GoCrypt

Highly secure file encryption and simple dispatch, great ease of use for users

There are many options for file encryption and the digital transport of data, be it email encryption with PGP or S/MIME or proprietary cloud applications. Most of these offerings have one major disadvantage: they are not user-friendly to use, users are confronted with private/public keys, signing, certificates... ... The technical setup is time-consuming and complicated, and it is not known whether the recipient has implemented all the necessary security steps. In addition, it is not known via which servers or countries the e-mails are transported. User acceptance is not particularly high due to the additional work involved.

Alternative method for encrypting emails Hybrid encryption

technology

As the developers of GoCrypt, we have taken this as an opportunity to develop a local file encryption with subsequent data transport that is intuitive and easy to use for the user at the level of the General Data Protection Regulation (GDPR). With the GoCrypt program for Windows, the user does not have to generate a key pair and distribute the public key himself, GoCrypt takes care of this with a one-time registration.

The user selects the recipient and the files to be encrypted (drag & drop) and clicks on the Go button. That's all!

GoCrypt has by no means neglected data security for the sake of convenience. GoCrypt works with **hybrid encryption technology** and uses globally recognized techniques such as symmetric AES 256-bit file encryption, asymmetric RSA 2048-bit key generation, signing, integrity checking and authentication. In addition, GoCrypt also offers an even higher level of security with the integration of FIDO tokens to enable mobile use (home, office, notebook). The FIDO Alliance includes the largest tech companies, such as Microsoft, Google, Intel, Apple and many more. Our FIDO token not only supports Fido2 or Fido U2F but also has the applets Open PGP, Smart Card (PIV) and HOPT integrated. This means that the Fido Token can not only handle GoCrypt encryption, but can also be used for logging in / authenticating on many websites (Google, etc.) or for password less logging on to the computer.

For users who do not want to use a FIDO token, GoCrypt offers a version without FIDO, of course the two versions can be combined with each other.

GoCrypt is easy to use and the key exchange is automatic.

"Zero-knowledge" principle. Nobody except the recipient has access to the encrypted files - not even GoCrypt!

GDPR-compliant, in accordance with applicable laws in Germany and the EU.

Highest security, option between different security levels (FIDO)

Made in Germany, hosted on a German server

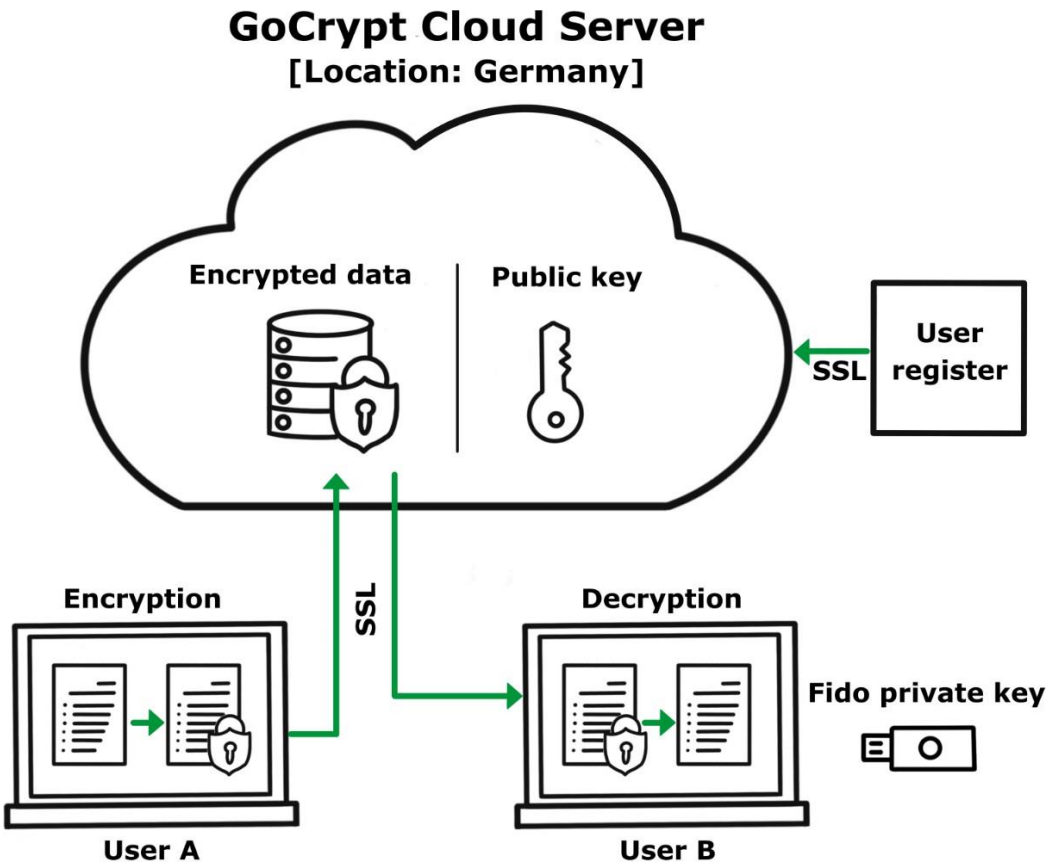
How it works:

1. Send file: User A wants to send a file to user B via the Internet.

2. Encrypt & transfer: User A encrypts the file locally on their computer with GoCrypt and sends it to the GoCrypt server. The original file remains on the computer.

3. Notification: User B immediately receives a notification about the provided file.

4. Download and decryption: User B downloads the encrypted files. After downloading, they are automatically decrypted locally on his computer using GoCrypt.



In addition to encryption, the focus is on user-friendliness:
With GoCrypt, everything is done with just a few clicks:

- You select your files.
- You determine the recipient.
- You click on "GO" and GoCrypt does the rest.

Immediate notifications:
The recipient is notified immediately when a file is ready for them. One click and the encrypted file is downloaded and then automatically decrypted on their computer.

Safety with every step:
During registration, GoCrypt generates a unique key pair for each user:

- **Public key:** Is stored on our server.
- **Private key:** Is securely stored locally on your computer. For Premium users, the private key with the corresponding e-mail address is stored in the Fido token.

- The files are **only** encrypted and decrypted on the local computer. The original files are **not** sent/received unencrypted via the network/internet, but only encrypted. There is no possibility of attacking our servers or our network (e.g. with traffic sniffers) to gain access to the original files. Public networks also offer no vulnerabilities for sent/received files.

- Sent files can only be restored to their original state by the recipient. Even the sender can **no longer decrypt** the file once it has been encrypted. The encryption technology is designed in such a way that no one else can decrypt the file.

- The files are encrypted and decrypted using the AES algorithm (256-bit). The symmetric key for the AES algorithm is then encrypted with a 2048-bit RSA key.

- A theoretical brute-force attack on a 2048-bit RSA key would take up to 300 trillion years using today's computer technology.

- The use of a Fido key further increases security:

- Protection against phishing
- No shared secrets, the private key never leaves the Fido key
- Man-in-the-middle attacks are made more difficult with the Fido Key.
- Physical security with the Fido Key compared to passwords only
- Authentication and integrity check with the Fido Key

GoCrypt supports data classification for file sharing

Data classification plays a critical role in access control, helping to ensure that only authorized users have access to certain data based on its classification.

Data classification is often applied to existing documents after the fact. GoCrypt file classification allows organizations to define the sharing of sensitive files based on the sensitivity of the data. Data is typically categorized as Public, Internal, Confidential and Highly Confidential. Based on these classifications, appropriate access rights can be assigned when sharing files, so that, for example, only employees with the necessary authorization can access confidential or highly confidential information.

By restricting access to sensitive data according to its classification, organizations can reduce the risk of data breaches and unauthorized access. This is especially important for data that contains personal information, trade secrets, or other types of sensitive information.

Many data protection regulations require organizations to take appropriate measures to protect sensitive information. By applying data classification to access control, organizations can demonstrate that they have taken proactive steps to ensure the security and confidentiality of data, helping to meet regulatory and industry requirements.