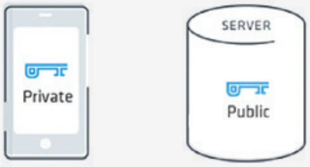
PREVEIL

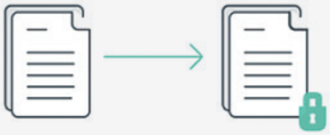
PreVeil's seamless key management system

The PreVeil key management system is designed to allow users to communicate and share encrypted data across multiple devices while completely hiding the complexities of keys from users.

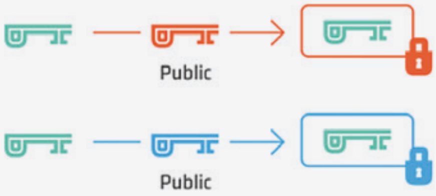
At sign up, each user is assigned a public/private key pair using Curve25519-based cryptography. The user's public key is stored on the server and is accessible to other users, and the private key is stored only on the user's device.



When a document or message is created, it is encrypted using a unique symmetric key.

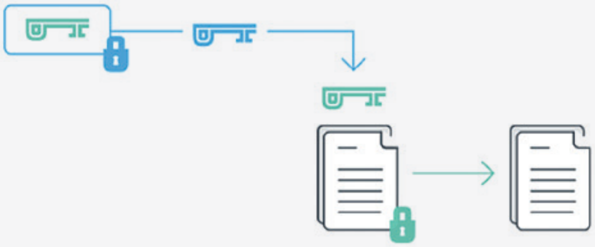


This document key is then wrapped (encrypted) with the public key of each user that has access to the document. For example, if Alice and Bob both have access to document D, the key that encrypts D is encrypted itself using Alice's public key and again using Bob's public key.



These two encrypted keys can now be safely stored on the server along with the encrypted document.

When Alice needs to access the document, the system retrieves the encrypted document as well as the encrypted key (i.e. the document key that was encrypted with Alice's public key). The PreVeil software on Alice's device then uses her private key to unwrap (decrypt) the document key. And now the document key is used to decrypt the document itself.



The creator of the document also digitally signs the document key so anyone else accessing the document can be assured they're dealing with an authentic document (as opposed to an attacker who may be trying to claim they're the author of the document).This offers significant protection from phishing and other attacks where hackers masquerade as legitimate users.

Most importantly, all of this key management and distribution is completely transparent to the user and happens automatically.

Contact Sales@PreVeil.com to learn more. | **www.PreVeil.com**