How does GoCrypt work?

GoCrypt uses asymmetric cryptographic algorithm - RSA (https://en.wikipedia.org/wiki/RSA_(cryptosystem)) to encrypt/decrypt the file you send. The peculiarity and advantage of the RSA algorithm is that it is a so-called asymmetric algorithm, i.e. there is a pair of keys used in the process - public key (used for encryption of the file) and private key (used for decryption). The names of the keys determine their use, i.e. the public key can be shared with anyone, there is no vulnerability, but the private key must be kept secret. Please note, if private key is lost, it is impossible to get it back somehow, so keep it carefully to avoid loss.

RSA key pair is generated when you register in GoCrypt system, public key is sent to the server where it is permanently stored, private key is kept secretly on your computer (in a version without token), or on a token, both passwords protected.

When the file is sent, GoCrypt needs the recipient's public key (stored on the server) to encrypt the file's contents. After encryption, the file is uploaded to the server for temporary storage. The file never leaves the sender's computer unencrypted, ensuring that no data can be stolen or shared in any way. When the file is uploaded to the server, the recipient receives a notification about the file waiting to be downloaded. Encrypted file is downloaded from the server, and using the recipient's private key, the file is decrypted. The recipient's private key never leaves the computer (for the version without a token), for the version with a token it is even more secure, because the decryption takes place inside a token, in this case GoCrypt does not have access to the private key.

Registration Process

During registration, GoCrypt generates a unique pair of private and public keys for the client. Public key is sent to the server where it is permanently stored, private key is securely stored on your computer (for version without token), or in a token. Mandatory action for registration - e-mail confirmation. After the key pair is generated, the server automatically sends an e-mail message to the e-mail address specified during registration with a link to confirm the e-mail address. You need to check the incoming folder for emails from noreply@gocrypt.de (you may need to check the spam folder) and open the email confirmation (account activation) link in a browser (copy/paste the link in a browser, or click on it to open it automatically in the default browser). If the confirmation process is successful, a successful web page should be displayed in a browser.

Security QA

Q: Is it possible for someone to steal my private key?

A: For version without token: private key is stored on your computer, but it is encrypted with password. Without the password, the private key is useless. For token version: private key is stored inside token, it never leaves token. Even if someone gets physical access to your token, they can't use it unless they know the token password.

Q: Is it possible that the file I send/download will be stolen by sniffer (traffic analysis tool)?

A: No, it is impossible. The file you send/download never leaves/comes to your computer decrypted. Encryption is done before sending and decryption is done after downloading, so there is no point in analyzing the traffic, files come through the network only encrypted.

Q: I'm going to reinstall Windows; will this affect the GoCrypt installation?

A: For version without token: private key is stored in Windows registry, it must be kept during Windows update (installation of update or a major update such as migration from Windows 10 to Windows 11). If it is a clean installation, you will have to register with GoCrypt again. For version with token: Changes in Windows do not affect GoCrypt, because it uses token to store private key.

Technical Information

Server Communication

GoCrypt communicates with the server using the GRPC protocol/framework. The server side provides a set of functions (Server API) to communicate with it. Authentication is required for some of the server API functions; it is performed after the JWT token expires (see Authentication flow below) during the next API call.

Registration flow

Registration occurs as a flow of the following events:

- GC collects information from registration form, sends registration request to server (via server API);
- Server, accepting the registration request, generates a response containing a nonce. Nonce - randomly generated 32-byte array;
- GC generates RSA 2048 key pair (depending on version, GC either uses .NET Framework functions to generate a key pair or calls Token SDK to force it to generate keys on a token);

- GC signs registration nonce received from server using generated private key and sends signed nonce + public key to server to complete registration;

- Server receives complete registration request containing signed nonce and user's public key. Nonce signature is verified against public key if signature is valid (this action proves that nonce was signed with private key tied to received public key) at first step, and then nonce is validated for correctness and time validity (nonce is valid only for short period of time to avoid it to be brute forced or manipulated somehow). If nonce passed validation rules, server sends email confirmation message, to an email address specified at registration.

- To start using GC, user must receive email with activation (confirmation) link. This link should be opened in browser to confirm that user owns this email address. To avoid manipulation with the activation link, it also has an expiration period of 3 hours from the moment of registration.

Authentication

Authentication process is similar to registration, based on a nonce signature. The flow is as follows:

-GC sends authentication request containing email address of registered account;

- Server validates email address and associated user, generates nonce - 32 random bytes array, sends it back to GC

- GC signs nonce with private key, sends it back to server as complete authentication request;

- Server validates signed nonce against public key for that user stored on server, if signature is correct, it also validates nonce if it is correct and not expired. If nonce validation passes, server generates JWT Token using HMAC-SHA256 algorithm. JWT Token is valid for 5 minutes, after token expires authentication process is repeated;

- GC receives JWT Token to use for server communication during token lifetime.

Encryption

File operations with server API are performed under authenticated channel. Below cycle repeats for each sending file:

- GC calls server to create file upload request;

- GC generates AES 256-bit key and init vector key;

- GC computes SHA256 hash of original file;

- File to be sent is encrypted with AES key;

- AES key is encrypted with recipient's RSA public key

- Original file hash, encrypted file, encrypted AES key, and AES initial vector are sent to the server.

Decryption

File operations with server API are performed over authenticated channel. The cycle below is repeated for each sending file:

- GC calls the server to create a request to download the file;
- Server responds and returns encrypted file, encrypted AES key and AES init vector to GC;
- GC decrypts the AES key using the recipient's private key. GC decrypts file using AES key and init vector;
- GC computes file hash of decrypted file, calls server to download full request;
- Server checks whether the original file hash matches the recipient's decrypted file hash. If hashes match, server marks file as downloaded and lets GC save file to user's desired location.

November 2023