POINTSHARP

20 years experience and made in Germany

Cryptshare Functions and Security

pointsharp.com

Table of contents

1. About this document

This document is intended to give an overview of how Cryptshare and its associated products work with respect to the security measures that are used. You will learn step by step how a data transfer will take place and which security measures will be used. The various possibilities (Web App, email integration, automation, etc.) of sending and receiving emails will be individually discussed in detail later in the document. For more elaborate descriptions, in particular for setting up and configuring certain security features, please refer to the Cryptshare documentation: https://wiki.cryptshare.com.

2. Sending files

2.1. Cryptshare Web App

2.1.1. Securing the connection

To send a file via the Cryptshare Web App the user first needs to open the homepage of their Cryptshare installation (e.g. https://cryptshare.yourdomain.com) in their browser.

The access to the Cryptshare Web App is protected by HTTPS/TLS, requiring a valid SSL certificate installed on the Cryptshare server. Therefore, Cryptshare appliances come with a self-generated SSL certificate, which ensures a sufficiently secure connection, however when accessing the server, the browser will issue a warning because it does not know this certificate. To avoid this, we recommend replacing the self-generated certificate with a commercial one. Detailed steps on how to do this are described in the Cryptshare documentation, which can be found here:
https://wiki.cryptshare.com/x/NYMP.

Access to the Cryptshare Web App established using an insecure HTTP connection can be automatically redirected to a secure HTTPS connection.

The key length for establishing the HTTPS connection is defined by the installed SSL certificate, so this is not a feature of Cryptshare itself. The cryptographic features of the https connection are determined by the cipher suites authorised on the server side and available on the client side. The permitted cipher suites can be configured on the server side. However, this does not take place via the administration interface of the Cryptshare server, but via a configuration file of the Jetty web server.

Cryptshare supports the latest standards in TLS, such as Perfect Forward Secrecy and HSTS (HTTP Strict Transport Security) headers.

2.1.2. Verification

When using Cryptshare for the first time, the sender of a data transfer must first verify their email address. They are asked to enter their name, phone number, and email address. A verification code is then sent to their email address and must be transferred to an input field of the Web App by copy & paste. Here, the code is bound to the browser session that the user used to enter their data, which means the code is only valid in the browser session in which it was requested. The code is no longer valid in other browsers or after closing and opening the same browser.

This procedure not only detects or avoids typing errors in the email address, but also verifies the authenticity of the email address. The typical attack scenario for the spread of spam, phishing, and malware - sending from a fake email address - is prevented by the Cryptshare verification.

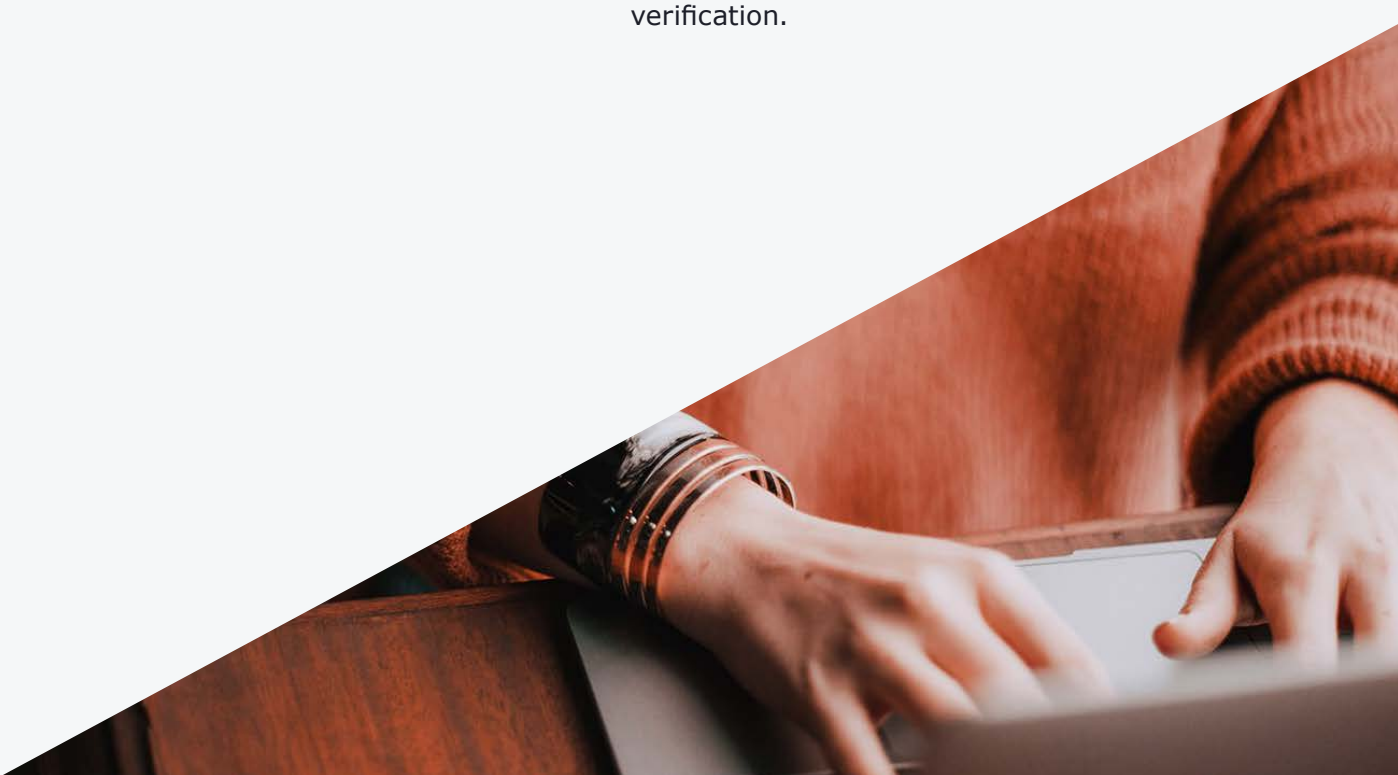
Once successfully verified, a Cryptshare cookie is stored in the user's browser. As long as this cookie is present, the email address does not have to be verified again. The lifetime of the cookie can be configured in the Cryptshare admin interface. With each use of the system, a maximum lifetime independent from use can also be set. If desired, all previously issued verifications can be invalidated at once.

The verification email is sent immediately when it is requested, but it is possible that it arrives after a delay - depending on the email infrastructure of the recipient. Due to the incurring delay, users may repeat requests occasionally, assuming to thereby speed up the process.

In general, each request for a new code invalidates all previously sent codes for the same browser session. However, there is the configuration option to define how many "old" codes the system will accept in the same browser session so that even if the user has requested several codes, the first code will still be accepted. At the end of the browser session, all of the requested codes become invalid.

Please note: The verification mechanism only allows the authenticity of the email address to be checked. The information regarding name and phone number cannot be verified this way.

Please note: A successful verification does not grant permission to use the system. Even if a sender successfully verifies their email address, it may be possible that the intended transfer is not permitted due to the policy, for example because sending to the desired recipient is not permitted. Only email addresses which are completely excluded from any use of the system due to the policy are automatically rejected during verification.



2.1.3. Password security

A one-time password must be set for every transfer, from which a key to the encrypted and stored files is generated (see chapter 2.1.5 – "Encrypting the file(s)"). The administrator can turn on or off qualitative criteria that passwords must meet. These are:

- Passwords must contain numbers
- Passwords must contain standard letters
- Passwords must contain special characters
- Passwords must contain uppercase and lowercase letters
- Ordinary words are not allowed as a password
- Repeating or successive characters are not allowed
- Minimum password length
- Maximum password length

These criteria can be applied in any combination. In addition, the administrator can specify which options are available to senders for assigning passwords:

2.1.3.1 Not setting a password

When this option is used, no password is assigned by the user, but the system automatically generates one and uses it for encryption. The generated password is sent to the recipient in plain text by email as part of the download link. The recipient simply needs to click on the link to get access to the file because the transfer ID and password will be automatically transmitted to the Cryptshare server. This option has the advantage that it is very easy for sender and recipient to handle, and data is still encrypted in transit. However, the level of security is lower than when using the other password options. The encryption of the file residing on the server is just as strong as it is when using the other password options, and all defence mechanisms against attacks remain the same. Since the password is sent via email, however, there is the risk that the email is spied on, compromised and that an unauthorised person uses the acquired data to access the file.

2.1.3.2. Generating a password

When using this option, a password is automatically generated by the system that meets the quality criteria set by the administrator. The password is displayed to the sender on the screen and can be copied to the clipboard. However, it is not automatically transmitted to the recipient or stored by the system. Sender and recipient need to share the password in a separate way (e.g. by phone or face to face).

2.1.3.3. Choosing your own password

When using this option, the sender assigns a password of their own choice. The password must meet the quality criteria set by the administrator. To make it easier for the user to do so, the requirements are shown with symbols below the password entry field. The symbols of requirements that have already been fulfilled are hidden immediately so that the user can always see which elements they still need to add to the password. In addition, a password repetition is required to avoid typing errors. As a graphic element, there is also a bar indicating the quality of the password. The indicated quality of the password is independent from the administrator's password requirements.

Please note: At no point are passwords stored by the system in plain text. In order to be able to check the accuracy of a password entered by the recipient, the result of a derivation that is based on a combination of the given password and a certain random component is created and stored using a suitable hash function.

As a result, passwords cannot be restored or reconstructed. They cannot be viewed, reset, or changed. Passwords must be exchanged between sender and recipient in a separate way and they are known only to them. If a password is forgotten or lost, the file cannot be decrypted and is automatically deleted after the retention period has expired. In this case, the file transfer needs to be performed again. In case a sender transfers a message to the wrong recipient, the recipient will not be able to open it because they have no knowledge of the password.

2.1.4. Upload and virus scanning of files

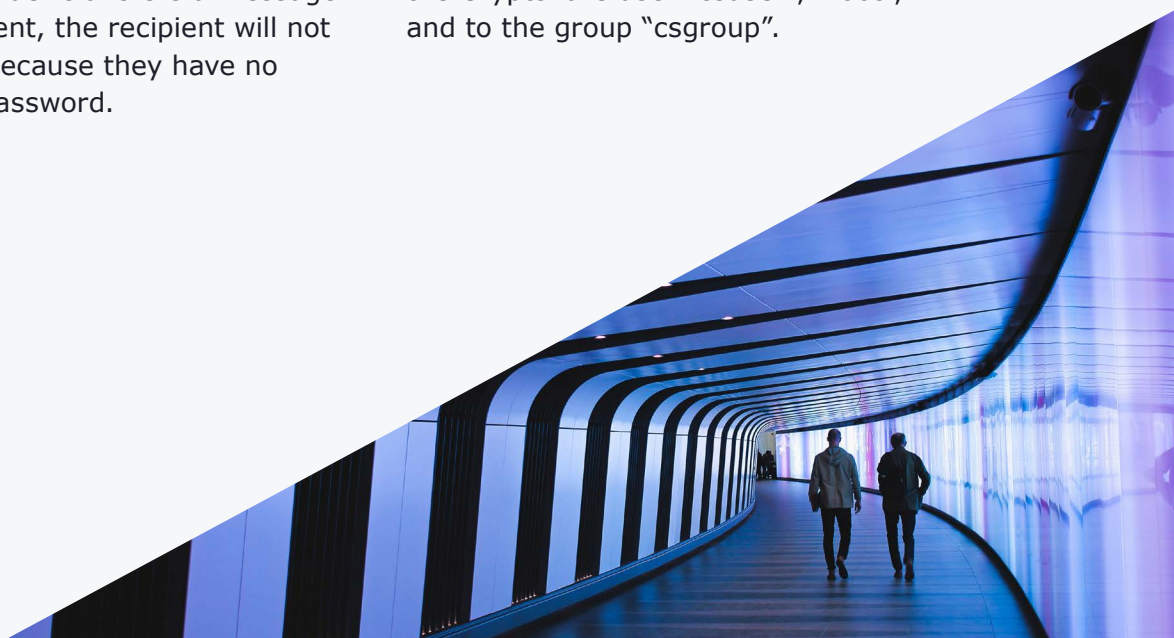
After a password has been assigned and the transfer options have been specified, the file is uploaded to the Cryptshare server. The file is still unencrypted, but it is transferred to the server via an HTTPS/TLS - secured connection.

Once the file has arrived in full on the server, it is checked during pre-processing by the tethered virus scanner. On Cryptshare appliances, a ClamAV virus scanner is preinstalled and integrated by default. On Cryptshare systems which are set up manually, the virus scanner configuration must be entered manually in the "pre-processing" section of the administration interface. You may also use a virus scanner of your own choice, provided that you can start it in the command line and that it delivers a return code.

Depending on the return code of the virus scanner, Cryptshare reacts either by continuing to process the file or by deleting the file and displaying an error notification in the user interface. All unsuspicious files are then transferred to the recipient.

During the upload and virus scan the file remains unencrypted on the system. In Linux-based systems, however, it is protected from unauthorised access by protective measures that are specific to the operating system.

When installed and configured properly, the appropriate directory is only accessible to the Cryptshare user "csuser", "root", and to the group "csgroup".



2.1.5. Encrypting the file(s)

After the virus scan has been performed with negative results (meaning that no virus was found), the files are stored encrypted using AES-256, the AES algorithm with a key length of 256 bits, in Cipher Block Chaining (CBC) mode.

In order to achieve the key length and key quality demanded by AES-256, an artificial key is derived from the password set by the user or the system that is unique for every file. The derivation process additionally includes a randomly generated value, the so-called salt, thereby ensuring that identical passwords do not result in the same key. The salt has a length of 16 bytes. As its key derivation function, Cryptshare uses the PBKDF2 algorithm with HMAC SHA-256 and 64,000 iterations.

Furthermore, to prevent identical encryption results in the (unlikely) case of identical keys and the same plain texts, the AES-256 algorithm takes another individual input value for each file, the IV (initialization vector). It consists of 16 randomly generated bytes.

For all random values that are relevant for security, a cryptographically strong random generator with non-deterministic output is used. The random generator receives the seed material from an entropy source the underlying operating system provides (e.g. /dev/random or /dev/urandom with Linux).

These laid out measures provide a very high level of security. With many systems, all data in storage is merely encrypted with the same AES key. With Cryptshare, every file has a unique key.

2.2. Cryptshare for Outlook

2.2.1. Securing the connection

The communication between the Outlook client and the Cryptshare server takes place via https. On request, unsecured HTTP communication can be used; for example, if the Cryptshare server and the Outlook client are located within the same protected network so communication is not taking place over the internet. This offers the advantage of checking the data stream for undesired content with suitable filtering systems more easily.

2.2.2. Verification

The sender needs to verify in Cryptshare for Outlook. However, verification takes place automatically. It works as follows: Outlook prompts an email containing the verification code from the Cryptshare server, reads the email from the inbox and processes the code automatically. As with the Cryptshare Web App, the user needs to provide their name and phone number which, however, cannot be checked for accuracy by the verification. Once the code has been successfully processed, a verification token is stored in the Windows user profile of the sender.

2.2.3. Password security

Regarding password security, the same mechanisms apply as when using the Web App (see chapter ‘Password security’). In contrast to the Web App, password requirements are also represented by symbols; these are not hidden but displayed in green when fulfilled.

In addition, Cryptshare for Outlook provides the ability to store senders’ passwords encrypted in the user’s local user profile. The user then has the option to click on the element in the “Upload Manager” which represents a specific upload. There, they can display the password they have assigned again at a later time. To do so, however, they first have to unlock the memory for their Cryptshare passwords with their MS Windows password. The assigned passwords of the transfers which are no longer displayed in the Upload Manager are deleted from the password memory.

2.2.4. Upload and virus scanning

Regarding upload and virus scanning, the same mechanisms apply as when using the Web App (see chapter ‘Upload and virus scanning of files’).

In contrast to the Web App, with Cryptshare for Outlook in the event of a virus detection the user may choose if the whole transfer shall be stopped entirely or if only the non-infected files shall be transferred.

The remaining upload procedure as well as the download work identically as described in chapter ‘Cryptshare Web App’.

2.2.5. Encrypting the file(s)

Regarding the encryption of the files, the same mechanisms apply as when using the Web App (see chapter ‘Encrypting the file(s)’).

2.2.6. Protective email classification

In addition to the option of giving the user the choice of using Cryptshare and the Cryptshare options, you can activate the feature of the Cryptshare email classification.

Depending on its configuration, the email classification may ask or demand the user to classify their message. The administrator can create levels of protection (e.g. public, internal use, confidential, strictly confidential) and apply certain names, colours, transfer options and configurations to them.

For example, if the sender classifies an email as strictly confidential, Cryptshare then handles all configurations according to an email with strictly confidential content in accordance with the corporate standards. The email is also marked technically and optically according to its classification and, when required, equipped with a short text that informs the recipient how to handle this piece of information correctly.

In addition to the purely technical aspect of this function, there is also a training effect for the employees: The email classification sensitises staff to handling confidential information correctly.

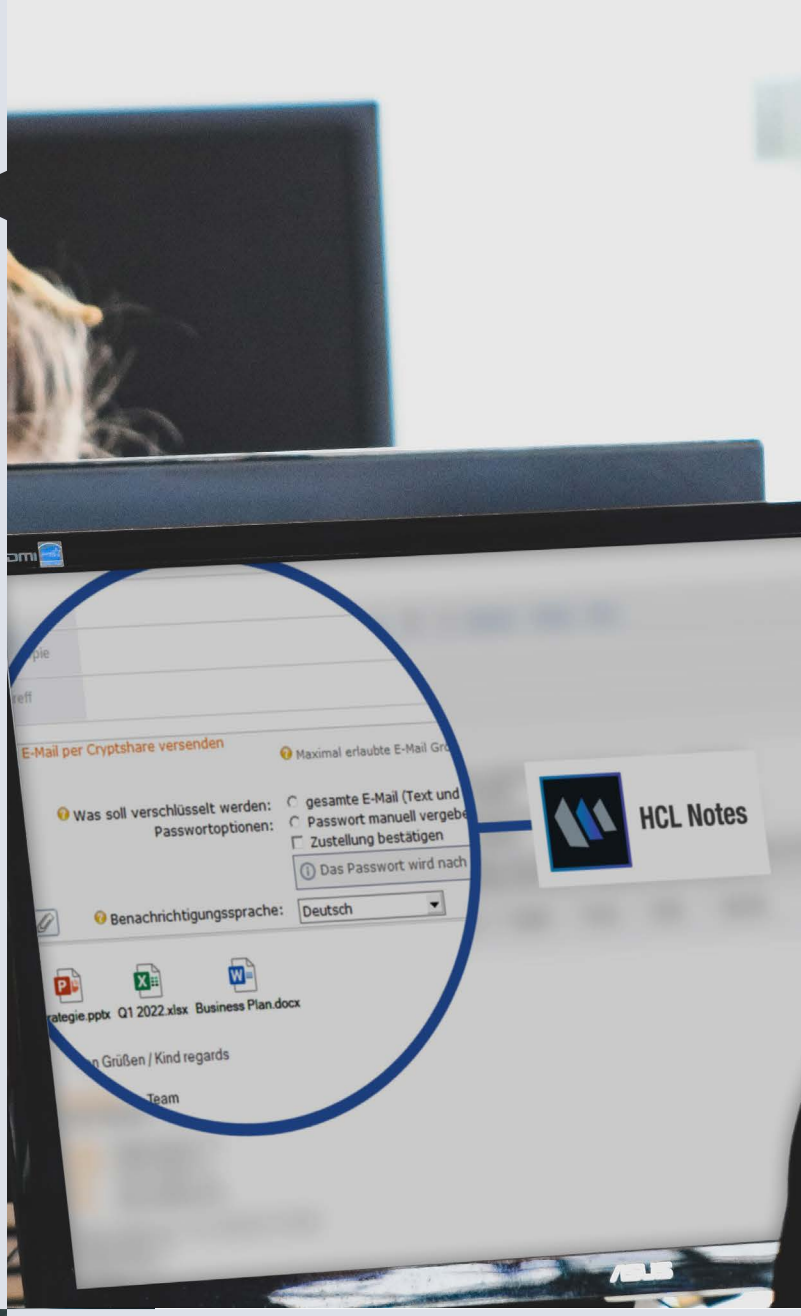
2.3. Cryptshare for Notes

2.3.1. Securing the connection

Cryptshare for Notes is installed on the Domino server. A local installation in the Notes client is not required. When using Cryptshare for Notes, the sensitive content is first transferred from the Notes client to the Cryptshare application (Cryptshare.nsf) on the Domino server.

Here, the same measures are used to secure the communication that have been defined for Notes client and Domino server for the entire Notes communication.

The confidential content is then transferred from Cryptshare.nsf to the Cryptshare server.



Communication between the Cryptshare application on the Domino server and the Cryptshare server usually takes place via https. You can also use insecure http communication, for example if the Cryptshare server and the Domino server are within the same protected network, so the communication therefore does not take place via the internet. This offers the advantage that the data stream is checked for contents by suitable filtering systems.

2.3.2. Verification

When using Cryptshare for Notes, no explicit verification of the sender is required because the security mechanisms of IBM Notes verify the authenticity of the sender. Only the Cryptshare for Notes application itself needs to be registered once on the Cryptshare server.

By using hardware properties, a code is generated on the Domino server that identifies the machine on which Cryptshare for Notes is installed. This code has to be registered on the Cryptshare server.

2.3.3. Password security

Cryptshare for Notes offers two possibilities of sending files and messages: manually or automated.

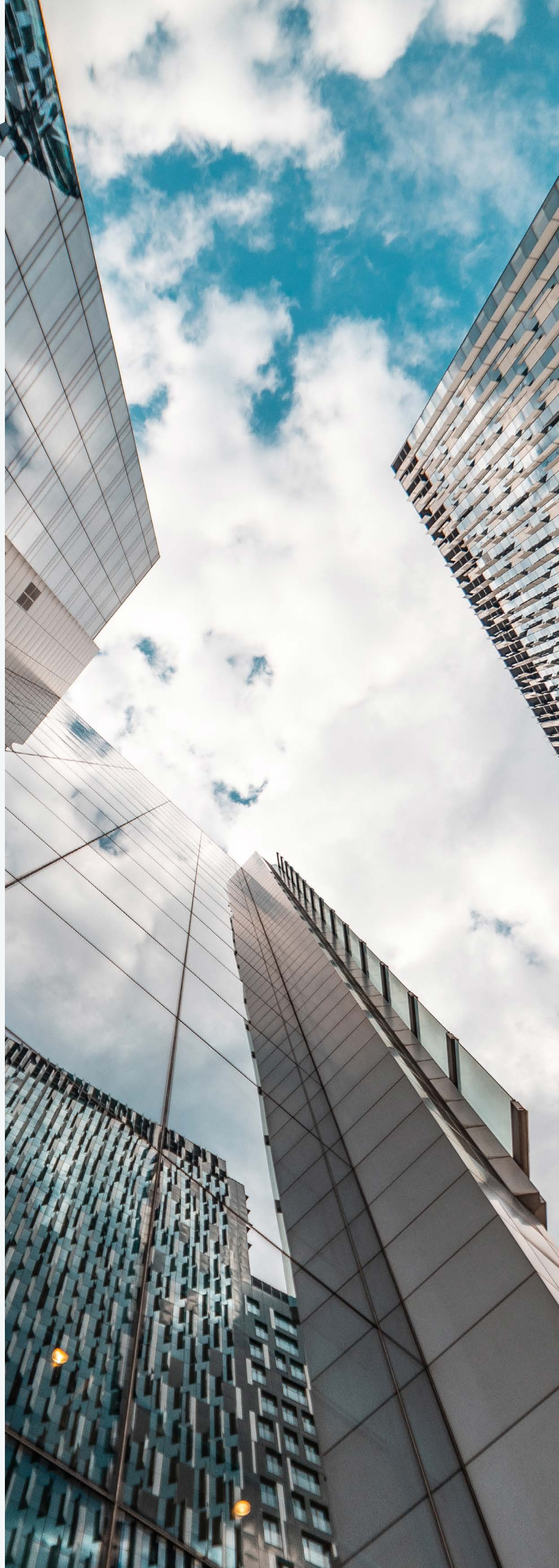
2.3.3.1. Sending manually

When choosing to send manually, the sender actively decides that the message or file is sent with Cryptshare.

They click either on the toolbar icon and a Cryptshare form opens, or they activate the Cryptshare function in the form for a new email and a subform unfolds.

In both cases, the user can make use of the same password options as described in chapter ‘Password security’. However, the defined qualitative requirements for passwords from the server side are not taken into account in Cryptshare for Notes.

Instead, only a minimum length for passwords can be set in Cryptshare for Notes. Furthermore, all special characters permissible for the generation of passwords can be defined and thus undesirable special characters can be excluded.



Please note: Because the password verification mechanisms on the server side do not match those in Cryptshare for Notes, Cryptshare for Notes – depending on your preferences – may create passwords that are not consistent with the server's preferences, so the server would refuse the transfer. In this case, the password check on the server side can be disabled for transfers initiated via Cryptshare for Notes.

This behaviour will be consistent in future versions of Cryptshare for Notes.

2.3.3.2. Sending automatically

In addition to manually creating messages with Cryptshare that function in a similar way to the Web App, Cryptshare for Notes allows email messages to be passed automatically and rule-based from Domino to Cryptshare for Notes. For example, emails which fulfil certain criteria (e.g. emails with file attachments larger than 10 MB) may by policy be automatically delivered via Cryptshare, relieving the email system.

In this scenario the sender does not yet know that their message will be processed by Cryptshare; therefore, the sender cannot assign a password.

In such cases Cryptshare automatically creates a password. It is possible to configure the system so that the password is sent to the recipient by email as part of the download link.

This option has the advantage of being very convenient for sender and recipient. However, the level of security is lower than it is when using the other password options. The encryption of the file residing on the server is just as strong as when using the other password options, and all the defence mechanisms against any attack remain. Since the password is sent via email, however, there is a risk here that the email is spied on, compromised and that an unauthorised person uses the acquired data to access the file. Alternatively, the automatically generated password is delivered to the sender with Notes email, so this password can be exchanged with the recipient in a separate way, e.g. by phone.

To ensure the security of the password, the email may be sent via the Cryptshare for Notes application using Notes' own public/private key infrastructure for encryption. Furthermore, Notes' own option that will prevent the email from being forwarded can be activated so that the password is not at risk of being forwarded, for example to a sender's replacement due to a mail rule.

2.3.4. Upload and virus scanning

The same mechanisms apply to upload and virus checking as when using the Web App (see chapter 'Upload and virus scanning of files'). If a file is infected by a virus, Cryptshare for Notes can be used to define who should be informed about the incident and how this information should look.

2.3.5. Encrypting the file(s)

Regarding the encryption of the files the same mechanisms apply as when using the Web App (see chapter 2.1.5).

2.4. Cryptshare Robot

2.4.1. Securing the connection

Cryptshare Robot communicates with the Cryptshare server via https. Generally, the same mechanisms apply as described in chapter ‘Securing the connection’.

On request, an insecure HTTP communication can be used, for example when the Cryptshare server and the machine on which Cryptshare Robot is executed are located within the same protected network and where communication is thus not taking place over the internet.

This offers the advantage that the contents of the data stream can be checked by suitable filtering systems.

Please note that Cryptshare Robot is a Java programme. The root certificate of the SSL certificate that you are using on the Cryptshare server should therefore be listed as a trustworthy certificate in the Java keystore.

2.4.2. Verification

Cryptshare Robot has two different verification methods. For both methods, a verification code must be generated by the Robot via a command line. The code then has to be deposited on the Cryptshare administration interface.

2.4.2.1. Client Verification

When using the client verification mode, the Robot installation is verified on the Cryptshare server. In this case, characteristics of the hardware are used to identify the client and to prevent the verification being used on another machine. In the case of a client verification, the verified robot installation can send transfers with any email address, provided that the license or policy permits this.

2.4.2.2. Sender verification

When using the sender-verification mode, each sender’s email address that Cryptshare Robot is supposed to be able to perform a transfer with has to be verified individually.

2.4.3. Password options

Generally, the same mechanisms apply as described in chapter ‘Password security’.

The password can be transmitted as a command line parameter. Alternatively, a password can be created by Cryptshare Robot, which is then released at the command line.

As a third option, Cryptshare Robot can generate a password which is sent to the recipient as part of the download link in plain text via email.

See also chapter ‘Not setting a password’.

2.4.4. Upload and virus scanning

The communication between Robot and the Cryptshare server is usually done via https.

On request, an insecure http communication can be used, for example if the Cryptshare server and the machine that is running Robot are located within the same protected network and the communication thus does not take place over the internet. This offers the advantage that the contents of the data stream can be checked by suitable filtering systems.

If a virus is found, a message is sent via the console, informing that a file or all files were removed from the transfer during pre-processing.

2.4.5. Encrypting the file(s)

Regarding the encryption of the files, the same mechanisms apply as when using the Web App (see chapter 'Encrypting the file(s)').

3. Retrieving files

Regardless of how a file has been provided, the download can take place via the Cryptshare Web App or via Cryptshare for Outlook.

3.1. General security functions

The following security functions apply regardless of how a file may be retrieved.

3.1.1. Protection against brute force attacks

To retrieve a file, one must enter the correct transfer ID and the correct corresponding password.

If the transfer has been sent without an assigned password (see chapter 'Not setting a password'), the password is part of the download link and is applied automatically so that the user does not need to enter anything.

If a password is repeatedly entered incorrectly when trying to retrieve a file, the system can respond by blocking or deleting the transfer, depending on the setting. The desired behaviour can be configured via the policies and thus depends on the sender-recipient combination of the transfer.

3.1.1.1. Transfer blocking

Upon revoking access to a transfer, access to the files for a specific recipient will be revoked for a configurable period of time. During the lockout period, this recipient cannot retrieve the transfer, even with the correct password. This effectively prevents automated brute force attacks to guess the correct password. The sender is notified of the revocation by email.

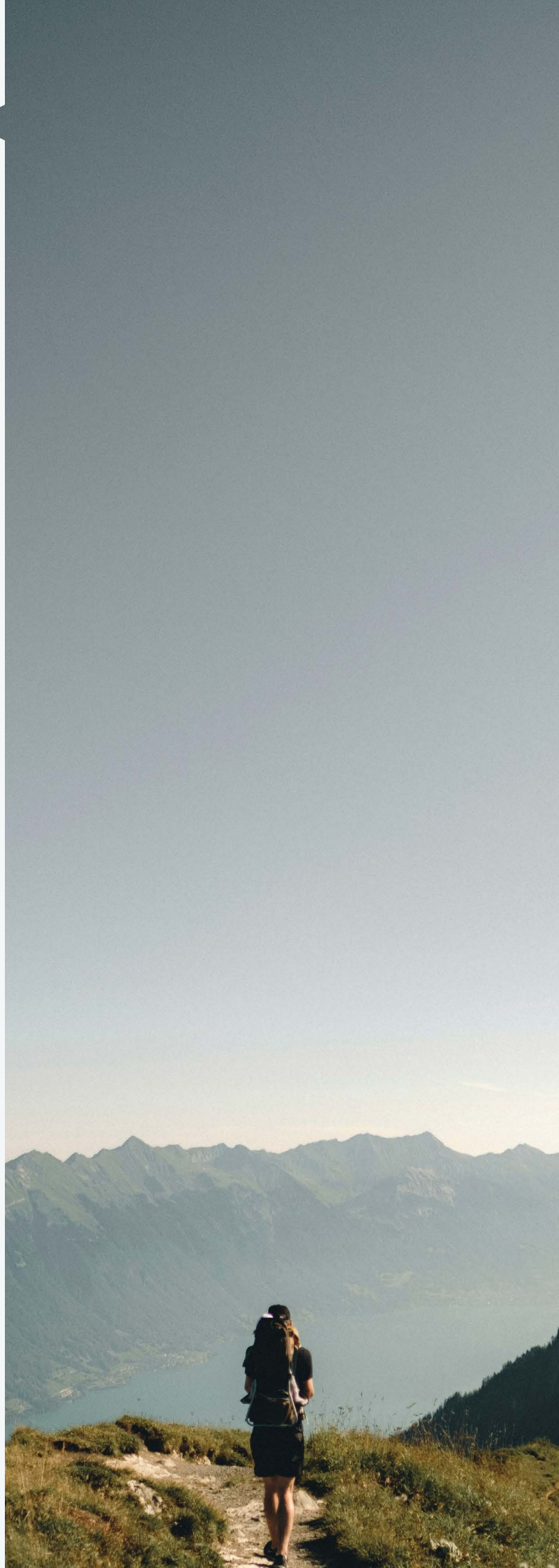
Furthermore, an entry in the log takes place. The administrator can easily unlock the revocation via the log view of the Cryptshare administration interface, if required.

Please note: For transfers that are sent to multiple recipients, a lockout only applies to one specific recipient who is blocked for a defined period of time. All other recipients can retrieve the files with the correct transfer ID and the correct password.

3.1.1.2. Deleting transfers

When the configured number of allowed failed attempts is exceeded, the entire transfer package is removed from the server. The sender and the administrator are informed about this fact and an entry is made in the log.

Please note: The deletion of the transfer cannot be undone. When a transfer with multiple recipients is made, none of the recipients will be able to receive the files any more.



3.1.2. Decrypting the file(s)

Thanks to the transfer ID in the download link, the system can find the files and the corresponding encryption parameters (salt, initialization vector). After entering the correct password, the same process is used to generate the key required for decryption, as described in chapter ‘Encrypting the file(s)’.

When the file is downloaded it is decrypted within the download stream. While this is in progress, no temporary files are created on the server. When the download is complete, an unencrypted file is available for the recipient for further processing.

Alternatively, the file can be opened in the browser for viewing. This function is restricted to certain types of files which can be displayed in the browser. In addition, the size of the files that can be displayed is limited because, for security reasons, the files are not stored unencrypted in the file system of the server but are kept in the RAM of the server only for the duration of the display.

4. Electronic Identity (eID)

The Electronic Identity feature allows organisations to demand users prove their identity digitally. By using an eID issued by a trustworthy provider, a user can identify himself to any system supporting this identification method.

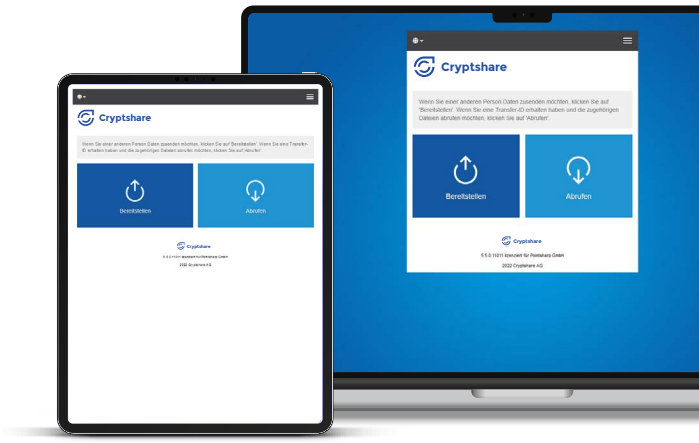
Cryptshare can use this technology both on the sender and recipient side. It can demand the sender to prove their identity to recipients and demands recipients to authenticate themselves for the retrieval of transfers provided with the security mode ‘Electronic Identity’.

In this mode, Cryptshare secures the transfer the same way it is done for the ‘No password’ mode, i.e. no password has to be exchanged between sender and recipient. Since there is the need to identify prior to being able to access the files, security for the transfer is provided.

3.2. Web App

3.2.1. Securing the connection

Regarding the measures to protect the web connection, the same mechanisms apply as described in chapter 2.1.1 – ’ Securing the connection ’.



4.1. Signicat Digital Identity Platform

Cryptshare uses the Signicat Digital Identity Platform as the basis for eID communication. Signicat is a company founded in Norway in 2006 and offers electronic signing and secure authentication solutions. Signicat has received several prestigious awards for its ground-breaking technology. By integrating Signicat's Digital Identity Platform, Cryptshare enables the integration of a multitude of different ID Providers. Regardless of which provider is preferred, communication is routed through the service interfaces provided by Signicat.

4.2. Identification Process

Cryptshare uses OpenID Connect (OIDC) for the authentication process as described in the Signicat Documentation for OIDC. All communication between the Cryptshare Server and Signicat services is done with a secure HTTPS channel.

4.2.1. Detailed authentication steps

The following steps describe the identification process as it is used in Cryptshare:

1. Cryptshare recognises the need for identification/authentication.

2. An intermediate screen is shown informing the user about the fact that the identification process will be initiated.

3. The user is redirected to the Signicat authorisation interface handing
   over the following processing information:

   - Redirect URL pointing to the next step (after the identification)
     in the Cryptshare Web App.

   - Additional unique personal information of the user for validation purposes on the Signicat interface.

4. The user performs the identification process himself. The procedure may differ depending on the ID Provider, but most common is:

   - Using a mobile device: A QR Code is displayed to be scanned with a mobile device. Scanning triggers the corresponding ID Provider app where the user authenticates himself (i.e. by entering the correct password).

   - Using a Desktop PC: An application is started where the user authenticates himself.

5. The user is redirected to Cryptshare using the Redirect URL from step 3. The following additional information is handed over to Cryptshare for further processing:

   - Authorisation code giving Cryptshare permission to request an access token. This access token allows requests for additional information about the users from their eID profile.

   - In case the identification process fails: Error codes and descriptions for displaying an appropriate feedback message for the user.

6. If the sender chooses to use eID authentication for himself, Cryptshare requests additional user information using the access token obtained in step 5.

7. The process is complete. If the sender uses eID authentication for himself, gathered personal information from the eID profile is used for further processing in Cryptshare, i.e. the name of the user or personal identity codes. For recipient authentication, Cryptshare grants access to the files in the transfer if the recipient has been authenticated successfully without obtaining further personal information from the eID profile.

5. QUICK Technology

Cryptshare QUICK Technology is an additional security feature which automates the management of one-time passwords for users. It does not change the way how files are encrypted and decrypted, nor does it affect other security aspects of the application.

If a sender has activated QUICK, he will not need to define a transfer password by himself, instead the QUICK technology generates a password in the background which the receiving device will be able to determine and apply using the recipient‘s QUICK credentials. The password is secured by a key chain only the participants of the transfer have access to.

For a detailed description how the Cryptshare QUICK Technology is integrated into the pro-visioning and retrieval process of Cryptshare, please refer to https://wiki.cryptshare.com/quick.

5.1. QUICK Key Chain

The QUICK key chain is built up as described below. Please refer to ‘Key Building Parameters’ and ‘Encryption Algorithms & Storage Details’ for details about the encryption specifics:

Each user is given a secure verification token consisting of 64 base64 encoded random bytes. This identification sequence is stored only on the client of the user. The verification token allows access to the personal key of the user. The encrypted personal key is stored on the Cryptshare Server. Per sender-recipient combination shared keys are created. The shared key is encrypted using the personal key of each user. The transfer password is encrypted using the shared key of each recipient and is part of each Cryptshare Transfer.

5.2. Key Building Parameters

The following table lists keys used for the Cryptshare QUICK Technology and how they are encrypted.

Key	Elements	Encryption Method
Transfer Password	64 alphanumeric random bytes	symmetric
Personal Key	64 Bytes (0-255)	symmetric/asymmetric
Shared Key	64 Bytes (0-255)	symmetric

5.3. Key Building Parameters

The following table lists details about the encryption algorithms used for QUICK and the details about the encryption parameters used for storing keys on the Cryptshare Server.

Details	
Asymmetric Encryption	• RSA with a 4096 bit key length • Padding: OAEP with SHA-256 and MGF1
Symmetric Encryption	• AES with a 256 bit key length • CBC mode • PKCS5 Padding
Key Derivation for Storage	• PBKDF2 with HMAC SHA-256 • Salt with 16 bytes • 64000 Iterations

6. Administrative security features

6.1. Access to the administration interface

The Cryptshare system can be configured and managed via the administration interface.

A separate, configurable port can be assigned to this administration interface. This gives you the possibility to tightly control access to the administration interface, for example with your firewall, so that it cannot be accessed from the outside, in this example.

In addition, users can be created with their own passwords and with different user rights. User rights control which elements of the administration interface can be viewed or operated by the user.

6.2. Logging

All transfers that take place via the Cryptshare server are logged in detail by the system.

Some details are always logged, while other details may be enabled or disabled depending on your policy settings (see chapter ‘Access management via Cryptshare policy’):

- tracking ID (clearly identifies the transfer process)
- transfer ID (clearly identifies each recipient of a transfer)
- time and date of upload
- IP address of the machine that carried out the upload
- verified email address of the sender
- name of the file (optional)
- file size
- file ID (the file name of the encrypted file on the disk of the Cryptshare server)
- subject and notification text (optional)
- selected transfer options for this transfer
- time and date of download or opening (for display to the recipient)
- IP address of the machine that has performed the download
- email address of recipient
- selected email classification of the message

6.3. Access management via Cryptshare policy

Cryptshare does not require traditional user account management, but on request there is the option to manage the use of Cryptshare. Managing Cryptshare offers even more options than there would be with merely managing via user accounts.

With the Cryptshare policy you can define if certain sender-recipient combinations are allowed by the system or not. If they are allowed, you can define further parameters that apply to transfers of exactly that same sender-recipient combination. The definition of the sender and recipient side may be carried out according to the following criteria:

- one or more email address(es)
- one or more email domain(s)
- LDAP user
- LDAP user group
- IP address area (only sender)
- regular expression, which is compared to the email address that is entered

This way, very fine-grained rights to access can be given, and the functionality and the level of security of the system can be adjusted to very particular use cases.

For instance, it would be possible to define the following requirements:

- As a general principle, all employees are allowed to send files up to 100 MB to any recipient. All details of the transfers are stored in the log.
- Employee John Doe is allowed to send files as big as 5 GB to any recipient of the marketing department.
- Employee John Doe is allowed to send files up to 100 MB to members of the HR department, but in this case not all details of the transfer are stored in the log. The names of the files and the notification texts are excluded from being stored in the log so that they cannot be read by the administrators.
- Employee John Doe is explicitly not allowed to send files to the email domain @competitior.com. But members of the domain @competitior.com are allowed to transfer files to him.

7. Quality assurance and general safety measures

7.1. Exclusion of attack scenarios

In order to ensure the highest possible level of security, all appropriate measures to eliminate known attack scenarios against web applications are taken. These include, for example, suitable validations of all fields; measures against cross-site scripting; preventing the display of status or error messages on the Cryptshare Web App that could provide an attacker with valuable information; using methods for intrusion detection, such as brute-force attacks, mail flooding; etc.

To ensure that our actions are effective and comprehensive, we additionally subject the software to automated security audits using established tools that are available for this purpose.

Many of our clients include their Cryptshare systems in their regular manual or automated security checks and penetration testing. We ask them to share their results with us so we can take the gained knowledge and improve our software solution Cryptshare continuously to the benefit of all Cryptshare customers. To achieve a very high level of quality, we apply the principles of "test-driven development".
That means that for each function module of the solution an automated test is developed first, and only then can the actual function module against this test be developed. This way, a high level of quality can be achieved and a large proportion of the application – in addition to manual testing – can be tested automatically.

7.2. Update procedures and response to security breaches

As part of software maintenance, we publish regular updates for Cryptshare:

- when a security risk in Cryptshare occurred for which there is a solution
- when functions can be improved that are relevant for security
- when an update becomes necessary due to compatibility with other components that are required for using the system (e.g. new browser versions)
- when new functions are available

If a security risk in Cryptshare becomes known, or a threat to a component is found as part of our security checks and risk scenarios during quality assurance or customer testing, or a known or possible security risk is detected in a technology that is used by Cryptshare (e.g. browser, Java, web server), we will respond as soon as possible to eliminate the risk for our customers. As part of this approach, after an analysis of the problem our customers receive:

- a statement about the impact of the known security vulnerability specifically with regard to Cryptshare
- a statement about the approach (e.g. the release of an update) and the expected time frame for the provision of the solution
- if possible, recommendations for temporary emergency measures to reduce or eliminate the risk (e.g. temporary change of configuration settings, deactivating Java, etc.)

7.2.1. Cryptshare Server

As soon as a solution becomes available as an update, it is provided by a central update server. The Cryptshare Server checks the availability of new updates every 24 hours. The connection between the Cryptshare Server and the update server is secured via TLS/HTTPS, and HTTP connections are automatically redirected to HTTPS.

To ensure the integrity of the provided update packages, a SHA-256 hash value is generated for each file (including metadata). The list of files with their hash values is signed cryptographically (RSA encryption algorithm using SHA-256). This ensures that packets cannot be exchanged or modified without being noticed. The Cryptshare Server verifies the identity of the update server against the SSL certificate, and the information provided by the update server using the signature and hash values of the files. When an update is available, the administrators configured on the Cryptshare Server are notified. These administrators can perform the update immediately or automatically at a scheduled time.

7.2.2. Appliances

For our appliances, we additionally provide updates and patches for the operating system from a central repository. Updates and patches that do not require a reboot of the system can be applied automatically. If a restart is required, the administrator of the system is informed of the provided update and can start it manually or set a date and time for the automatic update.

Please find the latest and more detailed information on the Cryptshare Web App, Cryptshare for Outlook, and Cryptshare for Notes as well as on the administration interface and on release notes in our wiki on https://wiki.cryptshare.com.

Pointsharp is a European cybersecurity company that enables organizations to secure data, identities and access in a user-friendly way. Because we believe easy to use security solutions lay the foundation for a modern digital workplace.

We deliver European made software and services that are made to support even the highest security and regulatory demands of large enterprise organizations and governmental institutions.

Our customers can be all around the world, often in markets requiring extra high levels of security, like the financial, governmental, industrial and defense sectors.

You can find our HQ in Stockholm, Sweden but we also have offices in Germany and the Netherlands.

Pointsharp – Security made easy

Visit our website for more information or a demo

wwww.pointsharp.com

POINTSHARP