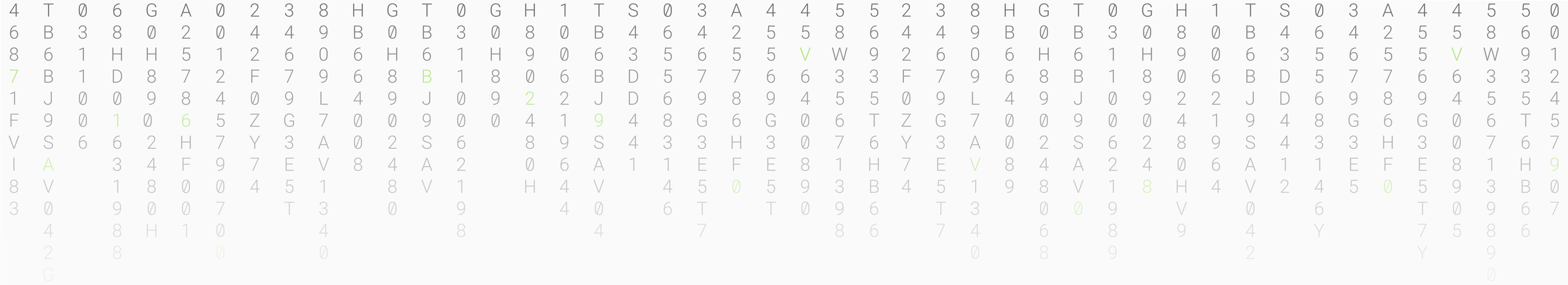

USECRYPT



# Bringing privacy back

TECHNICAL DETAILS

# How does Usecrypt work?

## A DEDICATED DESKTOP APPLICATION

Unlike many other products such as Dropbox, UseCrypt is an author's application, which completely eliminates the risk of working through a web browser and provides the user with a guarantee that the service provider will not have any access to his/her data.

Dropbox uses the "at-rest" model encryption, which means that the data are encrypted only on the server. During the transmission, they are protected only through SSL. You cannot clearly determine at what point the data are encrypted because the definition of "encryption-at-rest" allows us to interpret it broadly. The "at-rest" model also means no confidentiality as the data encryption keys are held by the service provider. That causes the service provider to access the data at any time.

UseCrypt encrypts data already on the workstation; then it sends them in an encrypted version through the UST secure author's communication channel. No one is able to decrypt them and has any access to customer data.

## UST COMMUNICATION ENCRYPTED CHANNEL

Having downloaded and started the application, a UST (UseCrypt Secure Tunnel) communication encrypted channel is established based on the Diffie-Hellman key agreement algorithm (defined in RFC 2631, IEEE 1363-2000 or ANSI X9.42:2003 standards), which ensures the security of data exchange between the application and the server.

## GENERATION AND DISTRIBUTION OF A UNIQUE ENCRYPTION KEY

At the time of registration, two long and strong private random keys RSA 2048 are generated as a result of the cryptographic distribution into two parts – the previously described HVKM. The unique “half” of the user is stored on the workstation in the form encrypted with the AES256 key, while the other part is on the server, also in an encrypted version that never leaves the server. When you work with an application, both keys are always separated. In case of loss of workstation or forgotten password, the user can generate a “recovery key”. The recovery key is a copy of the key half of the user device. It is generated in the form of a file that the user stores on a separate external device, preferably encrypted and in a safe place (e.g. deposited in a safe). Each recovery key is also randomly secured with a generated one-time password that the user should store in a separate location. Such process additionally secures the recovery key in the event of its acquisition.
In addition, the configuration of the application on a given device contains the parameters of the specific workstation which UseCrypt is registered on (authentication of a particular device).

## A MECHANISM OF KEY ENCAPSULATION

File encryption is performed on the user's workstation (the workstation must be in online mode) using the AES256 algorithm which is generated by the means of the KDF function. Decryption is performed in two steps, using the RSA keys. The first stage takes place with the "half" on the server, while the second stage – on the workstation. In addition, each file encrypted in UseCrypt is encrypted with a separate AES256 key, and each AES key is encrypted with an RSA public key.

Encrypted file sharing consists in creating an encrypted capsule (i.e. KEM - Key Encapsulation Mechanism), stored on the server and generated when the AES encrypted key of the file is sent to the server. While being shared with another user, it is then encrypted with the recipient's RSA public key, and then securely re-placed on the server as an encrypted secure capsule attributed to the designated recipient.

When you want to deprive the user of the access to the file, his/her capsule is deleted from the server and he/she immediately ceases to have access to the file, i.e. it is not possible to download and decrypt it. This is an additional advantage of UseCrypt over standard e-mail; when an e-mail has been addressed to a wrongly selected recipient, we no longer have a possibility to undo this process and the critical attachment remains in the e-mail server files.

## SECURE BY DESIGN

The system is designed under the so-called secure by design [program], i.e. the system in the design phase is created to be a secure space that excludes the chance of external interference and hiding backdoors that make unauthorized access to system resources possible.
The algorithms, mechanisms, and cryptographic protocols used in that solution, according to the manufacturer's

declaration, make it resistant to the well-known cryptanalysis methods, and the manufacturer itself has no technical possibility to access customer data.

## BENEFITS FOR IT DIRECTORS

The client software of the system can be installed on computers and smartphones running the Windows, Android, iOS and Mac OS operating systems. The UseCrypt system has a functionality that allows it to grant access rights at the file and folder levels by the means of a mechanism of managing the rights that are assigned by the owner of a given document within the implemented policy. UseCrypt does not integrate with directory services. Cryptomind assumes that integrating its solution with another device, such as active directory based on Lightweight Directory Access Protocol (LDAP), can be connected with promoting additional vulnerabilities and using the services to take the data over. The attacks based on the Active Directory vulnerability are well-known. The next step in development of the system will be the implementation of UseCrypt API, which will enable integration with external systems, such as workflow or office document loggers, and increase the security of such systems.

The system allows you to gradate the levels of rights by the means of which you can create several user access levels in a simple and secure way. The assigned rights may have an orderly and hierarchical structure that can be freely expanded.

A data owner is at the top of the hierarchy, and below there are operators who can assign rights for specific data. In addition, each user-initiated operation is confirmed with a digital signature, which allows us to eliminate such situation when the user denies performing a specific action in the system.

UseCrypt changes the situation of IT directors, security chiefs and administrators. In the systems where this solution is not used, the IT director has access to all

of the company data. With UseCrypt, the IT director does not have any technical possibility to view employee-encrypted data. It means that any attack on his/her account does not give any technical possibility to access the entire company resources. The result is that IT staff cease to be a primary target of attacks aimed at gaining access to sensitive data.

All this makes UseCrypt an important new element of the security system design that – in addition to the advantages for IT directors – also benefits the entire organization, making files storing and exchanging much safer.