

How Does Zero-Knowledge Encryption Work

TechRounder PDF Edition

Live article: <https://www.techrounder.com/security/how-does-zero-knowledge-encryption-work/>

By Vipin PG | Published November 24, 2022 | Updated November 24, 2022 | Format: Analysis | 4 min read

In brief

File encryption is an effective data protection solution for individuals and businesses dealing with sensitive data. Encrypted files are encoded, providing additional security and preventing unauthorized access.

File encryption is an effective data protection solution for individuals and businesses dealing with sensitive data. Encrypted files are encoded, providing additional security and preventing unauthorized access. In addition, it ensures that the files are read only by the users they were intended for.

Even more advanced than basic encryption is zero-knowledge encryption. This article will explain zero-knowledge encryption, how it works, and why you might need it to protect your data.

What is Zero-knowledge Encryption?

Encryption is a fairly common term on the internet. It implies that files are unreadable to all except authorized recipients. This protection is crucial when dealing with sensitive personal or business data. A Virtual Private Network (VPN) is a common way to encrypt data and remain anonymous online.

Zero-knowledge encryption is a newly popularized term that takes encryption to the next level. It means that no one except you (not even the service provider) has access to the secured files.

It's important to understand that zero knowledge isn't an encryption protocol like TLS/SSL. It's merely an encryption method that builds on these protocols with more, stricter rules. The term describes an encryption process where data is always encrypted, and only one person has the password to unlock it, making it particularly secure.

To be zero-knowledge, data must be encrypted before it leaves your device, while it transfers, and after it lands on a server. These three stages are known:

- Client-side encryption
- Encryption in transit
- Encryption at rest

These stages are associated with different encryption protocols, including TLS, AES, and others. Zero-knowledge combines these protocols into a single, heavily secure encryption method.

The password plays a massive role in zero-knowledge encryption. It's the key that allows you to decrypt the data. The password is never stored anywhere, not even with the service provider. Only you have the password, which means that even if someone infiltrates the service, they can't access the data. But how can the service verify your password if they don't store it? That's where zero-knowledge proof comes in.

What is zero-knowledge proof?

Zero-knowledge proof is a different concept from zero-knowledge encryption. They often work together to create zero-knowledge encryption, but that's not always the case.

Zero-knowledge proof is a cryptographic authentication method where the service provider asks that you prove your knowledge of the password instead of providing the actual password. For example, a banking app may ask you to provide the password's first, third, and ninth letters. Only someone who knows the password could give this, thus proving their authenticity.

Are there any drawbacks to zero-knowledge encryption?

Although zero knowledge is the most advanced encryption method, it has some drawbacks. That's why it's used sparingly and only when dealing with sensitive data.

The most glaring problem is how easy it is for you to get locked out of your data. If you forget your password, you can't recover it or create a new one since the service provider doesn't have it either. All they can do is ask you to enter the recovery key provided at the start of the encryption process. If you don't have that key, it will be almost impossible to regain access to your files.

Due to its added emphasis on security, zero-knowledge encryption also limits several features that improve the user experience. For example, you'll be unable to preview images or documents as they need to be decrypted.

Why you need zero-knowledge encryption

Despite its few drawbacks, zero-knowledge encryption is an excellent security option. However, it's best to only use it with highly sensitive personal and financial information, customer and business data, etc.

The main advantage is that no one other can access your data. You can control how the data is handled since it's first stored locally before reaching the server. Even if the service provider suffers a breach or attack, your data will remain protected as you're the only one with the password.

Zero-knowledge encryption is most prevalent with cloud storage providers and password managers. These services have advanced algorithms that make zero-knowledge implementation easier. If you have very sensitive data that you want to ensure remains protected, storing it on cloud storage that supports zero-knowledge encryption is a great option.

Final Thoughts

Encryption is an effective and much-necessary security measure in today's vulnerable online landscape. Zero-knowledge encryption is the most advanced method you should reserve for your most sensitive data. Zero-knowledge implies that only you have the password to unlock the encrypted data, making it significantly more secure.

When encrypting data with the zero-knowledge method, make sure you also remember the recovery key, as you may need it if you ever get locked out.

References

1. nordvpn.com - features / vpn-security - <https://nordvpn.com/features/vpn-security/>
2. nordlocker.com - features / zero-knowledge-encryption - <https://nordlocker.com/features/zero-knowledge-encryption/>
3. ethereum.org - en / zero-knowledge-proofs - <https://ethereum.org/en/zero-knowledge-proofs/>