seald

File encryption you will use

Your activity involves processing strategic or personal data, which is duplicated, saved and transferred multiple times. So how do you ensure confidentiality, traceability, compliance with legal retention periods and removal requests for each piece of data?

4M€ THE AVERAGE FINE IMPOSED UNDER THE GDPR

Every day, your company collects personal data from your customers, partners, etc., which impose certain constraints on you (in particular through the GDPR):
- confidentiality;
- traceability;
- exercise of the right of removal;
- compliance with the legal retention period.

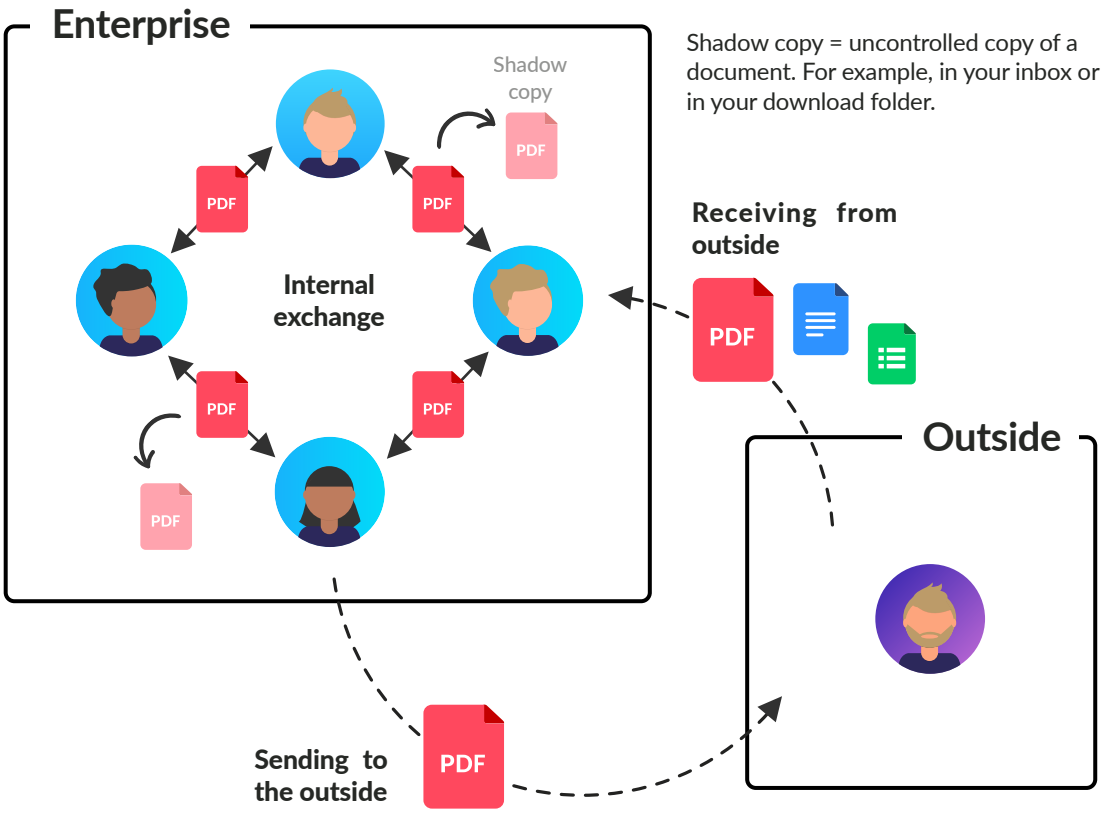
Ensuring that your customers' personal data remain confidential is necessary for the health of your company. **A single leak can irreversibly damage your reputation** and expose you to significant direct and indirect financial losses. **The only way to achieve this is to protect the data as soon as it arrives in your company.**

IT'S NOT A QUESTION OF IF BUT WHEN...

Threats do not only affect the personal data that your company manages. Your company also **produces strategic data every day that is vulnerable to cyber threats** that are intended for:
- economic espionage;
- destabilization;

of your company or your clients / subcontractors.

Your intellectual property, your financial data, your strategic plans, your business negotiations are all prime targets to achieve these goals. Protecting them is a universal challenge: the more collaborative your company becomes, the more difficult it is to control this valuable information.



80%
of CESIN companies report having suffered at least one attack in 2018

20%
of French companies only claim to be able to manage an attack

56%
of leaks are caused by a malicious third party

18M
pieces of data leak every day

3,6M€
the average cost of a data breach

220
days on average are required to detect a data leak

ALGORITHMS USED

- AES-CBC 256 bits
- HMAC-SHA-256
- RSA-OAEP, RSA-PSS 4096 bits

OS COMPATIBILITY

- Windows 7
- Windows 10
- MacOS (10.9+)
- iOS
- Android

A SIMPLE SOLUTION AT EACH STEP

Throughout their lifetime, your files are duplicated, forwarded or backed up, making it impossible to control them. More than just an encryption tool, **Seald integrates with disconcerting ease in all use cases.**

Receiving from outside

Seald Secure Transfer encrypts data before it is received in your company. Customize it to your colors or integrate it directly into your applications.

Internal exchange

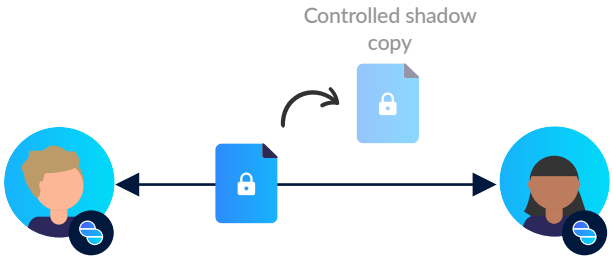
Seald applications allow you to encrypt, decrypt and control your sensitive documents with just a few clicks. No more nightmare of key & certificate management.

Sending to the outside

Seald technology allows you to send encrypted documents to your recipients who can open and read them without having to install anything. They are authenticated by email and/or text message.

Shadow copy

A file protected with Seald can be duplicated securely. Shadow copies are as protected as the original file.



COMPLETE PROTECTION OF YOUR FILES

Seald defends your files but also monitors their use and manages their access rights in real-time, even if the files have been downloaded.

Confidentiality

Allows you to make the contents of your files accessible only to authorized persons.

Management of access rights

Allows you to add or remove accesses to your files in real-time.

Traceability

Allows you to track the use of your files, to know where and when your files were opened.

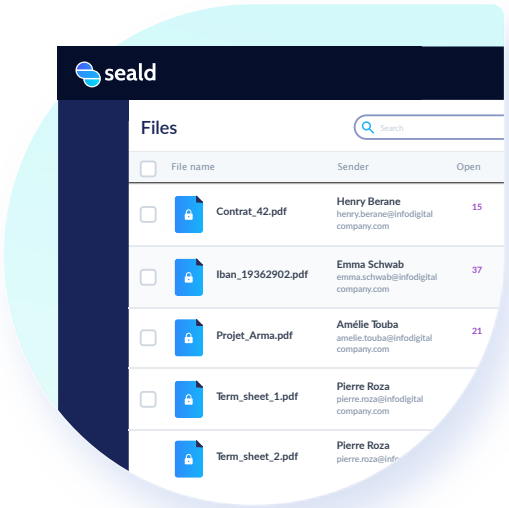
Secure transfer

Allows you to secure a file when it is received or sent.

A DASHBOARD TO TRACK AND CONTROL YOUR SECURE FILES

Seald allows advanced control over the granting or revoking of access to your documents, and also offers tracking tools.

- User management
- Device management
- File management
- Reversibility tool
- Usage statistics
- Audit trail
- Backup key
- SDK



SECURITY AT SEALD

As a security application, Seald must be transparent about how it protects both its infrastructure and your information. Indeed, the solution has been designed using state-of-the-art methods and following the strictest recommendations.

All Seald's servers are **hosted in France.** If you want to host your own instances, an architecture evaluation is possible.

Seald **follows the NIST and ANSSI recommendations** on encryption. Documents are protected with 256-bit symmetric keys using the AES-CBC-HMAC-SHA256 algorithm. These keys are then protected by asymmetric cryptography with 4096-bit RSA keys, using the RSA-OAEP algorithm, whose private keys never pass over our services.

Seald offers a security model designed to resist remote attacks. Indeed, all encryption operations are performed locally, including key generation. Thus, Seald servers never have access to sensitive data.

AFCDP · PSA GROUPE · Silicom. · TF Bank TUNISIAN FOREIGN BANK · DPO101 par Bensoussan & ASSOCIÉS · Exer

To learn more, contact us:

Seald
10, rue la Boétie
75008 Paris - France
contact@seald.io
+33 (0)184807877

seald
www.seald.io