ONLYOFFICE

# ONLYOFFICE Private Rooms: 9 security principles

Ascensio System SIA

September 2021

# Contents

# Introduction

In this paper, we describe the principles used in ONLYOFFICE Private Rooms to ensure security on every step of working with documents.

# Registering users in Private Rooms

Users are registered in Private Rooms automatically with the same credentials when their accounts in ONLYOFFICE Workspace are created. Logins are stored as plain text in ONLYOFFICE Workspace database. Instead of user passwords, their hash codes calculated using PBKDF2 algorithm is stored on the server. The unique instance id is used as a cryptographic salt.

# Storing and editing document

Private Rooms allow storing and editing Open XML files, namely DOCX, XLSX, PPTX. All the files stored in Private rooms are encrypted. Users don’t need to remember passwords for each file, decrypt them to edit in an unprotected form, and then encrypt them again. Encryption is performed automatically, including all the temporary files on the disk and data exchange between clients during co-editing (in this case data transfer is carried out using encrypted blocks).

## Encrypting documents with AES-256

In Private Rooms, documents are encrypted using AES-256, a symmetric block cipher algorithm. The encrypted information is written to files in accordance with Open XML specifications. This means that the encryption is performed the same way as in Microsoft Office and it's possible to open files, encrypted in ONLYOFFICE Private Rooms, in other applications that support the Open XML standard.

## Generating password for document encryption

Passwords for document encryption are automatically generated using a random number generator, created with the Mozilla library — https://developer.mozilla.org/en-US/docs/Web/API/Crypto/getRandomValues. The password is 32 characters long and has the form of a UUID identifier — https://en.wikipedia.org/wiki/Universally_unique_identifier.

A new unique password is generated for each new document. In general, the user does not know the password to any of their documents as the program automatically creates and stores them in encrypted form in the service area of the document. If necessary, the user can get their document passwords to edit the files in another application (e.g. MS Office).

## Storing encrypted document passwords

Studies showed that people tend to write long and secure passwords down as it is difficult to memorize them. In Private Rooms, passwords are encrypted and recorded automatically to the service area of the document. The RSA algorithm is used for password encryption.

## Encrypting document passwords with RSA

When a user enters Private Room for the first time, their private and public key are generated on the client. This pair will be used for RSA encryption.

The public key is stored as plain text in ONLYOFFICE Workspace user database.

The private key is encrypted on the client using the AES-256 algorithm and then saved to the database. User password hash calculated by PBKDF2 algorithm (See section 2) is used as a password for encryption. The user id is used as salt for PBKDF2 algorithm.

To record the document password to the service area of the document, the client software performs the following actions:

- downloads the user public key from the server;
- encrypts document password with the public key;
- records the encrypted password to the file service area.

To read the document password, the client software:

- downloads the user private key from the server;
- decrypts the password using the private key.

## Sharing encrypted files with other users

To grant access to the encrypted document to a colleague, the user needs to securely share the password to the file with them. The mechanism is the same as described in Section 7: the document password is encrypted with the public key of the user to whom the file is being shared. This password is then saved to the service area of the file.

This way, the service area of the file is used as storage for encrypted document passwords. For example, if the file is shared with 10 users, it will contain 10 encrypted passwords.

## Co-editing encrypted documents

Private Rooms allow users to co-edit encrypted documents in real-time. Encrypted passwords for each user, who will edit the file, are recorded in the service area of the document.

During the co-editing process, all user inputs are organized in blocks and passed to other users, who are working with the file, through the server. To exclude data leaks during the exchange between the clients and the server, all the blocks are encrypted on the client. This means that co-editing documents in Private Rooms is performed in the end-to-end encryption mode.

To encrypt the data blocks, the standard symmetric encryption algorithm AES 256 GSM with data verification is used. The document password serves as a key for encryption as it is known to all the users who are editing the file.

# Basic algorithms used in Private Rooms

ONLYOFFICE Private Rooms use the OpenSSL library acknowledged by cryptography specialists all over the world.

Currently, Private Rooms are available through ONLYOFFICE Desktop Editors as client software. Working in the end-to-end encryption mode in browsers and on mobile devices are on the roadmap.

The source code is available on GitHub, anyone can access it and conduct an audit if necessary:

- Encryption plugin for ONLYOFFICE Desktop Editors. See source code
- Core of ONLYOFFICE Desktop Editors, the client software. See source code
- Server components for work with OpenSSL. See source code