CIF-KM: SECURE DOCUMENT MANAGEMENT

CIF-KM
MAXIMUM SECURITY

- **General encryption:** Encrypted files stored in the server.
- **Individual encryption:** Access exclusively for authorized users, per file and necessity.
- **Simple use**

CIF-KM has three levels of security to guarantee that only the authorized users have access to the files stored in the document management system.

The first level of security is the one CIF-KM provides by definition. As a document management system, it provides access to the information by means of "smartbox": information cards that contain a series of data and files for their consultation and administration by a set of authorized users.

Each Smartbox incorporates its own system of permissions that determines who may access its contents and with which faculties.

However, there are times when it is necessary to have greater security that guarantees that no one external to the life cycle of the files has access to them.

The files are only obtained by means of the application, with permissions.

The general encryption prevents the leakage of information by means of the copy of files in the CIF-KM server.

GENERAL ENCRYPTION

The general encryption is a CIF-KM server configuration option to maintain the file repository encrypted, by means of the automatic encryption with an AES algorithm of all the files that reach the server, in such a way that these may only be viewed with CIF-KM, in accordance with each one´s access rules and permissions.

Thus, even though a person has access to the server where CIF-KM is hosted, which may always happen, he/she won´t be able to view any file stored in this server if he/she doesn´t use the CIF-KM application with the appropriate permissions in it. Thus preventing leaks by means of the copy of files.

However, for the CIF-KM user all is transparent, since both the encryption and decryption of files is done automatically from the application without any user intervention.

INDIVIDUAL ENCRYPTION FOR CONFIDENTIAL FILES

What advantages does the individual encryption

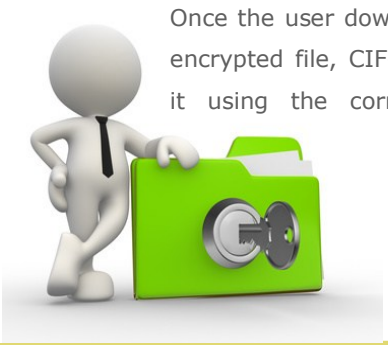
- A user may have in CIF-KM files **that only he/she may decrypt.**
- A group of persons may collaborate with the **certainty** that **only they may decrypt** the files that they use and that are made available to them.
- Two or more persons may correspond via email, reminders or CIF-KM notes, with **hyperlinks to confidential files** thus encrypted, with the greatest confidence that only they may view them, and no other person, even though that person may access his/her email folders

INDIVIDUAL ENCRYPTION FOR CONFIDENTIAL FILES

Is it a simple process for the user?:

Encrypting and decrypting is very easy for the user. CIF-KM only asks him/her to choose a secret word, or phrase that only he/she knows and that he/she doesn´t tell anyone.

Each time a file is encrypted or decrypted, CIF-KM will only ask the user to enter the secret word chosen and nothing else. It is this simple and transparent.



Once the user downloads the encrypted file, CIF-KM opens it using the corresponding application (for example, Microsoft Word) and he/she may make changes on it.

As soon as he/she saves all the changes, CIF-KM will save the file again in the server, encrypting it for all the users with access to it automatically and transparently. It still being possible to consult the history of changes of this file (always by authorized users).

The user may carry out the encryption or decryption in any computer that has the CIF-KM client program installed in which he/she identifies him/herself with his/her username and password.

Who may encrypt or decrypt files?:

Any user who:

- Is authorized with the faculty to use encryption keys (by means of the configuration of CIF-KM).
- Has permissions to upload and/or modify files in the corresponding Smartbox where the file is located.
- Is expressly authorized over the specific file to decrypt it, either because he/she has encrypted it or because he/she has been authorized by another user who was previously authorized.

Is the system of encryption robust and secure?:

The security is complete since it depends on someone being able to know the secret word that the user has chosen, apart from the username that identifies him/her in CIF-KM.

Then entire process is done with the CIF-KM client program in the workstation. The CIF-KM server doesn´t intervene in the encryption and decryption processes, it only receives and saves the files and encrypted keys.

The access is controlled individually per file, even within the same Smartbox, with secure and independent access lists for a greater control of the visibility of sensitive documentation.

CIF-KM uses standard technologies for encryption by means of asymmetric RSA keys and a Rijndale AES algorithm of 256 bits.

SECURE DOCUMENT MANAGEMENT

CIF-KM

www.cifkm.com/

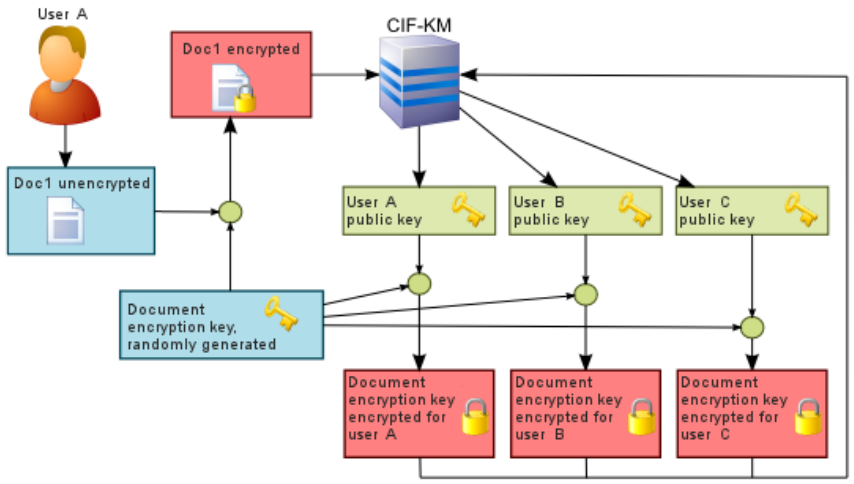
INDIVIDUAL ENCRYPTION FOR CONFIDENTIAL FILES

Operation:

Two random asymmetric RSA keys are generated for each user authorized to use encryption:

- **Public key** that will allow this user to encrypt information.
- **Private key** with which this user may access his/her encrypted contents.

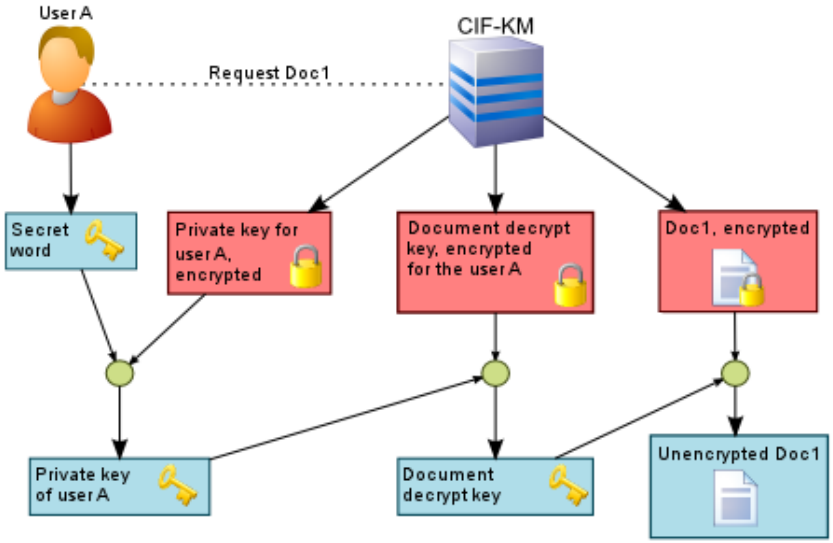
A secret word is required from the user with which the private key is encrypted by means of AES, and they are sent to the server.



When the encryption of a file is requested, **the client program of the user that does this generates a random key with which the file is encrypted using an AES algorithm, and this random key is encrypted in turn with the public key of each user** who is authorized to access this file.

SECURE CIF-KM

THE SERVER NEVER HAS ACCESS TO UNENCRYPTED INFORMATION.



The CIF-KM client program sends the server the encrypted file and all the encrypted keys (the server will never have access to the clear information).

To access an encrypted file, the client program requests the encrypted file form the server, the key for the decryption of this file for this user and the private key of the user.

The user confirms his/her access entering the secret word in the client program, with which first the file encryption key is decrypted, and then the file itself, showing the user the file so that he/she may work with it.