Privacy White Paper

Take back your privacy

For far too long, and without knowing it, people have traded away their complete security and privacy when storing their data in the cloud. Sync still believes in absolute privacy, and has built a cloud storage platform based on that foundation. While it may be common knowledge that encryption is the most reliable way to secure information on the Internet, it's meaningless if your cloud provider keeps a copy of your encryption keys.

Sync's unique, zero-knowledge storage platform guarantees your privacy by encrypting and decrypting your data locally (on your computer or device). Most importantly, only you have access to the encryption keys - which means only you have access to your data.

Who has access to your data?

Google Drive The Google terms of service gives their automated systems permission to access the data stored on their servers for the purpose of monetization through advertising.	**Box** The Box terms of service gives Box permission to view the files stored on their servers, to ensure users are in compliance with the Box terms of service.
Dropbox The Dropbox terms of service gives Dropbox employees and trusted "third-parties" permission to access, view and share the files stored on their servers at any time.	**Microsoft OneDrive** The Microsoft terms of service gives Microsoft employees permission to view the files stored on their servers, to ensure users are in compliance with the Microsoft terms of service.

sync.com

Technical Overview

Zero-knowledge, end-to-end encryption

✔ File and file meta data is encrypted client-side and remains encrypted in transit and at rest.
✔ Web panel, file sharing and share collaboration features are also zero-knowledge.
✔ Private encryption keys are only accessible by the user, never by Sync.
✔ Passwords are never transmitted or stored, and are only ever known by the user.

Private key

A randomly generated 2048 bit RSA private encryption key serves as the basis for all encryption at Sync. During account creation, a unique private key is generated and encrypted with 256 bit AES GCM, locked with the user's password. This takes place client-side, within the web browser or app. PBKDF2 key stretching with a high iteration count is used to help make weak passwords more cryptographically secure.

Encrypted private keys are stored on Sync's servers, and downloaded and decrypted locally by the desktop app, web panel or mobile apps after successful authentication. At no time does Sync have access to a user's private key.

Authentication and passwords

A username and password is required to authenticate and log into the Sync desktop app, the Sync web panel, and Sync's mobile apps.

During authentication, a BCRYPT hash of the user inputted password is generated locally on the computer or device, using a unique salt that is stored on the server. Bcrypt is a one-way hashing mechanism, meaning the hash cannot be unhashed or deciphered. The benefit of bcrypt is that it is slow by-design, which prevents brute force or rainbow table attacks. At no time is the user's actual password transmitted or stored.

The server authenticates against the hash, but at no time is the hash itself stored. Successful authentication allows the app to download the user's encrypted private key, which is then decrypted locally with the user's actual password.

Web panel

Sync's web panel runs client side, within the web browser, as a self-contained AngularJS app. The web panel utilizes the Stanford Javascript Crypto Library, a Javascript implementation of ISAAC (a fast cryptographic random number generator), and HTML5 local storage. This means only modern web browsers are supported - in other words, Internet Explorer 10 is the minimum requirement.

The web panel authenticates the user, downloads the encrypted encryption keys, decrypts the keys locally within the web browser, and then downloads and decrypts file and file meta data as required. Passwords are never transmitted or stored during this process.

The web panel is open source - source code is easily viewable from any web browser for those technically inclined to see how it works.

File and file meta data

File data is always encrypted, in transit and at rest. Sync utilizes a unique 256 bit AES GCM data key on each file, locked with the user's 2048 bit RSA key. File meta data is encrypted separately with the user's password (PBKDF2 key stretched) to generate a key for 256 bit AES GCM.

This happens locally on the user's computer or device before the files are transferred to Sync's servers, and ensures that the encrypted file data stored on Sync's servers is impossible to access, even in the event that the servers themselves are compromised.

Secure links

Secure links are locked with a unique password appended to the link after the hash tag (#) in the URL. The data appended to a URL after the hash tag is called a fragment identifier, which is never transmitted or stored, meaning the password is never known to Sync. The password itself is key stretched using PBKDF2 with a high iteration count, to generate the encryption key used to unlock the link.

Shared folders and collaboration

Shared folders utilize “key wrapping” to allow files to be shared between different Sync users privately, without the need to re-encrypt the actual file data when users are added and removed from the share. Sync never has access to file data, even when being shared.

When a new share folder is created, the unique encryption key on each file within the share is encrypted with a unique 512 bit share key that is created specifically for the share. The share key is then encrypted with the RSA 2048 public key of each user, and locked with the user’s RSA private key (which is encrypted with the user’s password).

Single sign on (SSO)

The Sync desktop app allows the user to log into the web panel automatically. To accomplish this securely, the desktop app generates a random one time password (OTP) which is used to encrypt the user’s 2048 bit RSA encryption keys. The encrypted encryption keys are then stored in memcache on the server for 30 seconds.

The web panel is then loaded locally, using a unique URL (also generated locally) that contains a memcache lookup value and the OTP value. These values are appended after the hash tag (#) in the URL to ensure they are never transmitted. The web panel decrypts the encrypted encryption keys locally within the web browser, using the OTP.

At no time during this process does Sync have access to the user’s raw encryption keys or the OTP. SSO can be disabled by enabling two-factor authentication.

SSL / TLS

Sync utilizes SSL / TLS (https) for all data transfers, however does not rely on SSL for any meaningful security, as SSL on it’s own cannot be trusted. SSL is applied as an extra layer on top of the 2048 bit RSA and 256 bit AES encryption used to encrypt each file. This ensures that in the event that SSL is compromised (for example a man in the middle attack, or an SSL software vulnerability), file data remains encrypted and impossible to access.

Last updated: September, 2015