Cryptshare®
Making e-mail better

Microsoft   suse   vmware   Our thanks to IBM

Data Transfer

Encrypted and stress free with **Crypt**share.
Guide and Terms of Use.

- Keeping your e-mail private
- Removing file size limits
- Bringing IT compliance

Guide on how to use Cryptshare®

Send messages and files securely

The Cryptshare® Web application allows you to easily and securely exchange sensitive information by storing encrypted files* and messages on your Cryptshare server. The files can be retrieved with a password. The server informs the recipient and sender about the operations on the server enabling you to keep on top of what is going on with your data.

When you configure Cryptshare for the first time your identity is authenticated via your e-mail address. This verification is valid for a typical maximum period of 30 days, although this is a configurable setting. After that time, you are required to verify again when logging in.

When you change your e-mail address you need to verify again. You are recommended to set a password of at least eight alphanumeric characters but password rules are also configurable and may be varied by policy rules and due to classification of your data.

To illustrate the functionality of the Cryptshare web application, the following two procedures are explained below:

1.   Procedure when providing files: pages 3 - 10
2.   Procedure when retrieving files: pages 11 – 12

Release Notes

Please find information on release notes and new product features in our partner area here: https://login.cryptshare.com/
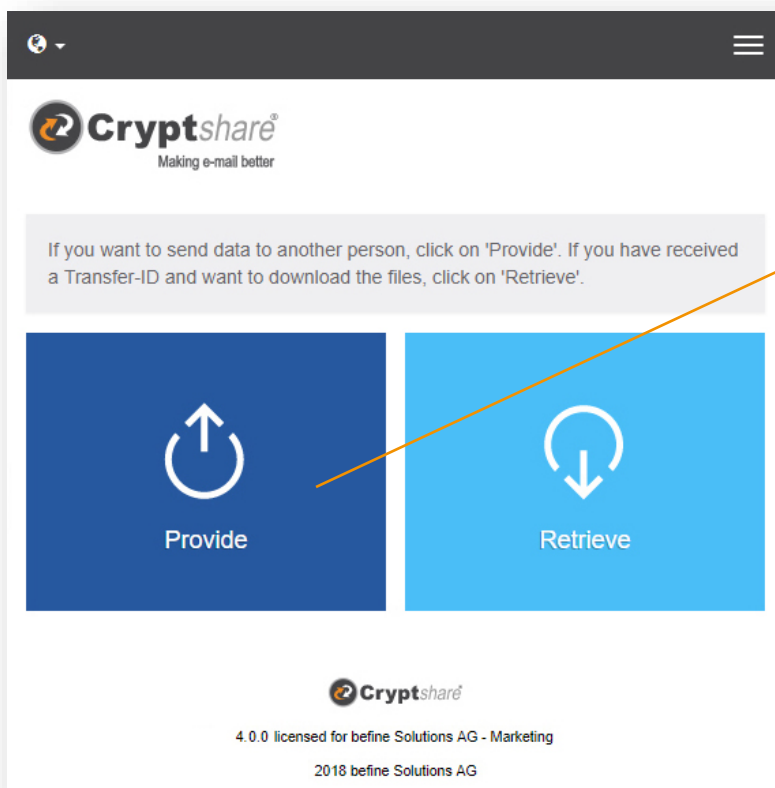
*as of 10/2017 Cryptshare uses a 256 Bit AES Encryption.
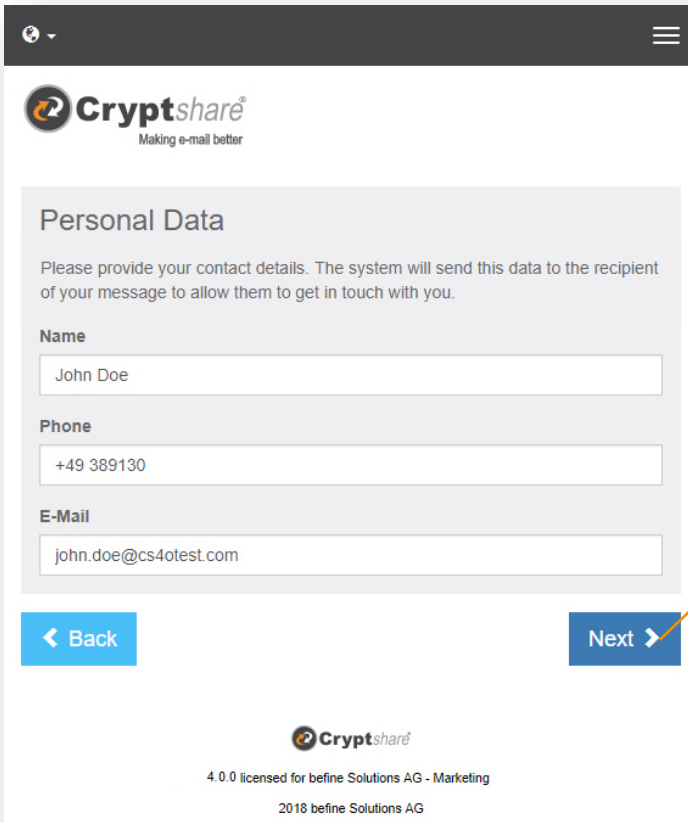
Procedure when providing files

The steps needed to exchange information are explained in the screen masks.

Use a browser of your choice and go to the Cryptshare web application on:
https://demo.cryptshare.com

You will see the following start page:

Step 1

Click on **Provide**

Cryptshare®
Making e-mail better
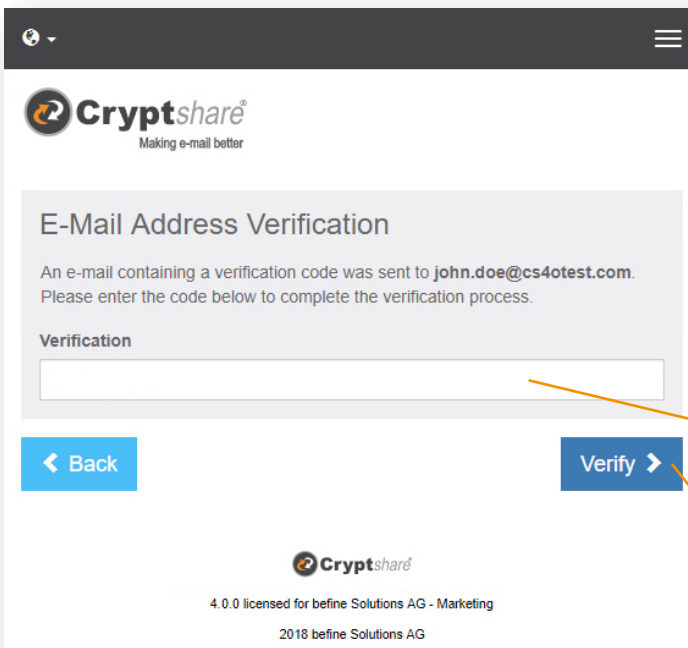
Step 2

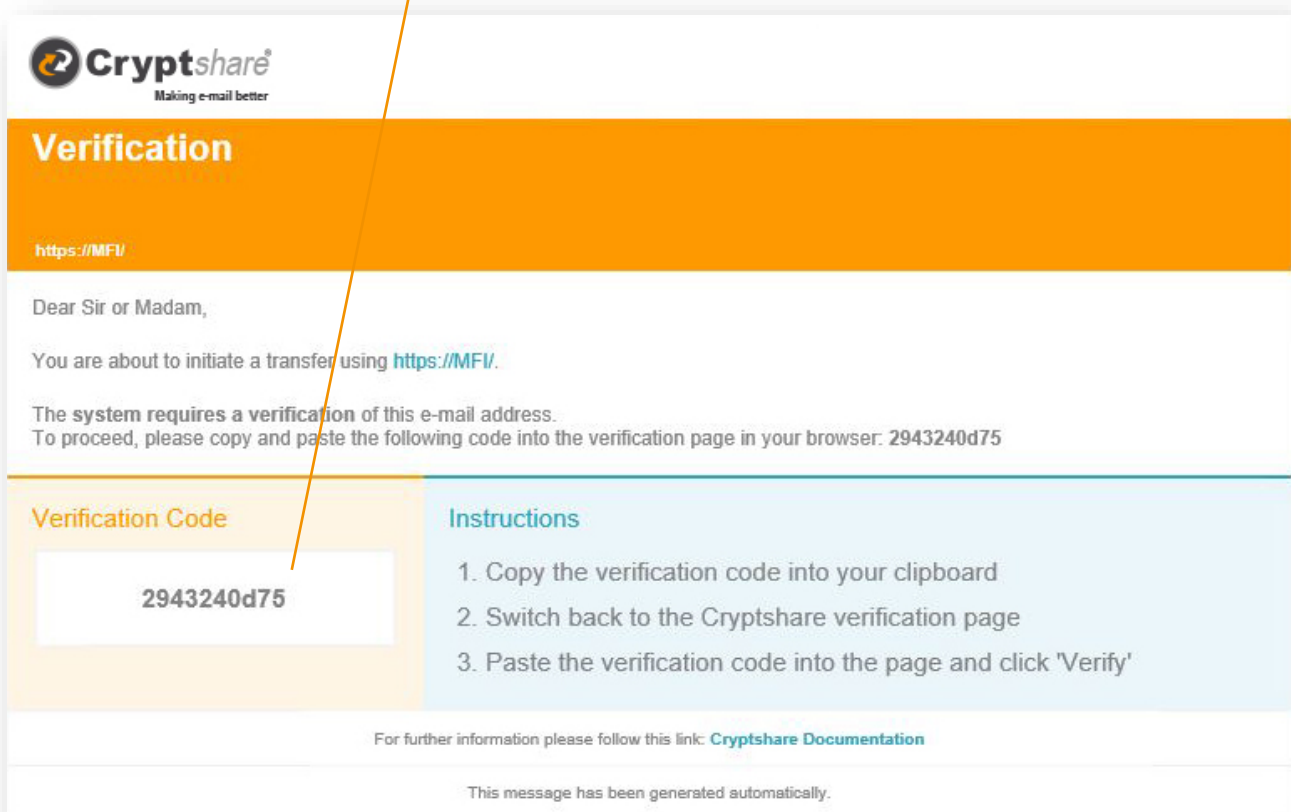Enter your contact information and click on **Next.**

Step 3
Verification Code:

When using Cryptshare for the first time, the authenticity of the e-mail address is checked for reasons of privacy. Verification is necessary after 30 days or when the e-mail address changes.

After having received the code via e-mail you need to enter it here.

Click on **Verify**.

1. Start your e-mail programme (e.g. MS Outlook)
2. Go to your inbox
3. Open the e-mail of the sender „noreply@cryptshare.com" that was sent to you automatically

4. Enter the verification code in your browser
5. Click on „Verify" (see "Step 3")

Cryptshare
Making e-mail better

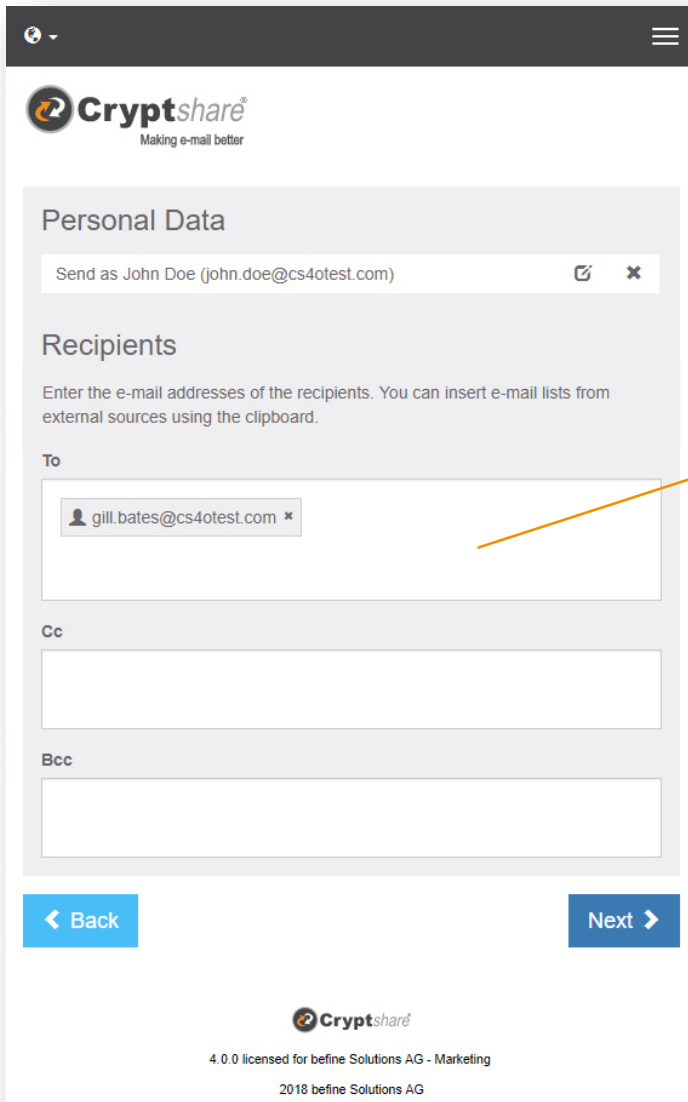## Verification

https://MFI/

Dear Sir or Madam,

You are about to initiate a transfer using https://MFI/.

The **system requires a verification** of this e-mail address.
To proceed, please copy and paste the following code into the verification page in your browser: **2943240d75**

Verification Code

2943240d75

Instructions

1. Copy the verification code into your clipboard
2. Switch back to the Cryptshare verification page
3. Paste the verification code into the page and click 'Verify'

For further information please follow this link: **Cryptshare Documentation**

This message has been generated automatically.

Step 4
E-Mail Address of the Recipient:

Enter the recipient's e-mail address here, just like when writing a normal e-mail.

Separate several recipients with a comma or a space.

Cryptshare
Making e-mail better

Add confidential message

Besides the notification to the recipients you can add an additional confidential message to this transfer. The recipients will receive this message as an additional file attached to this transfer.

Confidential Message

✉ Edit ❯

Add Files

The maximum transfer volume is 2,0 GB

⬆
Drag & Drop
Browse

General Market Development.pptx ✖
Image Video.mp4 ✖
Reviewed Numbers.xlsx ✖
Business Plan.docx ✖

❮ Back   Next ❯

Step 5
Add files

By clicking on the **Upload Button,** a Windows window opens and you may browse your pc for files and add them.

When you have added the files, click on **Next**.

Hint:

With Cryptshare you have the choice of shipping files securely and/or transferring a message encrypted. For the latter click on the symbol next to „**Add a Confidential Message"**, enter your message and click on „**Save"**.

**Step 6
Transfer Options**

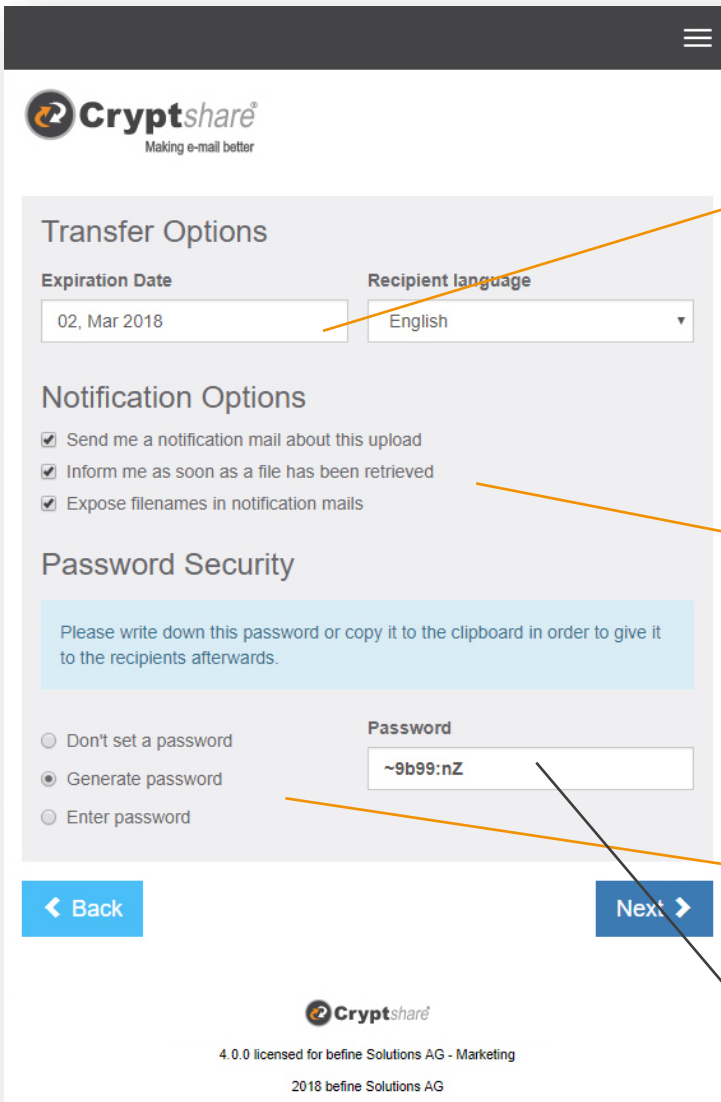Determine how long the file should be available for retrieval (max.10 days) and in which language the recipient should be notified.

You can choose if you want to be notified about the delivery and the retrieval of the transfer and you can decide, whether the name of the file should be shown in the notification e-mail to the recipient.

Finally, you can decide if you want to apply a password and if so, what kind and strength of password should be applied. *

Mark your password here. Copy it to the clip board with "STRG" + "C".

* To secure your transfer you can choose from **several password options**:

1. The option **Don't set a password** enables the sender and the recipient to exchange large files very easily without having to exchange passwords. Nevertheless, the data is transferred fully encrypted. However, the level of security is lower, since anyone gaining access to the notification e-mail, has access to the files.
2. Alternatively, you can have the system **generate** a secure **password** for you. (Write down or save this password, it will not be stored anywhere.)
3. Or **enter** a **password** of your choice.

Please note: Share your password with the recipient via telephone or SMS, otherwise they will not have access to the documents and/or message.
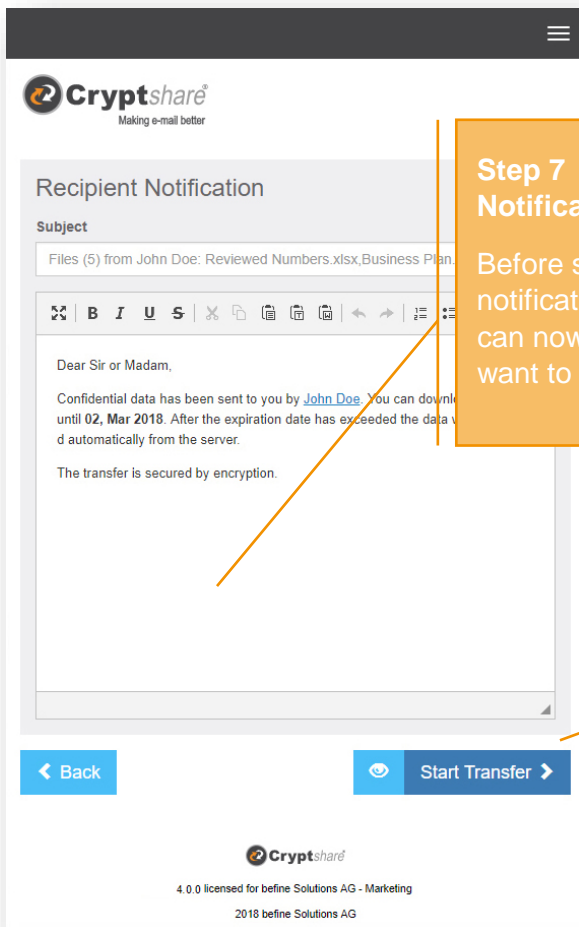
Step 7
Notification of the Recipient

Before starting the transfer, you will see the standard notification informing the recipient about your transfer. You can now alter the e-mail or the subject of your e-mail as you want to present it to the recipient.

If you do not wish to carry out any further changes, click on **Start Transfer.**
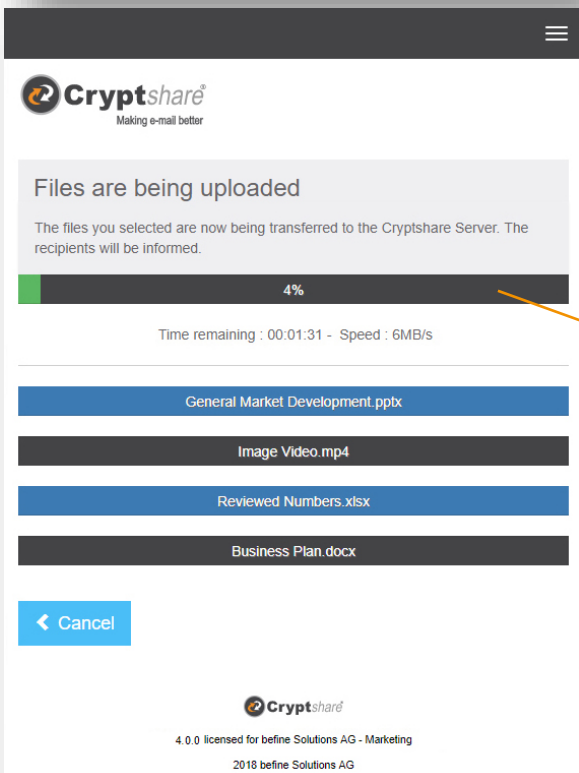
Step 8
The Transfer

After having started the transfer, your files are transmitted securely to the Cryptshare server and are stored there encrypted. The progress of the uploading process is displayed.

Summary

After all files were uploaded, you can see all details about the transfer in an overview.

This window is shown, while the transfer is still being encrypted on the Cryptshare server. When it comes to large files, this may take a while. In the meantime, no other action may be carried out in this window. But you may close it.
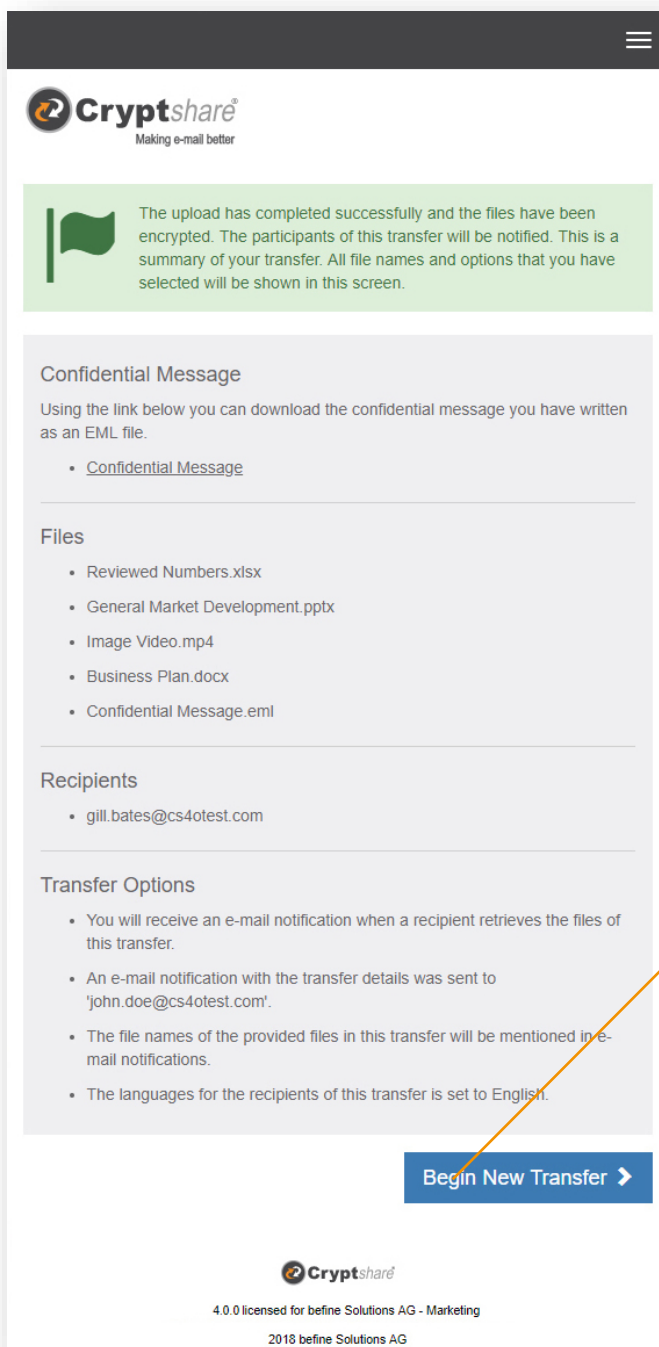
When the encryption is finished, you can start a new transfer. To do so, click on **Begin New Transfer**.

When you have finished, you can close the window.

Procedure when retrieving files

When you receive a Cryptshare transfer you are notified by e-mail. It includes details about the sender and a link to retrieve the files:
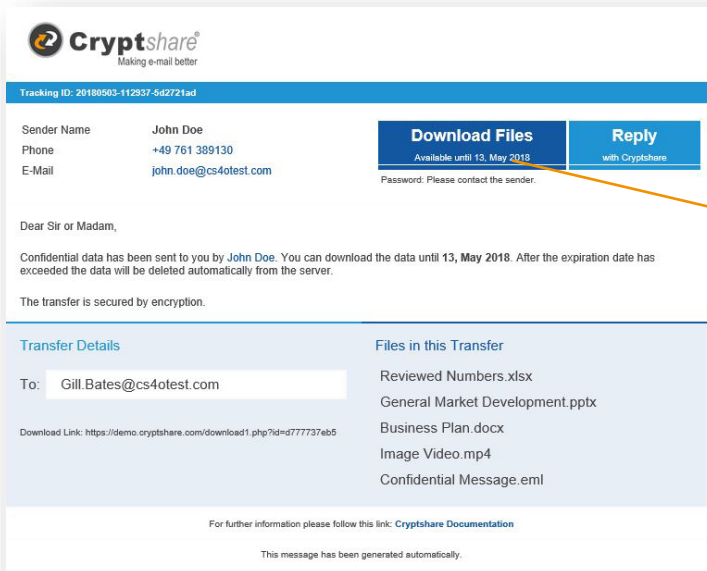
Step 1
Notification of the recipient

To retrieve the files, click on the link **Download Files** in the e-mail.

Step 2
Enter Password

A web interface occurs in which the transfer ID has been automatically filled in.

When the sender created a password, enter it here.

Click on **Next**.

When the sender did not create a password, move on to step 3.
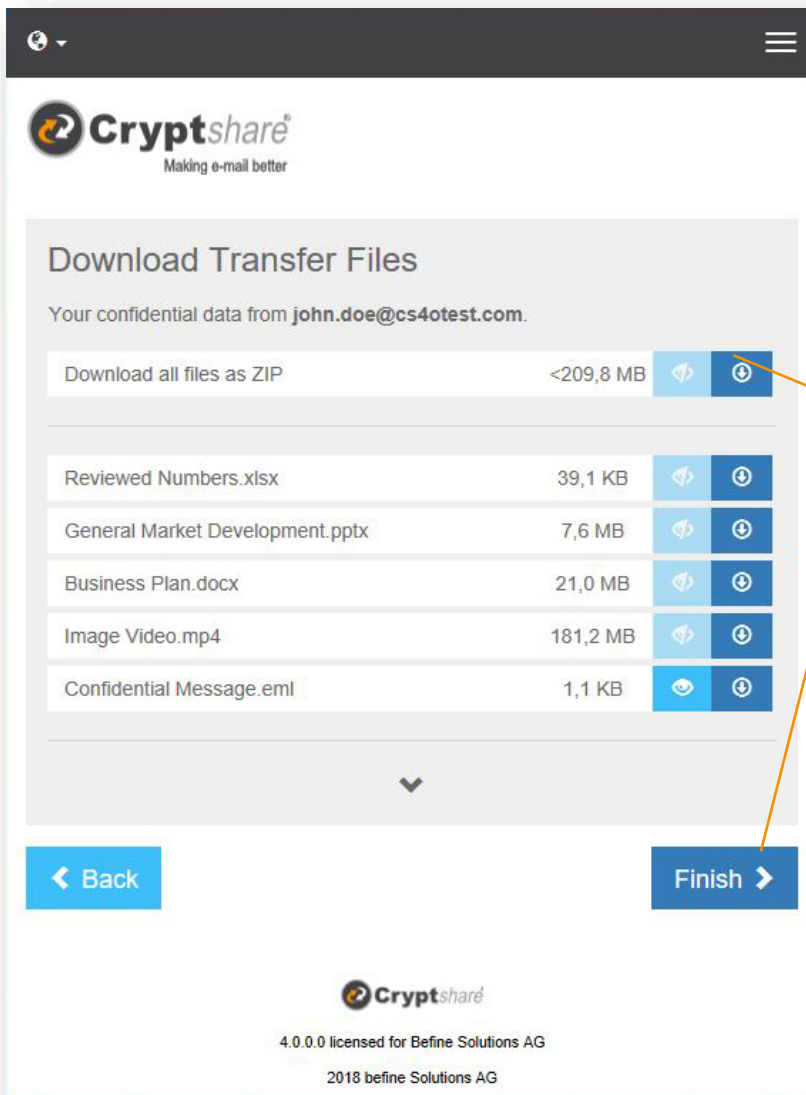
Step 3
Retrieval

With one click you can save all files as a zip archive

or open all files individually by clicking on the **name of the file**.

Depending on the security requirements of your company you can store the files directly onto your computer or open and look at Adobe Reader pdf files from the attached application, such as Microsoft Word or Excel.

When the sender has activated this option, he will be informed about the retrieval of the files automatically by e-mail.

Terms of Use for the communication via Cryptshare® – an Example:

1. Purpose of the communication via Cryptshare

For the secure electronic exchange of information with third parties, in particular with their business partners, the COMPANY uses the web application Cryptshare. The Cryptshare web application is not an e-mail programme. The application simply takes over the function of an electronic mail account. The senders provide their information on the system for retrieval. The recipients are informed by the server via e-mail about the files ready for them to retrieve.

2. Restricting the content of the communication

The communication via Cryptshare exclusively serves the purpose of exchanging confidential information. Information regarded as confidential in the sense of this regulation include information:

- that are the subject of trade secrets of the COMPANY
- that are subject to occupational and commercial secrecy of third parties
- that are personal data in the context of the General Data Protection Act considered worth protecting.

The COMPANY does not accept any legal transaction statements or contracts via Cryptshare without prior agreement.

3. Confidentiality and Data Security

To protect data from unauthorised attention and to ensure confidentiality:

► Storage of data on the Cryptshare system and the transfer of data (transfer when providing and retrieving data) is carried out encrypted.

► Access to each file put on the Cryptshare server is protected by an individual password.

The method that is used for the encryption corresponds to the recognised highest technical standards. When retrieving the files, they are not immediately erased from the Cryptshare system, but they remain there until the scheduled expiry date for further retrievals (figure 4 Arrival/Delivery of information / timely data retrieval).
As of DATE – COMPANY

The addressee / user must make sure that the delivered password is not accessible by unauthorised persons.

4. Delivery of Information and Timely Data Retrieval

Files transferred to Cryptshare are regarded as delivered to the addressee after successful retrieval (download). It is the addressee's responsibility to make sure to retrieve the files provided for him in time. The COMPANY points out that the files provided via Cryptshare can only be retrieved for 10 calendar days. The retrieval period starts once the files are available on the Cryptshare server.

5. Logging

The following operations are logged as part of the communication (data exchange):

Sender:

• Date and time when files are stored on the Cryptshare system

• E-mail address of the sender and the receiver

• The complete file name of the stored file

• The file size in megabyte

• An internally automatically assigned file identification (for authentication of files)

Receiver: (by their e-mail address)

• Date and time when files are stored on the Cryptshare system

• The complete file name of the retrieved file

• The file identification automatically assigned by the system to the file storage

This logged data is deleted at the earliest after 91 days and no later than 120 days.

6. Liability

The COMPANY assumes no liability whatsoever for disturbances or problems with the communication via Cryptshare which lie outside their area of responsibility. In addition, the liability of the COMPANY for interference / communication problems, insofar as it does not concern the violation of life, body or health, is limited to intent and gross negligence.

7. Changes concerning the communication via Cryptshare

The COMPANY is not obliged to maintain the communication capability via Cryptshare. Changes due to changes in legal, technical or other general conditions are possible at any time.

8. Customers of the COMPANY

The data transfer can be used to the same extent for the customers of the COMPANY. The customer simply goes to https://cryptshare.customer-example.com, uploads his files and enters his co-workers e-mail address.

Thanks to this added value, larger amounts of data can be sent by customers of the COMPANY in a secure way.

Keeping your e-mail private
Removing file size limits
Bringing IT compliance