ownCloud

Whitepaper

Data Protection and Data Secrecy in ownCloud

Introduction

Data Protection is more important than ever. The GDPR regulation in the European Union, which is effective since May 2018, with similar principles being adopted by other governments worldwide, have led to a prominent focus on data protection. The regulation and subsequent national laws require all data processors to apply state-of-the-art technology to the data of all users containing identifiable information.

Personal data should be protected against leakage to the public, failing which the organization may face legal, monetary or reputational implications. Data Secrecy, in contrast, means protecting any type of data which is important to an organization or to specific people. It might also be important for some organizations that certain data be kept private as obligated by contracts such as non-disclosure agreements that require internal corporate data to be handled in a stringent manner.

Data Protection, as regulated by the GDPR in the European Union, can be achieved by combining physical protection and organizational protection. Physical protection aims to make sure that no unauthorized user can access your data center and servers. Organizational protection, on the other hand, refers to the process of ensuring that the administrators are informed and all actions are logged and auditable. In most cases, these two layers of protection are enough to comply with GDPR.

Data Secrecy is inherently different from data protection. Generally all data is segregated between users inside ownCloud itself. If files are not shared with another user, the other user cannot, under any circumstance, access such files. There are policies available that prevent sharing or accessing certain files in certain ways through the ownCloud File Firewall or the ownCloud Document Classification extensions. Such policies, however, still allow the system administrator to read all the data accessible by ownCloud. Therefore, such data must be encrypted in order to prevent access by the system administrator.

Three Layers of Encryption

ownCloud comes equipped with various mechanisms to ensure data protection and secrecy within an organization. Both data protection and data secrecy can benefit from encryption. This paper discusses the different options of encryption available in ownCloud and how these options can help you implement data protection and data secrecy in your ownCloud content collaboration platform.

For both data protection and data secrecy, encryption can be an absolute duty, a helpful utility or a cumbersome practice to work with. Data can be encrypted at three different levels in an ownCloud setup – in transit, at rest and at the endpoint. The last option is also called end-to-end encryption.

1. Encryption in Transit

Encryption in transit is available in ownCloud by design and by default. This is assured by using HTTPS, leveraging the newest TLS protocols in all supported browsers and clients. The same is true for all connections to storage, directory and authentication servers or the supported collaborative editing services. Encryption in transit is mandatory under GDPR for data protection and already considered state-of-the-art by several court rulings. It is also mandatory for ensuring data secrecy.

2a. Encryption at Rest

Encryption at rest means encrypting all files saved from the ownCloud application server prior to saving them on the actual storage. ownCloud uses a master key encryption method for this that is supported on all file systems. For S3 object storage, the native S3 encryption mechanism is recommended. Master key encryption prevents files to be read from the storage. They are encrypted with a file key that is encrypted with the master key. As the master key is located on the storage, the system administrator can combine both the file and the master key to decrypt files. This form of encryption is sufficient to prevent data secrecy issues related to physical access to the storage including stolen hard disks.

2b. Encryption at Rest with Master Key in Hardware Security Module (HSM)

In order to exclude the system administrator from the ability to decrypt files, ownCloud makes it possible to put the master key into an HSM. This means that the file key is sent to the HSM and decrypted there through a process inside the ownCloud application. As long as the integrity of the ownCloud application server is intact there is no way for the system administrator to read the content.

For practical reasons, file names cannot be encrypted, and so they should not contain confindential information. This ensures that data secrecy is taken care of as long as you have proper organizational mechanisms in place to prevent and detect malicious behavior.

An HSM or a hardware security module, which secures the master key, reacts only on the request of the ownCloud application. Today, HSMs are also available as software, appliance solutions or small hardware dongles, which fit into an USB port. ownCloud supports certified HSMs via PKCS 11.

The above encryption at rest solutions have a distinct disadvantage with regard to performance: any encryption operation needs cycles and makes ownCloud slower. If you share 20,000 files with another user, a lot of keys must be added to the system and decryption and encryption of file keys must happen. For each file, a call to the HSM is needed. In this case, either a second ownCloud instance can be installed, which holds all the data with additional protection needs, or an end-to-end encryption solution can be deployed.

3. End-to-End Encryption

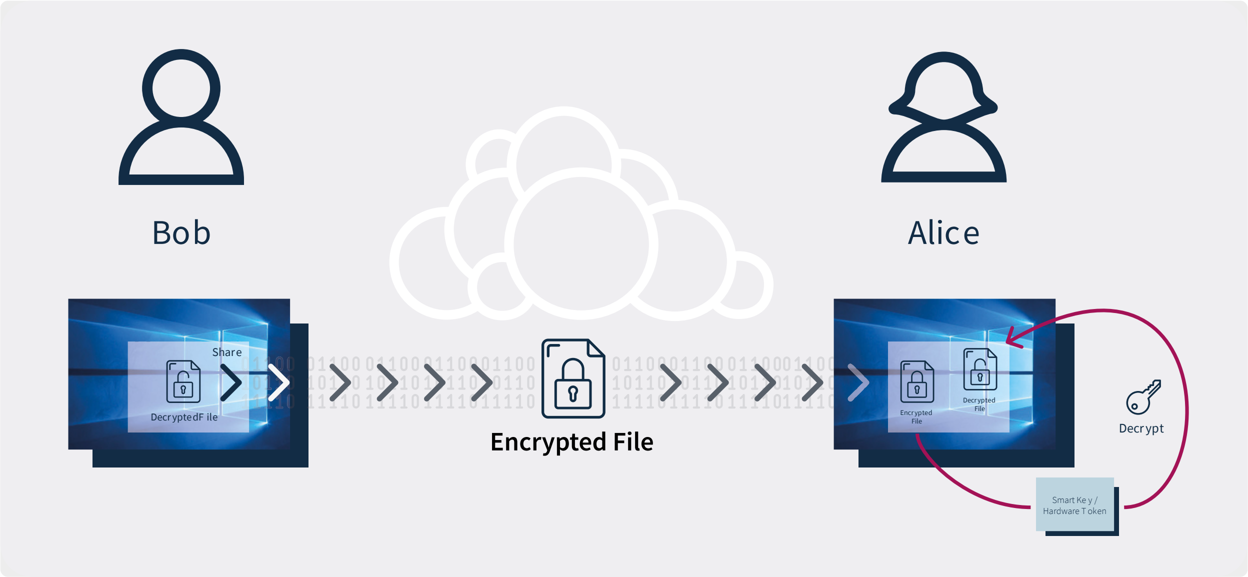
End-to-end encryption is the only viable solution that can claim to assure that no unauthorized third party can access the encrypted data, not even the system administrators. This is the highest level of data secrecy combined with the highest level of data protection. When using end-to-end encryption solutions, the user needs to consider the secrecy or data protection requirements of files in each folder and the performance overhead on the client side. It is also important to remember that the system administrator cannot recover any data for the user, and that, if the private key is lost, the data cannot be decrypted in any other manner.

ownCloud provides an End-to-End Encryption plugin in addition to the ownCloud Enterprise Edition subscription. The plugin subscription pricing starts at 1000 EUR/year for up to 50 users. When the plugin is enabled for a partical user, he/she can encrypt any empty folder. Additional users can be invited through the process of sharing.

For every file uploaded, the uploader can view a list of users to whom the particular file has been shared. Before uploading to the server, the file is encrypted inside the browser leveraging a JavaScript plugin delivered to the user's browser securely. The files are encrypted with public keys fetched from the server. The decryption mechanism happens inside the browser as well. This requires the presence of the private key in the browser.

For maximum security, ownCloud provides an additional key service. The key service assures that the private key can be kept outside of the browser, even in the form of a smart key, a piece of hardware which prevents that the private key of the user is ever known on the end user, living exclusively on the hardware device.

With end-to-end encryption enabled, it is not possible to leverage collaborative editing or any server-side function, including virus scanning. However, as the solution is inside the web browser, it is very convenient, easy to use and needs no additional software to be installed.



End-to-end encryption with a key service fulfills the highest needs for data secrecy and data protection.

The Role of the Outlook Plugin in Encryption

Email is still the number one file sharing utility, even though it is usually non-encrypted. ownCloud provides the Outlook Plugin, which helps users to secure their email communications. Any attachment is automatically put into ownCloud and replaced with a link, with the option of password-protecting the link.

Together with the ownCloud End-to-End encryption plugin, all attachments are encrypted using the receiver public key.

Exception: Medical data according to article 9 sentence 2.h in conjunction with sentence 3

If your organization deals with medical data, you need to apply either the master key in HSM or the end-to-end encryption method. Another possible option is to ensure that your system administrators are legally obligated to secrecy.

Summary

ownCloud has a solution for any challenges with regard to data protection and data secrecy. Please feel free to get in touch with us to discuss the unique needs of your enterprise, including the attack vectors you would like to be protected against. A proper ownCloud setup with the proper add-ons will deliver the highest security needs even for the most sensitive data, no matter the size of the organization.

About ownCloud

ownCloud develops and provides open-source software for content collaboration, allowing teams to easily share and work on files seamlessly regardless of device or location. More than 100 million users worldwide already use ownCloud as an alternative to public clouds – and thereby opt for more digital sovereignty, security and data protection.

For further information, please visit owncloud.com or find @ownCloud on Twitter.

Whitepaper Data Protection & Secrecy EN 202207

ownCloud GmbH
Rathsbergstr. 17
90411 Nürnberg
Germany

Contact:
owncloud.com/contact
Phone: +49 911 14888690
owncloud.com

@ownCloud
facebook.com/owncloud
linkedin.com/company/owncloud