CCL/12/2022/RC

Version 1.0

6 February 2024

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	06/02/2024

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AAA	Autentication Authorization and Accounting
BSI	Bundesamt für Sicherheit in der Informationstechnik
CLI	Command Line Interface

DLL	Dynamic Link Library
OS	Operating System
SSL	Secure Socket Layer
TCI	Tresorit Core Interface
TLS	Transport layer Security

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components", Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components", Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, "Common Methodology for Information Technology Security Evaluation – Evaluation methodology", Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[AIS34] Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1) version 3, Bundesamt für Sicherheit in der Informationstechnik (BSI), September 3rd 2009

[CCECG] AGD Documentation for Tresorit Core Interface v5.0, version 1.1 October 27th, 2023

[ETR] "Tresorit Core Interface v5.0" Evaluation Technical Report, Version 2, CCLab Software laboratory, November 23rd , 2023

[ST] Tresorit Core Interface v5.0 Security Target, Tresorit Kft., version 2.1, October 27th, 2023

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

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

This certificate is recognised under SOGIS-MRA up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

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

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product “Tresorit Core Interface v5.0”, developed by Tresorit Kft.

The TOE is a command line interface (CLI) application for Windows designed as an end-to-end encrypted file storage and sharing solution to protect the confidentiality and integrity of users’ files and file names. Users can share their files and folders with other users of the TOE. User files and folders are accessible to those who the user gave access to.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance level EAL4 augmented with AVA_VAN.5, according to the information provided in the Security Target [ST] and in the configuration shown in “Annex B – Evaluated configuration” of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Tresorit Core Interface v5.0” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Tresorit Core Interface v5.0
Security Target	Tresorit Core Interface v5.0 Security Target, Tresorit Kft., version 2.1, October 27th 2023 [ST]
Evaluation Assurance Level	EAL4 augmented with AVA_VAN.5
Developer	Tresorit Kft.
Sponsor	Tresorit Kft.
LVS	CCLab Software Laboratory (Debrecen site).
CC version	3.1 Rev. 5
PP conformance claim	None
Evaluation starting date	15 July 2022
Evaluation ending date	23 November 2023

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and in the configuration shown in “Annex B – Evaluated configuration” of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description it is possible to refer to [ST].

The TOE is Tresorit Core Interface v5.0. The TOE is a CLI software product designed for end-to-end encrypted file and folder sharing.

Users of the TOE can create cryptographically protected containers and share entire containers or part of their content with other users of the TOE. The TOE provides an end-to-end encrypted solution which guarantees that no one who has access to the communication channel between the users can access or modify the content of the shared files or the name of the files. The TOE provides its security functionality without the need to trust the developer’s servers. The TOE implements a state-of-the-art end-to-end encryption (E2EE) communication that ensures all encrypted information remains encrypted once it leaves the sender's device and remains encrypted until it reaches the recipient. This means that no third party has any way of accessing the exchanged information in unencrypted form, not even the developer of the TOE.

The TOE requires the following environment:

- the Windows: 10 (x64) or later OS;
- access to the Internet
- usage of a pre-defined cloud storage service provided by the Developer.

TOE has the same minimum hardware requirements as the underlying OS. The cloud service is a Microsoft Azure infrastructure architected and operated by the developer of the TOE. The TOE automatically uses this service without any interaction required by the user.
For a detailed description of the TOE, consult sections 1.3 and 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

It is possible to refer to sections 1.3, 1.4 of the Security Target [ST] for a more detailed description of the TOE.

7.3.1 TOE architecture

Tresorit Core Interface is a CLI application for MS Windows delivered to the users in the form of an installer named "*Tresorit.exe*".

The TOE environment architecture is represented in Figure 1: the two displayed TOEs are the running TOE software instances on the shown physical computers.

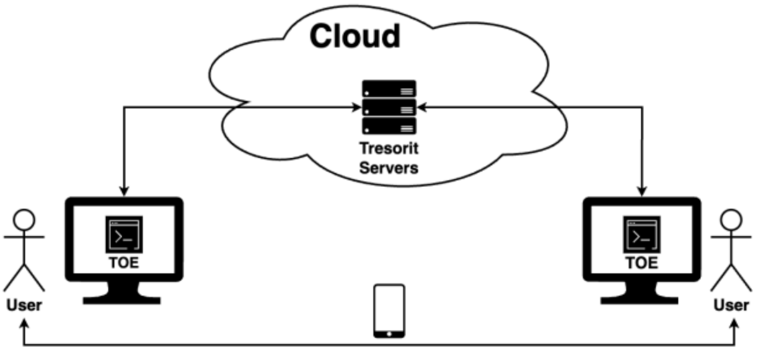

Figure 1 - TOE environment [ST]

Figure 1 illustrates an additional secure communication channel: this channel is needed to be established when a TOE user (inviter) shares a container with another TOE user (invitee) to communicate verification objects required to ensure the integrity of all messages exchanged during the container sharing process; such channel is only needed until the invitee accepts the invitation to the container.

The physical scope of the TOE consists of two files along with the necessary guidance documentation [CCECG]. Table 1 details parts of the physical scope of the TOE.

File	Identification	Version
TOE executable	*tresorit-core-interface.exe*[1] (the executable file which is to be started by the user to use the TOE)	5.0.3950.3950
TOE DLL	*Tresorit.dll* (the DLL file containing TOE functionality, used by the TOE executable)	4.13.17.3950
User guidance	*AGD Documentation for Tresorit Core Interface v5.0* (PDF document user guide and installation guide [CCECG]	1.1

Table 1 - TOE physical scope

TOE is part of the Tresorit product, which is a monolith application. The architecture is shown in Figure 2

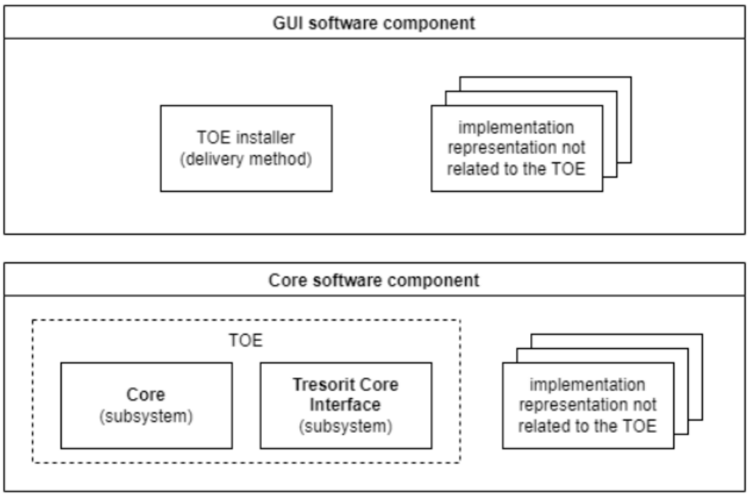
GUI software component
TOE installer (delivery method)
implementation representation not related to the TOE
Core software component
TOE
Core (subsystem)
Tresorit Core Interface (subsystem)
implementation representation not related to the TOE

Figure 2 - TOE Architecture

TOE's security features are provided via only one TSFI: TOE does not expose any of its functionality via its network TFSI. External entities cannot invoke TOE functionalities via the network.

All TOE functionalities are exposed in the form of commands via its user-facing CLI TSFI (see Figure 3) with one enforcing module (Core), two supporting modules (OpenSSL, ICU4C), six non-interfering modules (Protocol Buffers, zlib, SQLite, RapidJSON, Brotli, libcurl), one enforcing TSFI (CLI), and three interfaces to non-interfering modules (TresoritLoginServer, TresoritStorageServer, BlobStorage). In addition, the TOE has one non-interfering subsystem (TCI) with one non-interfering module (TCI).

[1] Not to be confused with the installer Tresorit.exe, v. 3.5.4549.3950

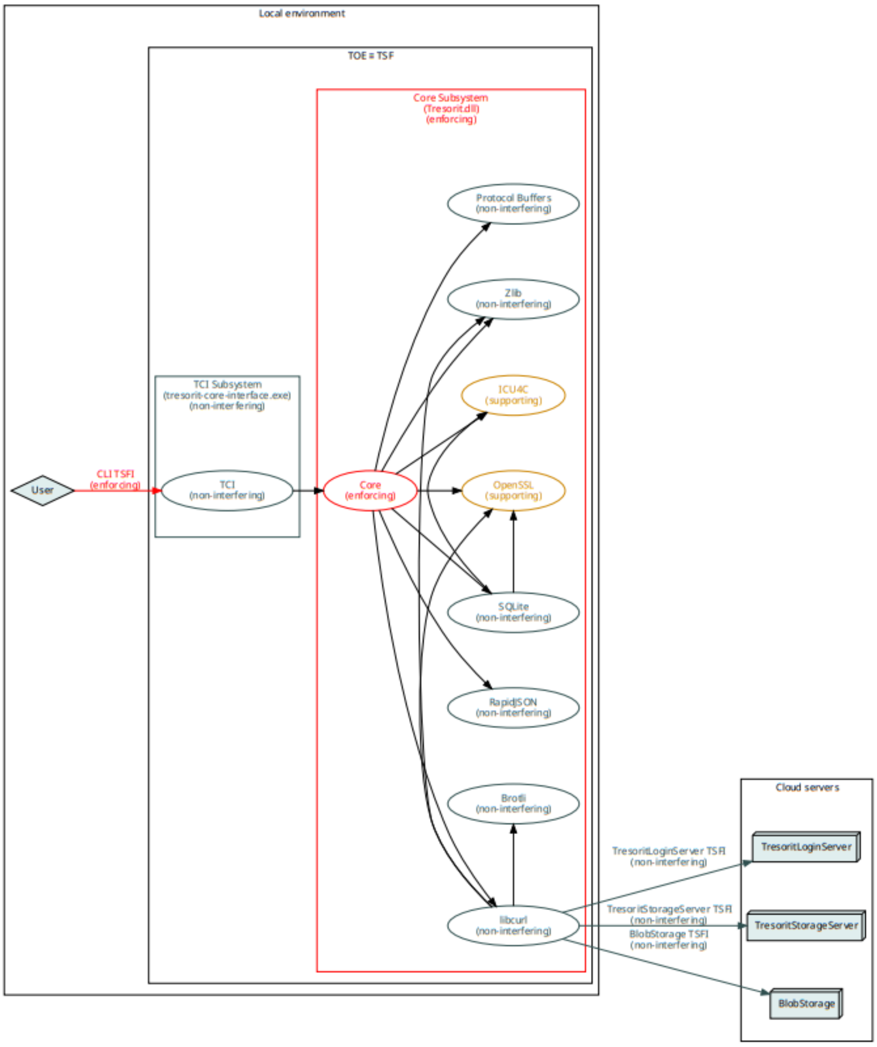

Figure 3 - Tresorit Subsystems and TOE boundary

The TCI subsystem is the subsystem of the TOE responsible for providing a user-facing command-line interface to the TOE. Its purpose is to parse and forward commands the user entered to the Core Subsystem for execution and then to present the results of the actions to the user.

The Core Subsystem is responsible for the cryptographic operations, container and file management operations, user management, and secure communication with entities outside of the TOE. The Core Subsystem is the one performing the actions belonging to a command received from the TCI Subsystem.

The TCI module has the purpose of processing user input from the command line interface of the TOE. It parses incoming user commands along with their parameters, performs validation on them, then invokes respective actions of the TOE, ultimately invoking functionality of the Core Subsystem's Core module. The TCI module also serves as the entry point of the TOE, containing the "main" method the TOE executes first when started.

The Core module is the central and sole manager and orchestrator of all internal TOE actions that are run as the result of the TOE user invoking a command, along with its internal background operations. It is responsible for enforcing all SFRs of the TOE, orchestrating cryptographic operations for securing files that are uploaded to the cloud servers, and handling requests sent to, and responses received from the cloud servers. The Core Module also serves as the entry-point of the Core Subsystem. The TCI subsystem uses the Core Subsystem by communicating with the Core Module.

OpenSSL (Module) is used to implement cryptographic operations inside the TOE by the Core Module and the SQLite Module, to parse X.509 certificates returned by the cloud servers by the Core Module, and to establish TLS connections by the libcurl Module.

ICU4C (Module) is used by the Core Module to do character encoding conversions, Unicode string operations, date time formatting and regular expression matching, and also internally by the SQLite Module.

Protocol Buffers Module is used by the Core Module to serialize and deserialize messages sent through the AsyncAPI between the Core Subsystem and the TCI subsystem.

zlib (Module) is used by the Core Module to compress the uploaded files and by the libcurl module to handle compressed HTTP responses.

The Core Module uses SQLite (Module) to store the content of its local cache to the disk.

The Core Module uses RapidJSON (Module) to serialize the JSON messages required by the various Network interfaces and to parse the JSON response returned by said interfaces.

Brotli (Module) is used by the libcurl module to handle compressed HTTP responses.

The Core Module uses libcurl (Module) to establish a connection to the cloud servers, send HTTP requests and parse the received responses.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sections 1.4.2 and 7.1 of the Security Target [ST]. The most significant aspects are summarized in the following sections.

The TOE can be used to share files and folders with other TOE users in a secure way that guarantees that no third party has any way of accessing the exchanged information in unencrypted form.

The TOE is responsible for the confidentiality and integrity protection of user file contents, file and folder names transmitted over network with state-of-the-art encryption solutions based on cryptographic best practices.

The major security features of the TOE are described in the following sections.

7.3.2.1 Encrypted communication with other TOE users

The TOE encrypts the names and contents of all files leaving the TOE, meaning that no cloud servers or network devices have access to the file names and file content shared between TOE users.

7.3.2.2 Secure key exchange

Exchanging encryption keys between TOE applications is done in a way that only the communicating parties gain access to the keys, ensuring no third party can access them in unencrypted form.

7.3.2.3 Key generation and management

The keys used for encrypting information are generated by the sending party and are managed by the participating parties in a way that no third party can gain access to them in unencrypted form, not even temporarily.

7.3.2.4 End-point authentication

All parties can be sure that the public keys belong to the desired party, and a potential attacker cannot inject their own public key to execute a man-in-the-middle attack.

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile (PP).

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the SFRs have been selected from CC Part 2 [CC2].

Security Target [ST] provides a complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory (Debrecen site).

The evaluation was completed on 23 November 2023 with the issuance by LVS of the Evaluation Technical Report v2 [ETR], which was approved by the Certification Body on 15 December 2023. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration". Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report v2 [ETR] issued by the LVS CCLab Software Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Tresorit Core Interface v5.0" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with AVA_VAN.5, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives for the operational environment	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle mode	ALC_LCD.1	Pass

Assurance classes and components		**Verdict**
Well-defined development tools	ALC_TAT.1	Pass
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - conformance	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	*AVA_VAN.5*	*Pass*

Table 2 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4 augmented with AVA_VAN.5.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives for the operational environment	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		**Verdict**
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle mode	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - conformance	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	*AVA_VAN.5*	*Pass*

Table 2 Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product “Tresorit Core Interface v5.0” are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the “Security Objectives for the Operational Environment” specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.2 of the Security Target [ST] shall be satisfied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, “Annex A – Guidelines for the secure usage of the product” includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([CCECG]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The TOE is a CLI application delivered to the users in the form of an installer named *Tresorit.exe* with version of the installer 3.5.4549.3950. The developer maintains an email address for customers to ask their questions at “support@tresorit.com”.

The user guidance documentation and the installer of the TOE can be accessed for users upon request submitted through the above-mentioned email address or through dedicated sales representatives for enterprise customers. Each part of the TOE (the TOE executable, the TOE DLL and the guidance document) and the TOE installer are digitally signed by the developer.

Figure 4 describes the semantic scope of the TOE.

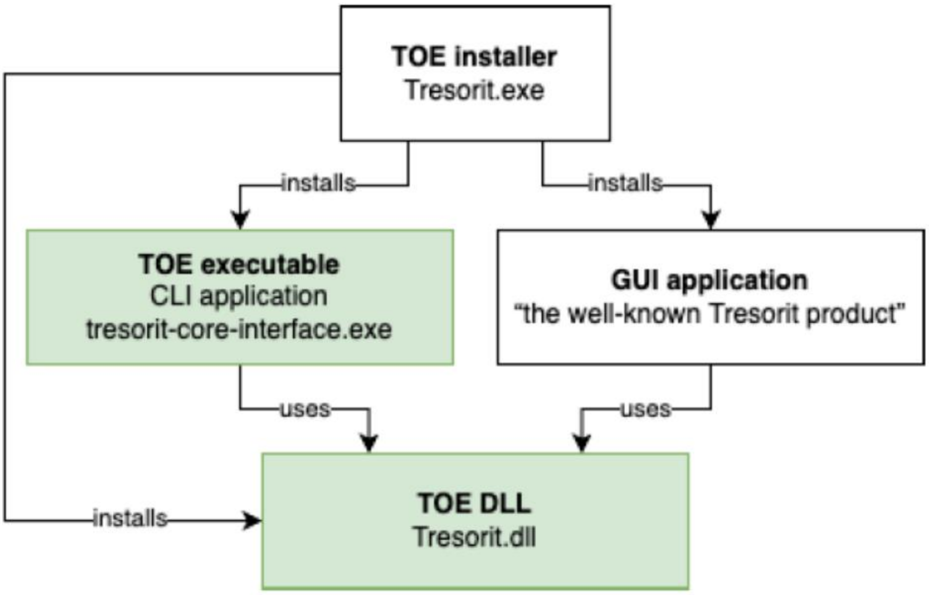

Figure 4 - Semantic of Tresorit components including TOE.

The installer of the evaluated TOE instance can be downloaded from the following URL:

https://installerstorage.blob.core.windows.net/public/zkpy42jitvcm80ximtlj/Tresorit.exe

User is then required to (for detailed procedure see [CCECG], section 6.3):

- check the version (3.5.4549.3950), the digital signature and the hash (c654c3fb4506980c269859bc8478ab82404c10d8a6188164a02601e4a86b418d) of the *Tresorit.exe* installer;
- check the version (5.0.3950.3950), the digital signature, and the hash (ae7eaab51c2d3319bf084f5ef7bc1fd84e1e10246d9a6c80c8f7a01fee21a2b4) of the *tresorit_core-interface.exe* file;

- check the version (4.13.17.3950), the digital signature, and the hash (97fd3cf5cd0807afc9d56fe59f19d1437c6de4d968d02a599e686a8ced621661) of the *Tresorit.dll* file;
- Install the TOE software.

9.2 Installation, initialization, and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the Common Criteria Evaluated Configuration Guide [CCECG] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

TOE is the Tresorit Core Interface v5.0. The TOE is preconfigured according to internationally recognized standards to use cryptographic parameters and it does not provide users the option to change these. The only security parameter that can be changed by the TOE user is the user's account password.

Users are responsible to choose hard to crack, complex password. The TOE enforces the following restrictions on the password, based on Unicode code points and character classes:

- minimum of 8 characters long,
- contains at least 1 uppercase letter,
- contains at least 1 lowercase letter,
- contains at least 1 digit.

Although not required, the following extra recommendations should be taken into consideration by TOE users when choosing their account password:

- use at least one or two special characters ($ * !);
- don't use of common words like "password" and refrain from the use of names (e.g., personal name or the name of a family member, username, the name of a pet);
- stay clear of common character substitutions (e.g., p@55w0rd);
- don't use sequences like "123456" or "abcdef". Even reversed sequence of characters, like '654' and 'ONM' will weaken the password;
- watch out for neighbouring keystrokes (e.g., qwerty, asdf);
- refrain from using repeated characters (e.g., aaaaaaa);
- don't use full dates, like "01261987" or other easy-to-guess personal information. Especially avoid using birth dates, phone numbers, addresses, license plate numbers, or anything else someone could guess or look up about the user;
- avoid using the same password that is used for other accounts, including non-TOE services of Tresorit.

10.1 TOE operational environment

The LVS reproduced the test environment with:

- two virtual machines with freshly installed Windows 10 Home including the newest security patches available at the test activity date, also fulfilling the requirements for the minimum OS and hardware;
- access to the Internet;
- a pre-defined cloud storage service provided by the Developer. The cloud service is a Microsoft Azure infrastructure architected and operated by the developer of the TOE.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

Testing activities have been carried out from the LVS premises.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the Common Criteria Evaluated Configuration Guide [CCECG] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The developer has provided automated tests which can be run sequentially or individually.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly. Evaluator created a dedicated environment for testing the TOE with two virtual machines with Windows 10 Home including the newest security patches. They also verified that the test environment was properly set up.

Testing the TOE can be divided into two parts:

- automated tests (the Evaluator conducted on both virtual machines all the automated python test cases listed in the test documentation provided by the Developer);
- tests prepared by the laboratory, mainly related to new accounts registration, containers creation and user association for the new containers, access rights revocation for a specific container, container usage (e.g. files upload and download).

Evaluators conducted all test cases for verification of correct implementation of cryptographic functionality using the OpenSSL's testing suite.

11.3.2 Test results

All the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

The Evaluators conducted vulnerability analysis and penetration testing activities using [AIS34] as a basis for the applied methodology of Vulnerability Assessment .

A search on public vulnerabilities for third party libraries (Protocol Buffers, OpenSSL, ICU4C, SQLCihper, zlib, SQLite, RapidJSON, Brotli, mime-db, libcurl), have been conducted. The analysis confirmed that there are no public vulnerabilities exploitable with the TOE implementation and configuration.

The evaluators conducted penetration testing activities on the same instance of the TOE configured for functional and independent testing. TOE executable and TOE DLL references have been also verified.

The evaluator could then conclude that the TOE is resistant to an attack potential of level High in its intended operating environment. No exploitable or residual vulnerabilities have been identified.