ONLYOFFICE

End-to-end document encryption

January 2021

Abstract

To help protect sensitive information stored in documents, ONLYOFFICE presents end-to-end encryption of documents via Private Room feature of ONLYOFFICE Workspace that employs two-stage encryption mechanism. It is applicable not only to resting files, but also to active data: with Private Rooms functionality, it is possible to encrypt documents, spreadsheets and presentations to safely store them in ONLYOFFICE, edit and co-edit them with other users in the encrypted form. Read this white paper to understand the technology, mechanisms and usage scenarios for this functionality.

This White Paper describes the components and mechanics document encryption in ONLYOFFICE Workspace. Before referring to the contents of this paper, it is important to compare the version of the encryption functionality relevant to user organization's software.

Contents

Introduction

Document encryption is available in self-hosted solutions of ONLYOFFICE to give users additional individual means of protecting electronic documents from unauthorized access from the outside and the inside the organization.

File storage and desktop editing can be secured by known measures such as one-step AES encryption, but document processing and management scenarios are not limited to just that. These also include online editing and collaboration, and there the related gaps in file security - in real-time data transfer and authorized sharing. Overcoming these limitations of previously existing individual document protection is the key objective of the encryption scheme in question.

Key technological advantages of ONLYOFFICE encryption scheme:

- Document encryption model in ONLYOFFICE allows reaching level of data protection highly tolerant to known methods of encryption hacking, while offering secure and convenient key management.
- Symmetric AES-256 encryption is ultimately resistant to brute force.
- There's little to no chance for users to mishandle the passwords to documents because they are generated automatically and stored in encrypted form.
- Asymmetric encryption of document passwords allows safe sharing of protected documents between users because no plain text password exchange is involved.
- This model allows real-time encrypted editing and collaboration.
- True end-to-end: encryption and decryption are carried out on user's machine.

Role within typical threat model

The technology is designed to compliment other data security practices against unauthorized access to the files and to establish security regulation compliance.

Protection from unauthorized access from the outside

Individual file encryption helps protect organization's sensitive information from breach and alteration. In case the attacker obtains access to the file system (with illegitimate authorization, social engineering, etc.) or direct physical access to data carrier itself.

Protection from insider actions

Individual file encryption might be the best way to protect sensitive information against malicious actions of individuals having legitimate access to the file system.

This stands not only for actual employees of the company, but also for external contractors and consultants that are given access to the data relevant to their primary tasks.

Regulation compliance

Commonplace cloud security threats not only directly shape the data protection policy, but also become a ground for preventive regulations aimed at leveraging these threats at the macro scale.

Establishing safeguards for sensitive data protection may be required by industry- or government-specific legislation among technical requirements for organizations dealing with certain types of data.

For example, medical organizations seek compliance with HIPAA in order to carry out operations in the USA and elsewhere, while the Act requires data encryption as one of the technical safeguards.

Deficiencies of the universal approach

With agility of present-day data sharing methods come numerous related security issues that are not solved by most, if not any, of the existing solutions:

- Safe password creation requires knowledge in basic password strength standards. It also relies on manual safekeeping of these passwords.
- Insecure sharing of this data presents a direct threat to the information.
- Single-stage encryption and decryption necessarily limits the abilities such as group access and co-editing, forcing the users to restructure common workflows.
- Centralized key management schemes in storage encryption relocate the threat focus, but said model of encryption does not allow individual file protection.
- Basic training in data security is required to teach data safety principles and tools to the employees.

The encryption scheme applied in ONLYOFFICE Private Rooms provides necessary technological basis to lift these limitations:

- Document encryption model in ONLYOFFICE allows reaching level of data protection highly tolerant to known methods of encryption hacking, while offering secure and convenient key management.
- Symmetric AES-256 encryption is ultimately resistant to brute force.
- There's little to no chance users mishandle the passwords to documents because they are generated automatically and stored in encrypted form.
- Second-layer asymmetric encryption of document passwords allows single-action safe sharing of protected documents between users because no plain text password exchange is involved.
- This model allows real-time encrypted editing and collaboration.
- True end-to-end: the encryption is carried out on user's machine and no centralized key management is involved.
- No training is required, as the users work with protected documents in the same way.

Encryption model

Two-layer encryption model used in ONLYOFFICE involves symmetric encryption of documents using AES-256 algorithm and RSA asymmetric encryption of document passwords necessary for authorized sharing and collaboration.

Users need to be registered and authorized in ONLYOFFICE Workplace instance and to acquire the credentials for performing document encryption.

While Private Rooms storage unit is located on the server, encrypted editing is possible exclusively with ONLYOFFICE Desktop Editors app that needs to be installed additionally.

With current model of encryption, its is possible to achieve the following:

Privacy of the encrypted data. Unlike data encryption at rest, end-to-end document encryption in Private Rooms deals with active data of each user or group of users and is not subject to central administration.

Attack-tolerance. AES-256 algorithm ensures that brute force approach to password cracking will not be effective against the document security regardless of the applied computational power.

Secure key sharing model. Message-based principle of the RSA algorithm appears to be the most reliable model for managing authenticated access to the encrypted data as long the private keys are not mishandled by the users. It also allows carrying out operations with partitioned data to maintain the same level of protection while processing data in real time.

File formats

Currently, it is possible to encrypt only OOXML formats, which are DOCX, XLSX, and PPTX. The reason for this design is not only that OOXML are the core formats of ONLYOFFICE editors, but because these formats have composition convenient for performing encryption.

OOXML documents are basically ZIP archives where the XML files are stored. This file structure allows encrypting documents and storing the unencrypted information alongside, in a single file. When these are encrypted using AES-type encryption, the encrypted XML data is placed inside a Compound File Binary File (MS-CFB) that also contains the information necessary for file decryption.

In the chosen model, this standard was used for performing the asymmetric encryption of the initial data to later add the data relevant to further encryption stages while working within a single micro file system-like item.The structure of encryption stages applied in this model is explained in the following chapters.

ZIP-like structure is not exclusive to OOXML file formats and similar encryption scheme can be used when encrypting other formats. However, this version is an early stage of implementing document encryption functionality in ONLYOFFICE, and this paper is dedicated to the current prototype.

Key generation and management

Each user obtains a pair of encryption keys, private and public, when they first log in to the system from their application instance. This personal pair of keys is a necessary element in the asymmetric layer of document encryption and decryption mechanisms.

The scheme of generating and reading the encryption credentials looks as follows:

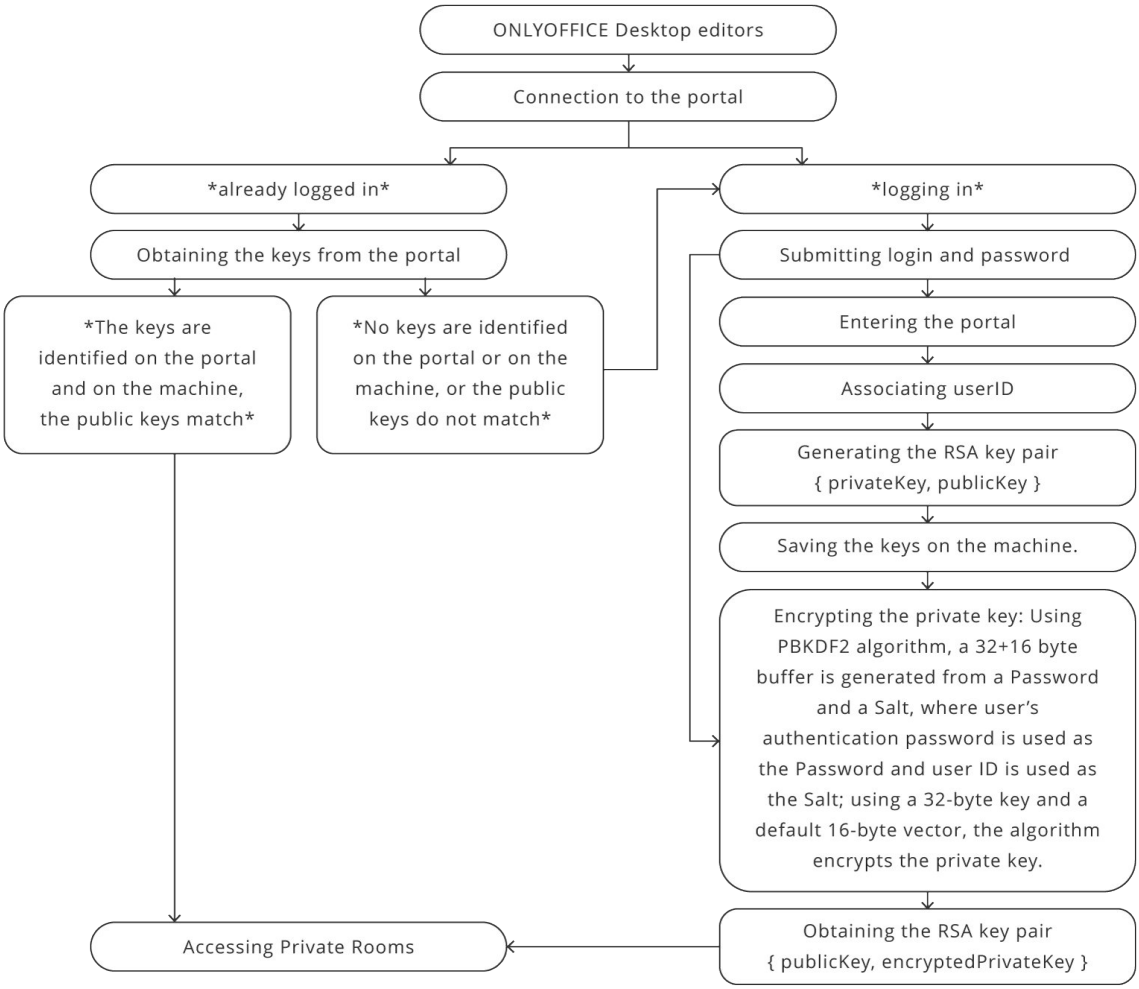

Figure1: Generating and reading the encryption credentials

Here, to to generate the RSA keys, the NSOpenSSL::RSA_GenerateKeys method is used. To encrypt the private key before saving it to the database, ONLYOFFICE uses the NSOpenSSL::AES_Encrypt_desktop algorithm based on AES 256 Cipher Block Chaining.

The private key decryption is performed when a synchronised temporary file copy needs to be decrypted when editing it. To decrypt the key, the NSOpenSSL::AES_Decrypt_desktop algorithm is used.

Operations with encrypted files

To perform operations with encrypted files, including file encryption, decryption, creation, editing and sharing, ONLYOFFICE uses the the individual credentials of users (RSA key pair) and a document password (document encryption key).

The encrypted files, besides the ciphertext itself, contain the arrays of public keys of all users and the document passwords encrypted with these keys. This allows establishing collective access to the file, therefore making possible sharing and collaboration on the encrypted documents.

The file password is encrypted with each authorized user's public key using NSOpenSSL::RSA_EncryptPublic_desktop method.

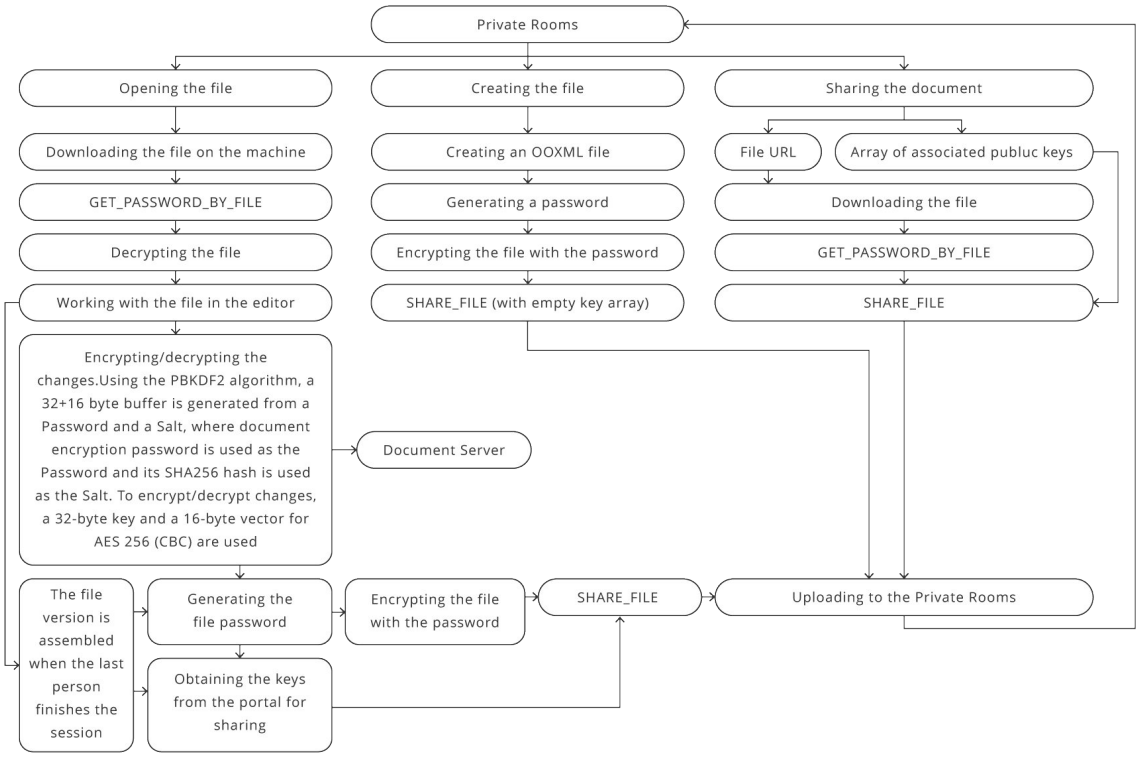

Figure 2: Operations with encrypted files

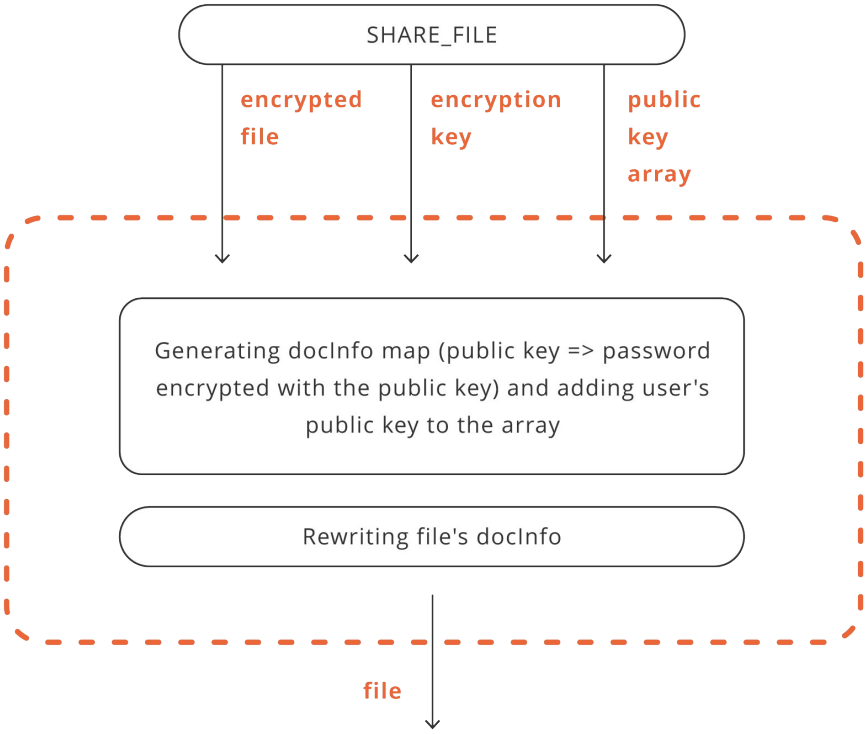

Figure 3: Updating the changed file on the server (SHARE_FILE)

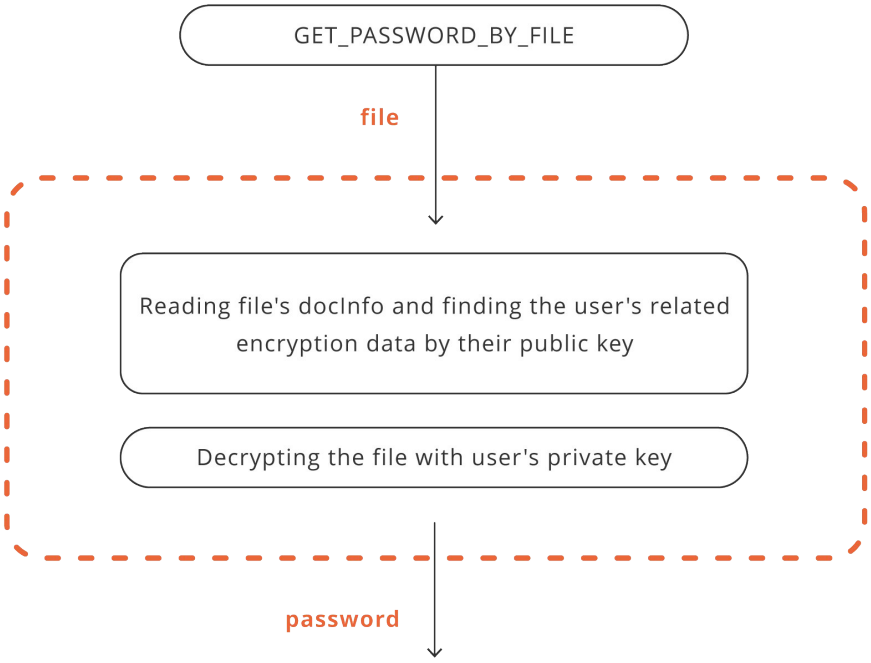

Figure 4: Adding the new user's encryption credentials to the encrypted file when creating or sharing (GET_PASSWORD_BY_FILE)

To encrypt the file password with each authorized user's public key the NSOpenSSL::RSA_EncryptPublic_desktop algorithm is used. The reverse NSOpenSSL::RSA_DecryptPrivate_desktop algorithm is used to decrypt the file using the user's private key.

When accessing the encrypted file, it is first is sent to the user's machine before the application begins the decryption.

Each individual input in the document during the editing session is encrypted using NSOpenSSL::AES_Encrypt_desktop algorithm based on AES-256 CBC.

All saved changes are then sent to the portal and are individually decrypted on each user's machine using NSOpenSSL::AES_Decrypt_desktop method.

Data location

ONLYOFFICE leverages data storage, for documents and the encrypted data between the cloud storage and the user's local storage to maintain the applied scheme. The distribution of data looks as follows:

Item	**Location within the instance**	**Location on device**
Private key	Encrypted, in the Database	-
Public key	Database and within encrypted files in the (file system)	-
File encryption key	Encrypted, within the encrypted files (in the file system)	-
User password	-	-
Encrypted files at rest	On the server	-
Encrypted files when editing		On machine, In temporary folder

Limitations

There are several limitations that apply to document encryption in Private Rooms, as well as limitations of otherwise default functionality necessary to provide sufficient level of security.

Access to Private rooms. This functionality is available only via ONLYOFFICE Desktop Editors app, to users that have personal pairs of encryption keys. It also means that sharing and collaboration is not possible if a partner doesn't have an associated pair of keys.

Encrypted file management. Private Rooms contain encrypted files and folders owned by current user, as well as those shared with them. All files in the Private Room are encrypted end-to-end: Users can create new encrypted files, or upload existing files which will be automatically encrypted.

Operations with encrypted files. There are certain actions users can and cannot perform with the encrypted files in Private Rooms:

+	-
Creation of files and folders	File and folder copying
Access to items shared with user	Moving items outside Private Rooms
Moving files owned by user, only within Private Rooms	Moving items shared with user
Permanent deletion of files	Recovering files from bin
	Recovering file versions
	File overwriting

Storage mechanics. Each file is downloaded on device before editing as a synchronized copy, and all the changes are sent to the portal of ONLYOFFICE instance in the encrypted form when saved.

Compatible formats. At this point, document encryption is available for OOXML files only.

Software requirements. To have access to Private Rooms functionality, it is required to have ONLYOFFICE Workspace with ONLYOFFICE Control Panel version 11.0 and higher installed on private network, as well as ONLYOFFICE Desktop Editors version 6.0 and higher installed on the user's machine.

Conclusion

In private and public cloud environments, sensitive data stored in electronic documents remains vulnerable to breach from outside and inside of the organization. Protecting these files with casual means such as password encryption is a halfway measure because aspects of file sharing and collaborative editing remain hardly secure and most certainly not convenient.

ONLYOFFICE created a mechanism for end-to-end document encryption that makes safe storage, editing and collaboration possible without significant limitations in terms of the user experience: Private Rooms. This paper explores the technology behind this functionality, it’s principles and components, limitations and UI mechanics.