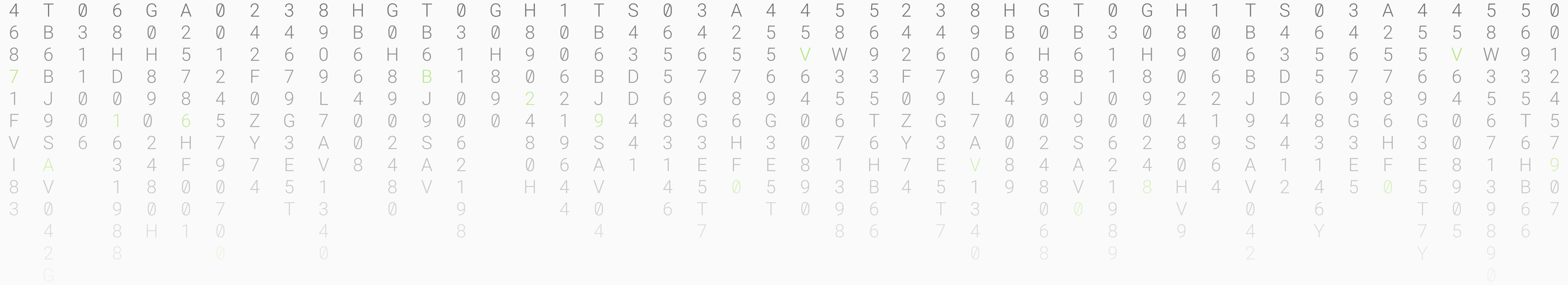
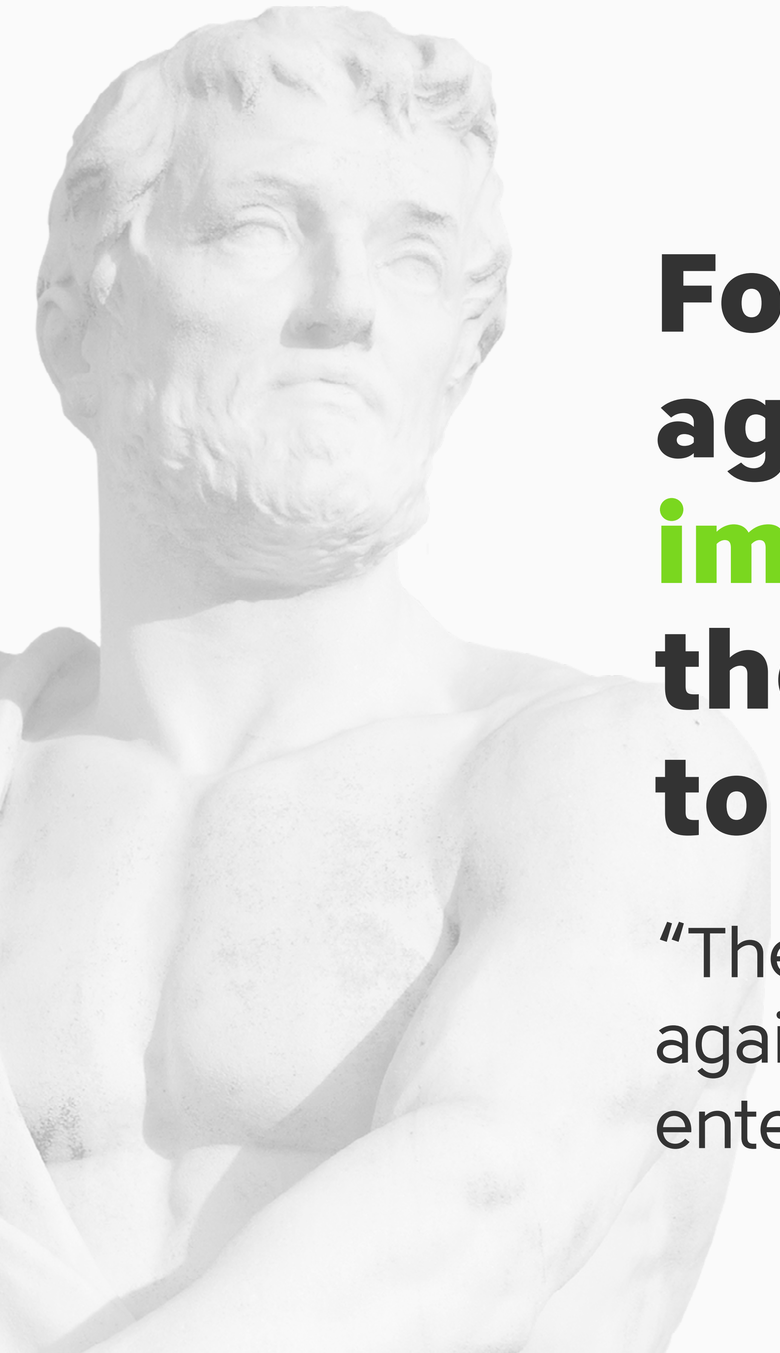

USECRYPT



Bringing privacy back



c. 100AD

For centuries, people have agreed that privacy is important, even when they didn't know how to define it yet.

"The desire for safety stands against every great and noble enterprise." — TACITUS

14c.

The first definition of privacy has its origins in late Middle English word:

private (adj.), late 14c.

pertaining or belonging to oneself, not shared, individual; not open to the public

Privacy used to be obvious. Today, it must be protected. That's why we've created the most-advanced data encryption system. We're bringing privacy back.

Our legacy speaks for us

Photo: Polish Press Agency

1932

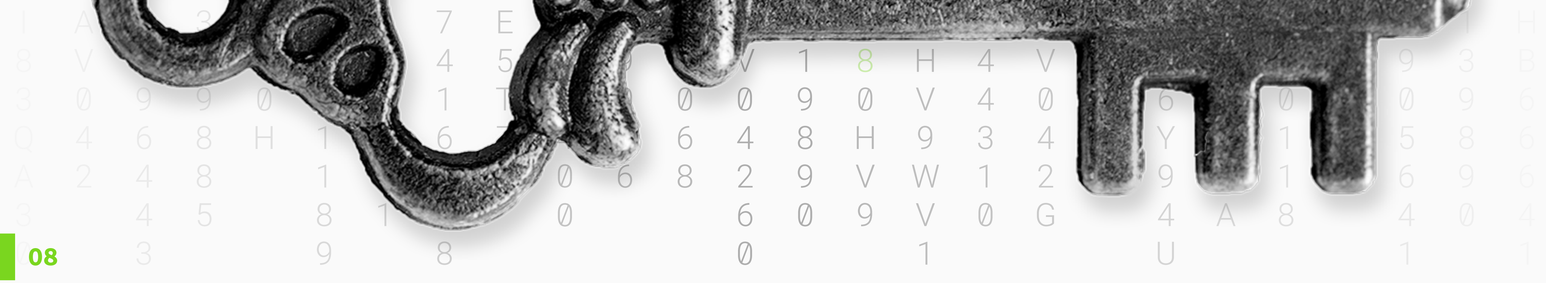
Enigma was a modern cipher machine used to develop codes and send secret massages during World War II. It had approximately 158,000,000,000,000,000,000 possible solutions, and was supposed to be unbreakable.

And it was. Until 1932, when **three Polish mathematicians finally cracked Enigma's code.** That was a milestone in WWII. Even the CIA agrees.

2017

Now, 85 years after the Enigma code was cracked, the enemy has become virtual.

How can you protect yourself from someone you cannot see?



HVKM

What makes your data truly private? The solution is HVKM.

Hybrid Virtual Key Management is a unique method of encrypting all types of digital data. It’s based on cryptographic division of the RSA private encryption key into two parts.

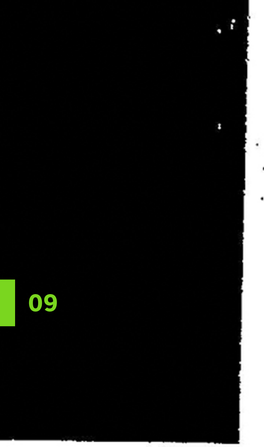
HVKM technology is registered by the European Union Intellectual Property Office and the International Bureau of the World Intellectual Property Organization.

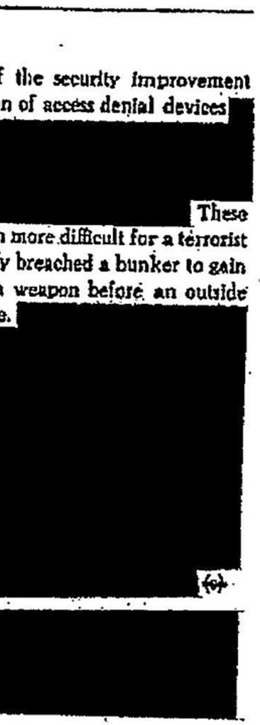
The key used to encrypt every file works only when you are in possession of the partial keys. Your unique half of the private key is stored on your device, the other part is stored on the server. Decryption is possible only when those two parts of the key work together in the on-line mode. Your part of the key is protected by your device using various cryptographic keys. The other part is protected by the server, which controls the integrity of the whole process. Neither sever nor device can decrypt the data by itself.

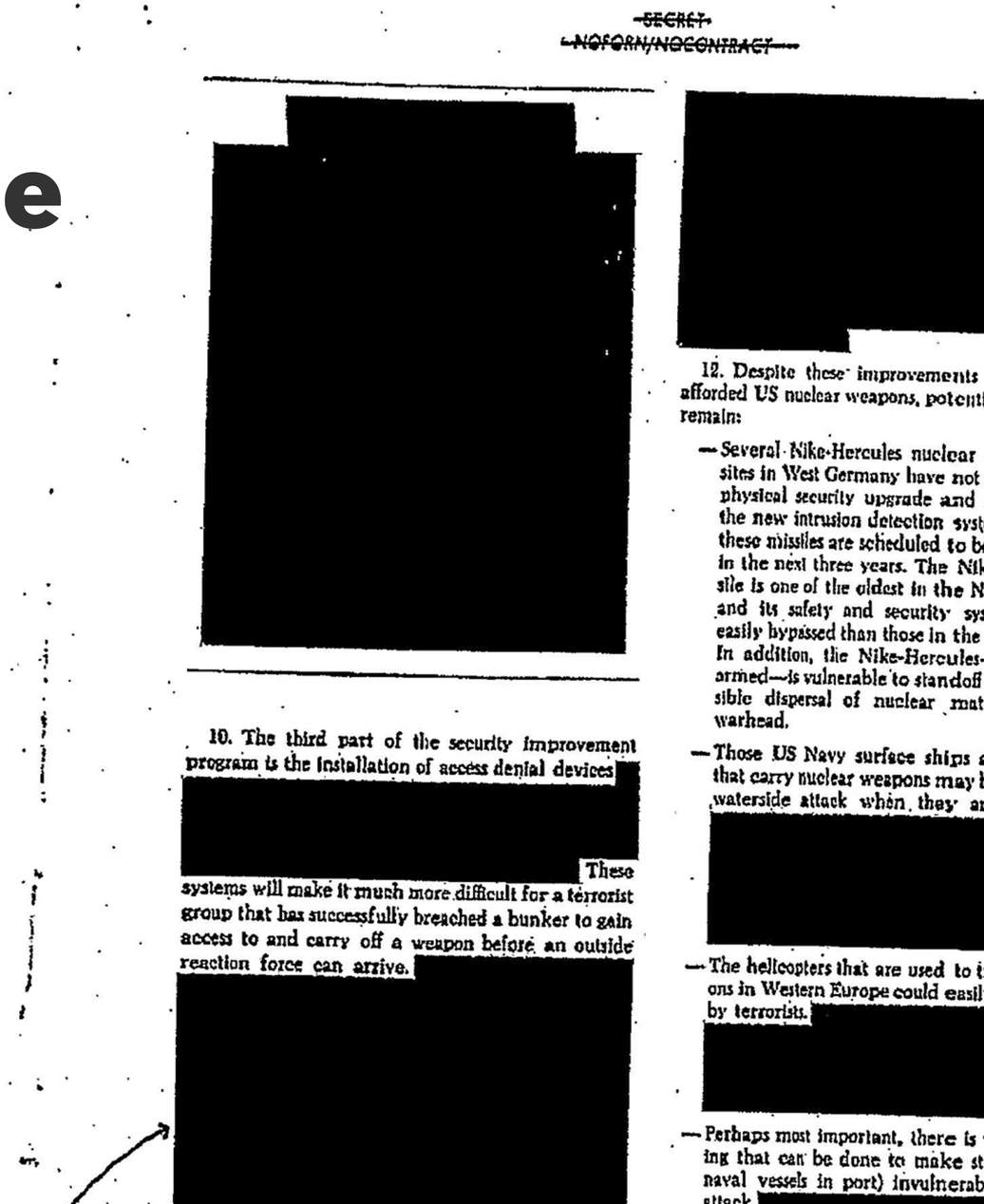
WHY ARE WE UNIQUE

With HVKM, no one can see your files. Not even us.

Neither software producers nor system administrators have the technical possibility to access your data, because they don't have your unique half of the private key. Not only files are encrypted, but also their names are. The only thing that we know, is a storage quota you use.







NEW ELEMENT OF SECURITY SYSTEM

Privacy by design

01 Revolutionary HVKM mechanism guaranting confidentiality for enterprises and private users

02 End-to-end encryption

03 Strong connection between client’s device and service account (device authorization)

04 Available in SAAS and on-premise

05 100% Polish solution with no hidden backdoors

USECRYPT SAFE

The key to a secure world

Usecrypt is **a desktop app, which encrypts data in connection to a server by using HVKM technology.** With end-to-end encryption you can easily secure your files and:

01 Store

Store and archive files on your device and in a secure cloud

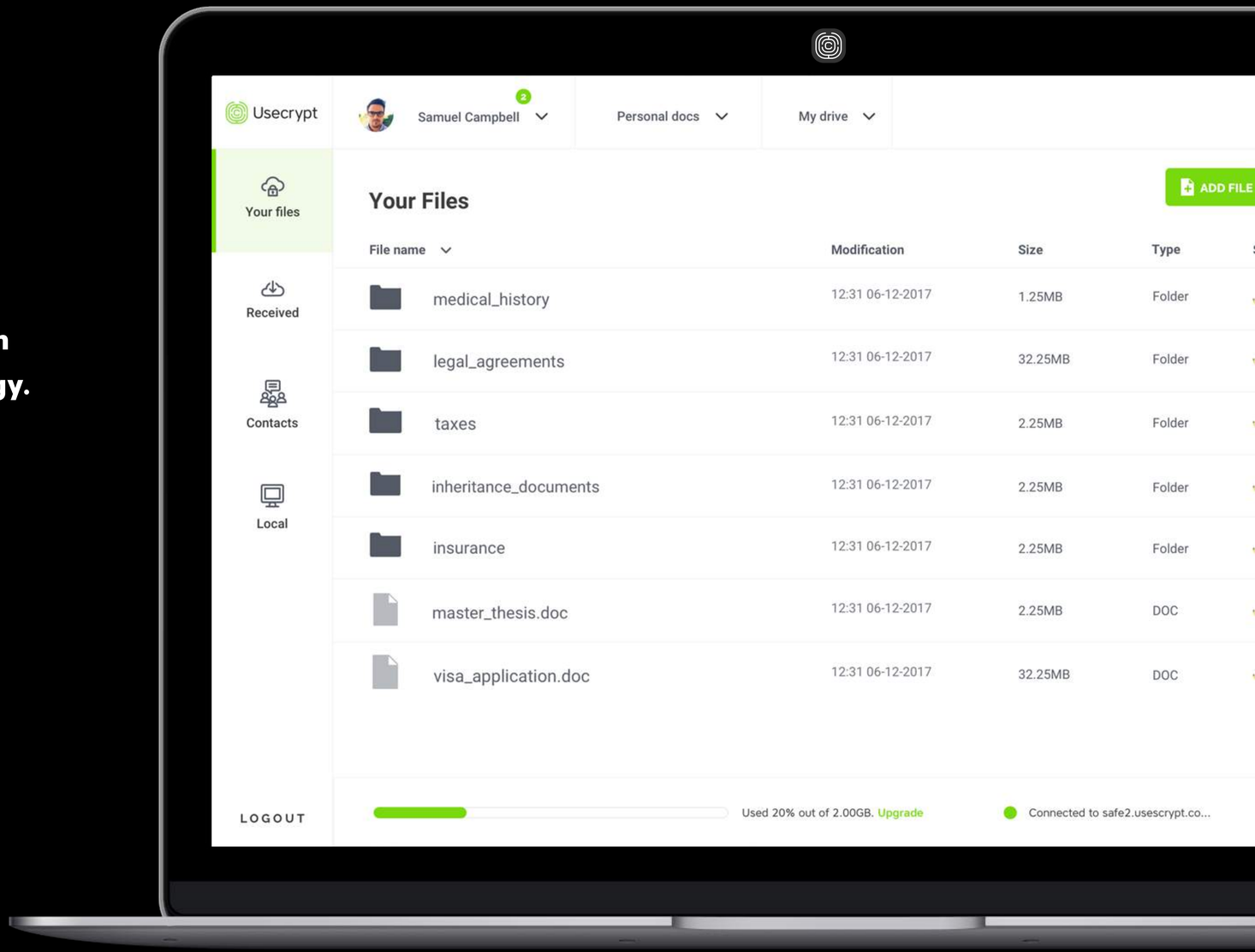
02 Send

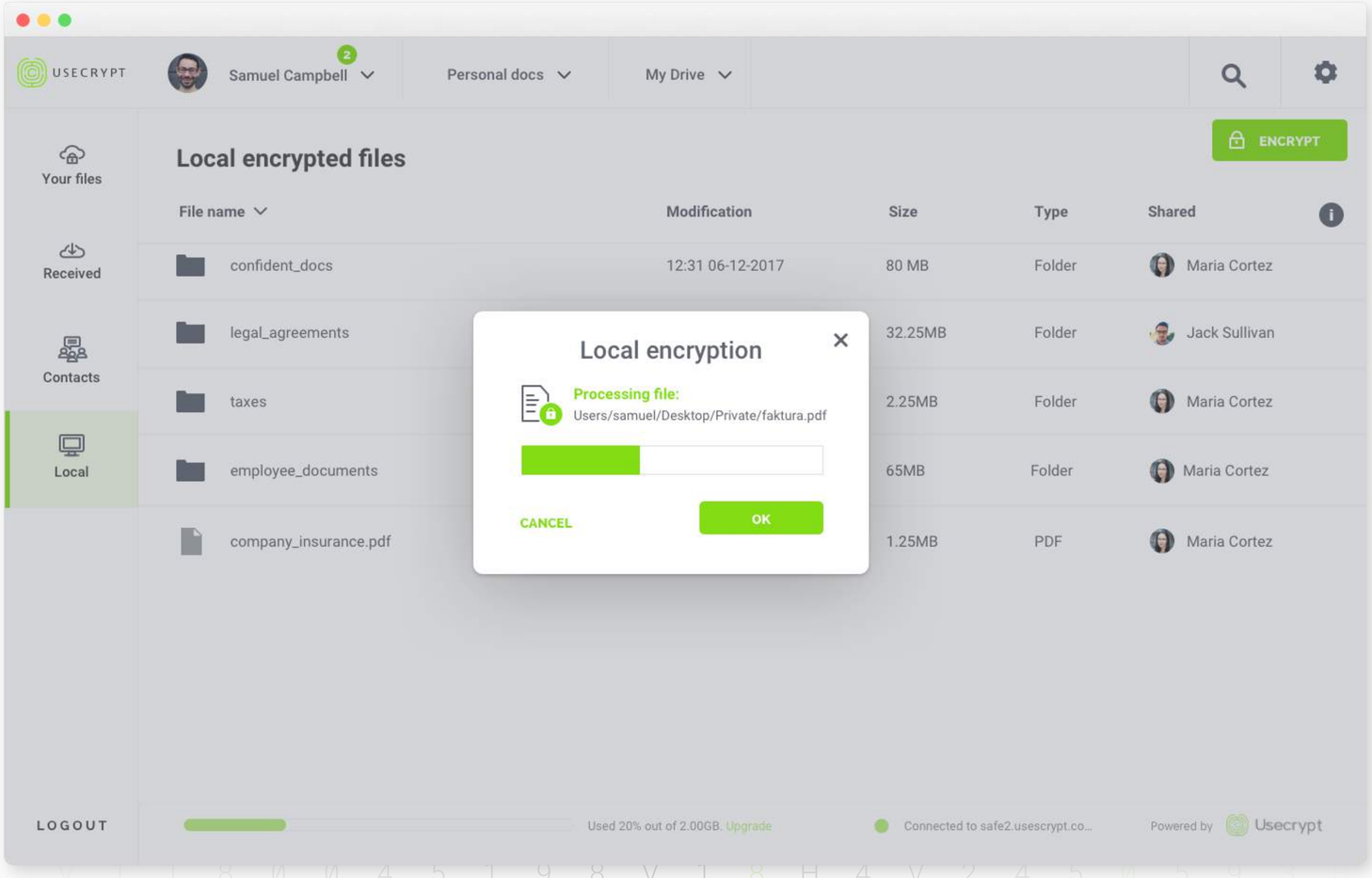
Send files to trusted recipients

03 Share

Share data among groups and companies

Available on:





Store & archive

Data is encrypted on your device using HVKM. It is encrypted in .enc format in the folder chosen by you.

Secure server

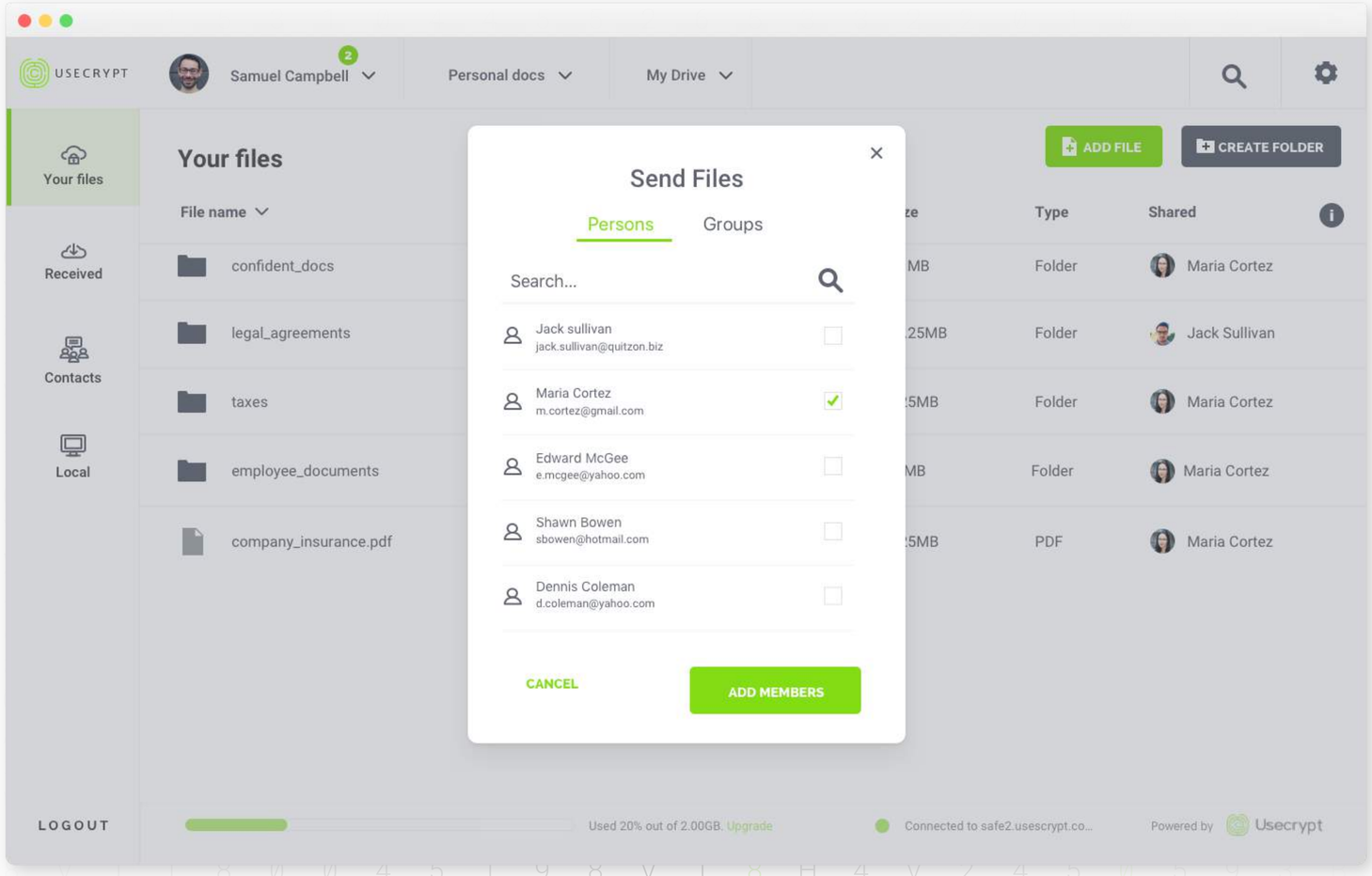
You get a safe storage for your data. You can remove the original file from your device and leave only the encrypted copy in a cloud.

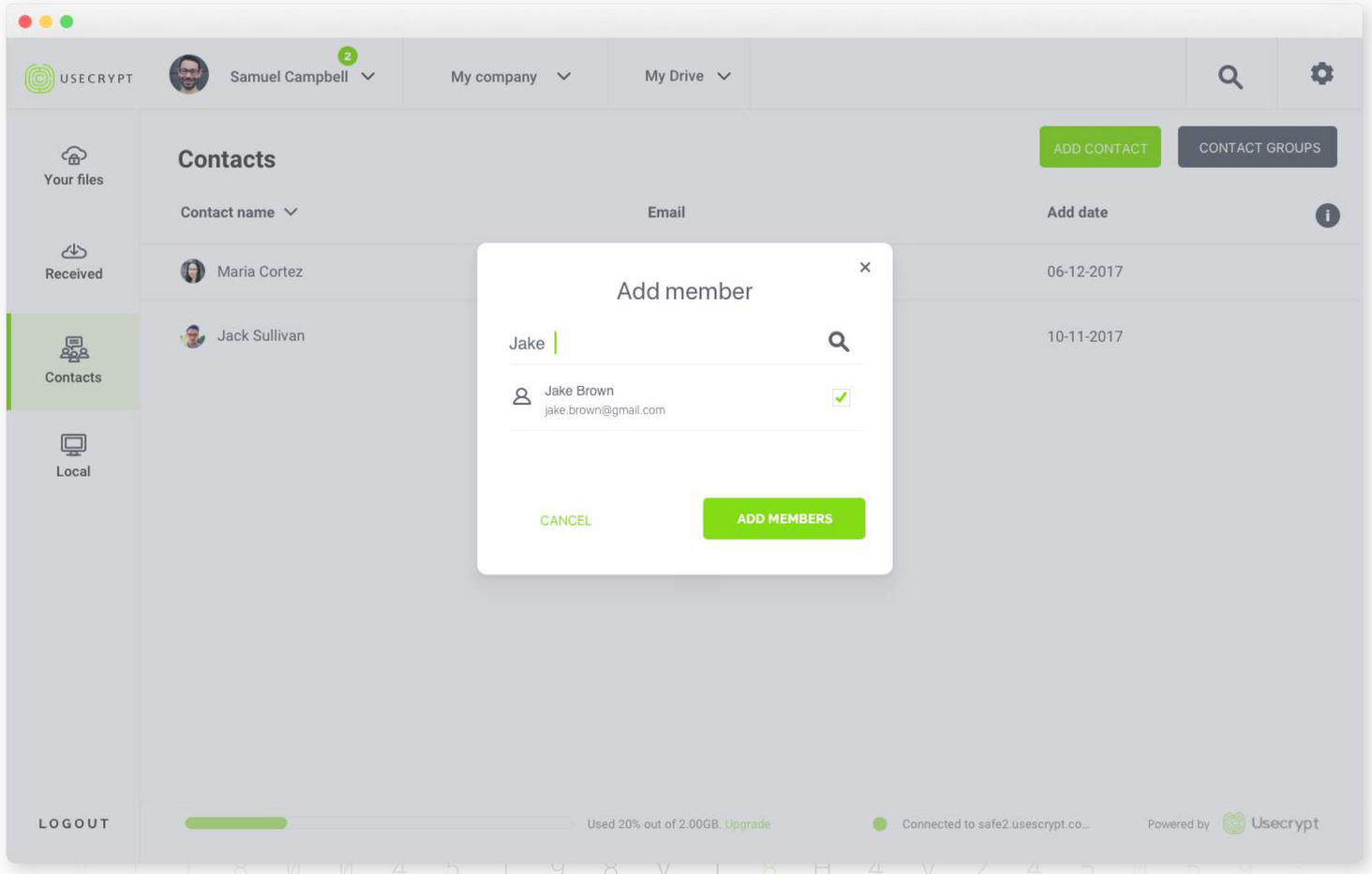
Send

You can send any encrypted file to trusted recipients and track every modification. You are the owner of your data, so you decide who sees it. Files are always encrypted with HVKM and sent via Usecrypt Secure Tunnel. Once they get access to the files, recipients will get informed about it via e-mail.

Other functionalities:

- taking back the access to the files that were already sent,
- notifications about receiving and opening the file by the recipient,
- unlimited file size.





Share

You can effectively and securely share any data within your group of trusted members. You can create larger teams and share specific files within members. App allows three different levels of data access: data owner, operator and user. You can also track every operation made on the file.

Other functionalities:

- categorized access to the resources,
- elements of files workflow policy,
- space saving – once you store a file on the server, it won't get multiplied.

OUR PARTNERS

They take privacy seriously

IBM Bluemix

Usecrypt uses IBM Bluemix Bare Metal Servers, which guarantee a worldwide range and huge computing power. IBM Bluemix also lets the biggest companies have their servers physically separated from the servers of other clients.

EY

Usecrypt has qualified for the EYnovation program for the fastest growing and most innovative Polish tech companies. EY and Usecrypt work together for the enhancement of data protection in business activity.

WAT Military University of Technology

Usecrypt got a positive opinion from WAT regarding the cryptographic protocols used in the tool. The University administration also uses our app to store and share data.

INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

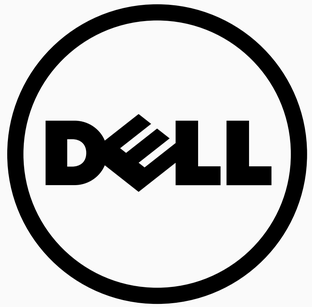
“The Usecrypt tool meets the requirements of encrypting data and can be used as an amplification of the complex secure system of the company’s software.”

IBM **Bluemix**

ENCRYPTED IT INFRASTRUCTURE

The most secured cloud in the world

All data encrypted by Usecrypt is securely stored on the **IBM Bluemix** cloud on bare metals servers. Usecrypt is the first Polish company offering full secured and encrypted IT infrastructure, resistant to all cryptographic methods know to date.



USECRYPT X DELL

Working with the biggest players

In Poland, selected Dell’s best selling laptops have Usecrypt app pre-installed. That makes Dell users prepared for the new GDPR law implementation at the moment of device purchase.

THE TECHNOLOGY

See what makes our technology so unbreakable.

THE TECHNOLOGY

Eight layers of security

We use well-known, advanced cryptographic mechanisms that ensure the highest level of security. All the algorithms and cryptographic protocols have certificates from specialized institutions.

01 HVKM
Hybrid Virtual Key Management

02 E2EE
End-to-end encryption

03 UST
Usecrypt Secure Tunnel

04 DH
Diffie-Hellman

05 AES
The Advanced Encryption Standard

06 RSA
Rivest–Shamir–Adleman

07 MAC
Message Authentication Code

08 KDF
Key Derivation Function

HVKM

Hybrid Virtual Key Management

HVKM is our original technology of asymmetric encryption process. You encrypt files with a public key and the receiver decrypts it by using their private key. The private key is divided into two parts. One of them is stored on your device, the other part is kept on the server. To decrypt the file, both parts of the private key must be used at the same time.

E2EE

End-to-end encryption

E2EE is a system of communication where only the communicating users can read the messages. Your data is always secure, whether you want to store, share or send it via Usecrypt. Only you and the people you choose have the keys to decrypt and view the files. Nothing leaves your device unencrypted – your files are always protected.

UST

Usecrypt Secure Tunnel

Are you familiar with little padlocks that you see in your URL bar? It’s the sign of the SSL protocol and it means that your data is being sent securely. In theory. The SSL protocol has gaps, which make it vulnerable to data captures. **Usecrypt uses its own communication tunnel,** based on strong asymmetric and symmetric algorithms.

DH

Secure connection

Diffie-Hellman is a method of securely exchanging cryptographic keys over a public channel. It’s used in Usecrypt for the first connection between the device and server to establish a Usecrypt Secure Tunnel (based on standards: RFC 2631, IEEE 1363-2000 and ANSI X9.42:2003).

AES

The strongest encryption

The Advanced Encryption Standard is an algorithm used globally, also known by its original name – Rijndael. It's a specification used in encrypting data. It's based on the strongest 256 bit symmetric key randomly chosen by your device (in accordance with FIPS 197 norm, certificate in X.509 form).

RSA

Based on verified methods

RSA is a well known and widely used algorithm, where the encryption key is public and is different from the decryption key, which is private (in accordance with PKCS#1 2.1 standards). This method is used in Usecrypt together with the KEM encryption technique, which eliminates the complexity of the padding scheme.

MAC

Resistant to hackers

Usecrypt applies a Message Authentication Code (MAC) to each file. Every file has a randomly designated code. Even if somebody hacks your system, they can’t modify anything without your knowledge. And they can’t modify your file, due to the fact that the key to it is stored and encrypted, and can be decrypted only by your device.

KDF

Securely generated key

KDF is a mechanism of creating cryptographic keys. It’s an essential component of cryptographic systems that basically takes a human readable text password and turns it into bits and bytes to be used as the key to a cryptographic algorithm (in accordance with the IEEE 1363-2000 standards).

GDPR

Get Usecrypt now or cry later

General Data Protection Regulation (GDPR) will change how businesses and public sector organizations process and handle data and information about customers.

This European Union law will come into force on May 25, 2018. If there is a security breach in data administration, an organisation can be fined up to €20 million. That’s quite a lot. To avoid leaks, data must be encrypted. Efficiently.

GDPR

With Usecrypt, all technical GDPR requirements are covered:

01 Personal data encryption

02 Worksation protection

03 Personal data transfer protection

04 Secured archivization

05 Data access policy

06 Right to be forgotten

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.

PLANS

Why buy expensive hardware, when you can get inexpensive software?

Pro

$13

Per user per month

- 1-25 licenses
- starting at 100GB per user
- for personal & business use
- 24/7 support line

Custom

$

Custom plans for larger teams

Need a non-standard offer for an enterprise? We will prepare a dedicated plan for your organization

Additional cloud storage: **$65/1TB per month**
On-premise: **$26/1TB per month**

Q&A

Still have questions?

Good, because we have answers. Visit our Q&A section at:

USECRYPT.COM

CONTACT

We’re here for your privacy

Tel.: (+48) 22 213 96 44
Email: office@usecrypt.com
www.usecrypt.com

ul. Twarda 18
00-105 Warsaw
Poland