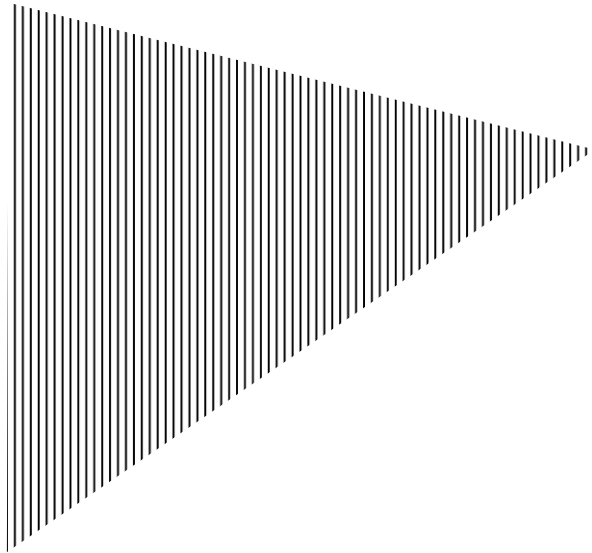



2019 OCTOBER



Tresorit Security Evaluation Summary

Penetration Test, Source Code and Cryptographic Review of	
Tresorit End-to-End Encrypted File Sharing and Sync Service by Ernst & Young Advisory Ltd	
THIRD PARTY MEMO	



I. Executive Summary

The security review of Tresorit End-to-End Encrypted File Synchronization and Sharing Service was performed by the EY Advanced Security Center in August and September 2019. Tresorit implements End-to-End Encryption so that Tresorit as a service provider ensures high data confidentiality while maintaining data anonymity by not accessing the content of its users.

The scope of the assessment included the technical security evaluation of the end-to-end encryption, web application, mobile applications and desktop applications developed by Tresorit by means of attack, penetration testing, source code and cryptography review. The findings result from our attempts to discover, validate, and exploit vulnerabilities that were considered within the engagement's scope and duration.

The security review paid specific attention to Tresorit's claim regarding end-to-end encryption and to identify potential security deficiencies. Tresorit claims that they encrypt data on the client side, to ensure high confidentiality and continuous security against malicious parties. In addition, they do it in a way that Tresorit servers and employees never receive cleartext data or the encryption keys. The assessment has found no contrary evidence, and the claim is well founded.

II. Tresorit Technical Summary

Tresorit offers an end-to-end encrypted file synchronization and sharing service. It offers file synchronization and collaboration for teams with permission controls and file history.

Encryption and decryption are done on the client-side. No one is able to access stored data, except for the owner and users authorized by the owner. This claim can be verified (audited) by a professional looking at the behavior of the applications, reducing the trust dependency in the cloud storage provider.

The encryption is performed with a fresh, randomly generated 256-bit symmetric key chosen by the client-side application. The encryption algorithm Tresorit applies is AES256.

Each file version gets a fresh, randomly chosen 128-bit IV in order to guarantee semantic security. Encryption keys of files and directories are changed from time to time, using a so-called "lazy re-encryption" scheme. This means that after the group's membership changes, the encryption key is regenerated the next time a file's contents change (see patent US9563783).

This guarantees that if you remove somebody from a group you shared files with, they will not be able to decrypt any new information they did not have access to before their removal. In the meantime, you don't need to re-encrypt everything right away, saving computing resources and time.

III. Objectives and Scope

The objective of our security review was to evaluate the current level of information security of the selected components of Tresorit to ensure that information security risks are understood and addressed, key controls are in place and operating effectively.

We evaluated information security design and controls by means of attack, penetration testing, source code and cryptography review. A time-limited security assessment was performed with the following details and goals:

- ▶ Perform review with specific attention to Tresorit's claim regarding end-to-end encryption and identify security deficiencies, vulnerabilities, architectural deficiencies or any other deficiency that may potentially undermine this claim.
- ▶ Evaluate current state information security design related to Tresorit using Open Web Application Security Project (OWASP) guidance on attack, penetration testing and leading practices.
- ▶ Test implemented security measures to determine whether they sufficiently limit the risks associated with hackers or malicious personnel gaining unauthorized access to Tresorit components, functions, any business-critical data stored or handled within.



- ▶ Identify security deficiencies and vulnerabilities; evaluate the associated business risks.
- ▶ Formulate clear recommendations for mitigating identified risks.

Testing activities addressed selected components of the product suite including both back-end and front-end application components to provide a detailed understanding of the security level of Tresorit. Below is the list of components selected for the scope of our testing:

▶ **I. Penetration testing**

Testing activities:

- Back-end services black box testing of Tresorit Web, mobile (iOS & Android) and desktop (Windows, Mac & Linux) application. Test results found no deviation from Tresorit's data confidentiality claims.

▶ **II. Source code review**

Testing activities:

- Full Source Code Security Analysis of the Tresorit source code. Test results validate that implementation is in accordance with the concepts described in Tresorit's white paper.

▶ **III. Cryptography review**

Testing activities:

- NIST statistical tests were performed on multiple occasion on the encrypted data to validate the level of security of the implemented cryptographic routines. Test results showed no deviation.

Attack and penetration testing of web and mobile applications, as well as the browser extensions were performed from both the perspective of an unknown, unauthorized party and from the perspective of known, authorized users (i.e. Tresorit users with different roles). *Note: Tresorit service suite contains additional components such as:*

- ▶ *Windows mobile application*
- ▶ *Active Directory synchronization elements (thick client application, Windows service)*

All these and all other remaining, unspecified components were out of the scope of our work.

IV. Specific Additional Terms and Conditions

Our work will not be performed in accordance with generally accepted auditing, review, or other assurance standards in [the relevant jurisdiction] and accordingly does not express any form of assurance. None of the Services or any Reports will constitute any legal opinion or advice. We will not conduct a review to detect fraud or illegal acts.

Notwithstanding anything to the contrary in the Agreement or this SOW, we do not assume any responsibility for any third-party products, programs or services, their performance or compliance with your specifications or otherwise.

We have based any comments or recommendations as to the functional or technical capabilities of any products in use or being considered by you solely on information provided by your vendors, directly or through you. We are not responsible for the completeness or accuracy of any such information or for confirming any of it.