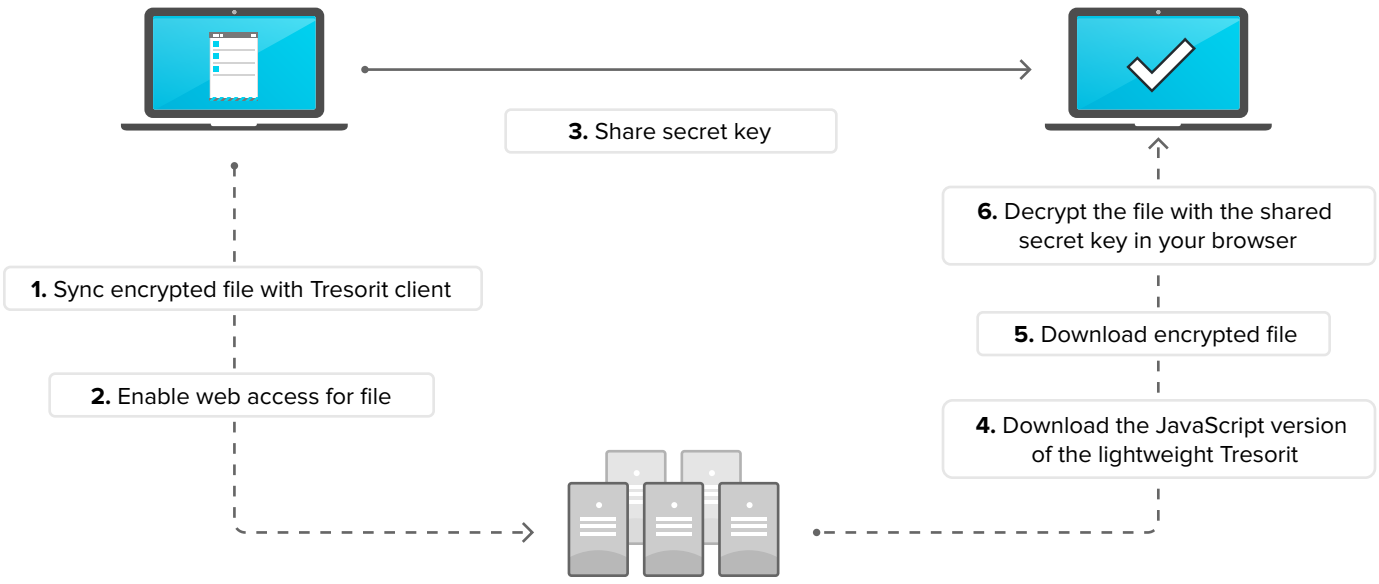
tresorit

Encrypted link Whitepaper

Tresorit's encrypted link is a web based, encrypted file sharing solution. Linked files have the very same encryption and integrity protection as files synced with the Tresorit client. To protect your data we set up a decryption environment, and process your data in the browser.

As a zero knowledge sharing solution, encrypted links contain fragment identifiers (identified by the hashmark - #). When an encrypted link is opened, the web browser requests the encrypted data from Tresorit servers, and sends the URL (without the fragment) to the server. As the fragment itself will not be sent, the server cannot access the data sent, but the browser, by combining the encrypted file and the key contained in the fragment, is able to decrypt it.



No security compromise: Tresorit servers cannot access the data decrypted on your computer. Encrypted links are a Tresorit feature, designed to share pieces of your workflow (documents, pictures, or any other files types) quickly and smoothly in your browser.

COMPATIBILITY: Tresorit encrypted links support only the following browser versions: last two versions of Google Chrome and Firefox, Internet Explorer 10 and up. We don't recommend downloading encrypted links in mobile device browsers, however primary tests ran with promising results. Download the official Tresorit app for Android or iOS to access sensitive content, these are also easy to use and include many handy features.

KEEPING CONTROL OVER CONTENT: To stay in control over the linked files, users can revoke links manually any time, preventing further access via the link.

Please note that the encrypted link's crypto-security model depends on the confidentiality of the keys displayed above - your files will be available to anyone if they manage to gain access to the encrypted link itself. Avoid transmitting encrypted links through insecure channels. Public distribution of your encrypted files is not recommended either.

CONSIDER THESE FACTORS IN TERMS OF SECURITY OF YOUR LINKED FILES:

1 Transmission channel you are sharing encrypted links through

In case the URL is exposed, your files lose their full protection. In case you share the encrypted link's URL in email the servers the mail travels through can scan and parse the mail for links like this. While this is a common behavior at companies like Google, Microsoft or Facebook to detect online scam and fraudulent links, they may store the URL in their history. This can lead to the leakage of information, government agencies can issue a request to collect and easily access your encrypted files.

PROTECTION: If needed, you can revoke the encrypted link manually to prevent further downloads.

2 Tresorit webservers

If Tresorit's webservers are hacked, you can be served with a modified version of the lightweight Tresorit client. This way, the attackers can inject code into the Javascript client and forward the decrypted contents to them.

PROTECTION:
This is a highly unlikely scenario, but you should be aware of this kind of attack. We continuously monitor our service's integrity and ***we have a shutdown policy in case intrusion is detected.*** This is the industry protocol in such cases, applied by security-conscious organisations like banks and health data operators.

3 User's browser

In case there is a vulnerability in the downloader's browser, it may expose the encrypted link's data to attackers. This is part of the reason we don't support old browsers like IE8, IE9 or FF3.

PROTECTION: Even the most modern browsers need to be updated to their latest versions before you use them. Since browsers change versions often, you need to upgrade them regularly. If you are not sure what to do, please contact your system administrator or our Support Team.