



SDBIC Digital
FORTRESS
powered by SecureSafe

As simple as Dropbox, as secure as a Swiss vault



No one except you has access to your account not even Digital Fortress or SecureSafe.

Complete encryption of your data — on a customer-specific and personal basis

- Every document and every password you store in your digital safe deposit box is encrypted with an individual key. This key is then saved in a personal keychain, and then is encoded with a master key.
- The master key is recalculated directly from your password each time you log in to your digital safe deposit box. Digital Fortress and SecureSafe do not store your password or your current master key anywhere.
- Like your bank, both AES-256 and RSA-2048 are used as cryptographic standards.
- Any service that can reset your password can access your data. Because we do not save your personal Digital Fortress password anywhere, the data you store here is protected against a very wide variety of attacks.
- We cannot reset your password, but you can. To do so, please print out your personal recovery code and keep it in a safe place in case you should ever forget your password.
- Learn more at: [Digital Fortress FAQs](#)

Triple redundancy in bank-compliant Swiss data centers

- All customer data is stored with triple-redundancy in two Swiss data centers, which meet the strict requirements of the Swiss Financial Market Supervisory Authority (FINMA).
- All systems are described in full in a configuration system and any change is immediately detected and escalated. Reboots automatically lead back to the original configuration.
- Customer data is stored in a former military command bunker deep in the Swiss mountains - this site is disaster-proof. Moreover, your data is stored exclusively in Switzerland. This means that your privacy is protected by strict Swiss data protection laws.



Secure encryption for iPhone, iPad and Android apps

- Our SecureSafe App does not rely on the data protection provided by Apple or Google. All data is encrypted and stored temporarily on your mobile phone, using an additional AES-256 encryption. Because of this, users have been protected against all known attacks on iOS or Android devices to date.

Secure login with SRP and two-factor authentication

Protected by the Secure Remote Password Protocol

- Digital Fortress relies on the Secure Remote Password Protocol (SRP, RFC-2945) for basic authentication. This highly sophisticated security protocol, developed at Stanford University, protects your digital safe deposit box against common online attacks such as man-in-the-middle attacks.

Strengthen web login with SMS code

- To heighten the protection of your data, a two-factor login procedure is offered. Once enabled, you will receive a unique code by SMS to your mobile phone each time you want to log in to your digital safe deposit box. The code is needed to complete the login. This ensures that if someone steals your password and username, your account will still be effectively protected against unauthorized access.

Secure login for mobile access and for data synchronization

- The two-factor login procedure is also activated for the mobile app and for the data synchronization with your desktop.
- DoubleSec automates the two-factor authentication on all mobile devices, as well as on your desktop.



Secure infrastructure for collaboration

- In order to exchange documents securely with third parties and in Team Spaces, there is an integrated Public-Private Key Infrastructure (PKI). Shared data is encrypted with an AES-256 key, which is in turn encoded with a public key. Because of the highly transparent integration of the PKI, it does not complicate the user experience in any way.

Double protection for safe data transfer and synchronization

- Data that is uploaded or downloaded using the desktop app is always transmitted as double-encrypted. Here, both SSL and an AES-256 encryption are implemented.

Maximum protection in the password safe

- In addition to the SSL protection, particularly critical data, such as passwords you store in your password safe, is encrypted with a session key. This especially protects your digital safe deposit box when used in public, e.g. at the airport. Passwords are also encrypted in the memory of the employed computer while the password manager is in use. A password is only decrypted and released in a controlled manner when a user actually looks at it.

Open, view and send files securely



SecureViewer

With this function, you can view images and PDF files from any device without leaving a digital trace.



Secure file transfer

Transfer files of up to 2GB in size to anyone you want - and protect them with a separate security code.