End-to-end encrypted spheres

Native Cryptoner technology

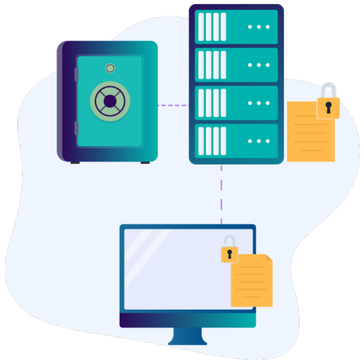
Whaller

Cryptoner

Whaller offers native end-to-end encryption of messages and files shared in spheres.

This encryption system, called « *Cryptoner* », is a major innovation: it is based on the SKRED and OLVID messaging solutions, but applied to a more complex collaborative environment, and accessible via a browser.

This is the first web-based solution for end-to-end encryption of a digital workplace, without deporting secrets to the server side.



Server encryption

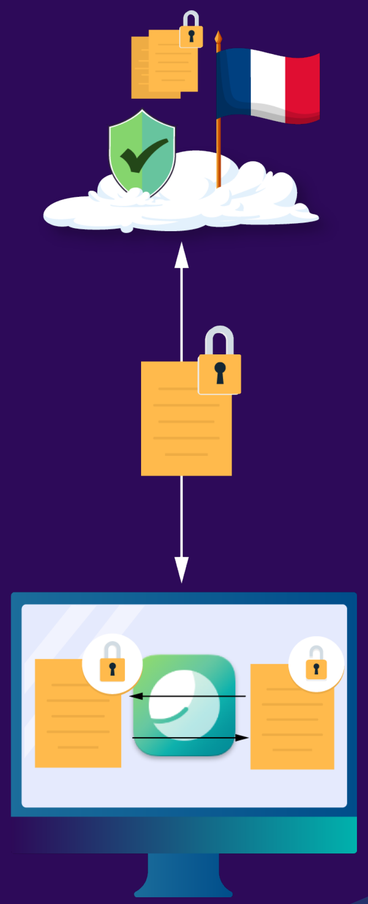
Classic end-to-end encryption architecture

as: Seald, Tanker

« *Cryptoner* » architecture by Whaller:

client-side management of peer-to-peer secrets.

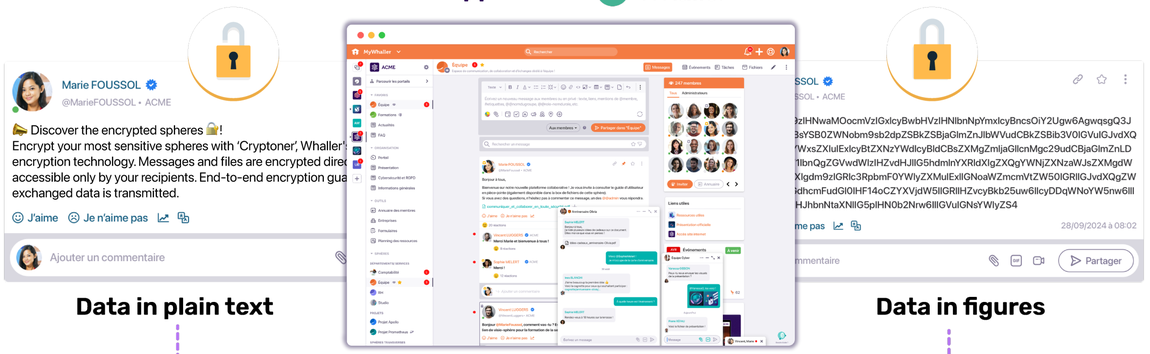
End-to-end encrypted spheres



- The creator of a sphere can decide, when creating a sphere, to encrypt all future exchanges and files.
- In this way, customers can have both encrypted and unencrypted Spheres on their network.
- Whaller provides true end-to-end encryption: no secret is transferred to the backend, all data is encrypted
- The data cannot be deciphered by a system administrator or an attacker who has managed to gain access to the infrastructure
- Only members of an encrypted sphere can decrypt its contents

Simplified block diagram

Web application Whaller

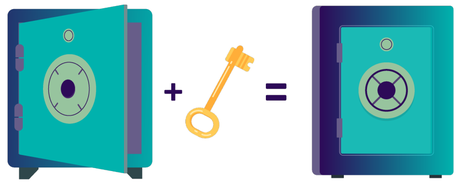


Data in plain text

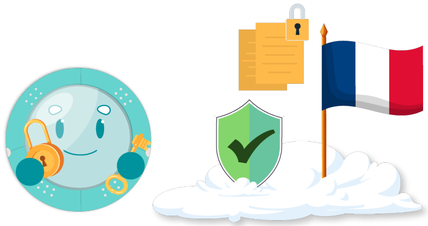
Data in figures

Browser-based encryption

Peer-to-peer key exchange, end-to-end encryption serverless



Figures only



Secrets: the core of end-to-end encryption

Definition: secrets are symmetrical keys used to encrypt and decrypt messages and files exchanged within one or more Whaller spheres.

Sphere secret generation:

An AES-256 symmetric key is randomly generated on the device of the first member of the sphere (the user who created the sphere) using a cryptographically secure random number generator. Algorithm: AES (Advanced Encryption Standard) with a key length of 256 bits.

Secure storage:

Key derivation (PBKDF2): The secret is encrypted with a key derived from a PIN code defined by each user, for each sphere.

Peer-to-peer transfer:

To share the secret of a sphere with other members of that sphere, Whaller uses ephemeral asymmetric keys: RSA-OAEP (4096 bits).

Peer-to-peer transfer: enhanced security

What is it?

- **Secure transfer of the « *Secret* »:** the Secret (data encryption key) is exchanged directly on a peer-to-peer basis, i.e. browser-to-browser, between users on the same Whaller network. This process eliminates any intermediaries, considerably reducing the risk of data interception or compromise.
- **Public/private keys:** Peer-to-peer transfers are encrypted by the temporary creation of a public/private pair, which is deleted once the transaction has been completed.
- **Secure storage:** the Secret and the keys are never stored on a server, but exclusively locally on the user's device, guaranteeing maximum confidentiality.

Secret generation, storage and hydration.

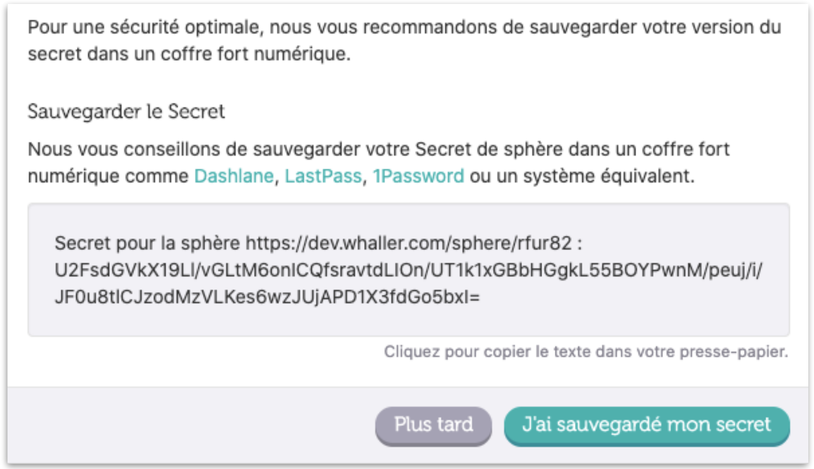
A secret is generated either for each sphere, or for all the encrypted spheres in an organisation.

This secret is generated the first time an encrypted Sphere is activated by anyone.

This secret must be saved by the user (the customer) in a safe place (encrypted and protected by a password) and replicated.

The secret is then transmitted to all the peer-to-peer users. For this to happen, another user must be connected at the same time when they first connect to an encrypted sphere.

The users can then see the secret and save it.



Encryption perimeter and limitations

Data protected by end-to-end encryption :

- **Messages and comments:** all text entered by users within the spheres is encrypted.
- **Shared files:** attachments to messages and comments are encrypted.
- **File box:** all files stored in the file box are encrypted.

Technical limitations to be taken into account :

End-to-end encryption offers maximum security for your critical data, but it does imply certain functional restrictions.

1. **Searching content:** messages and documents cannot be searched by content due to encryption, only by file name.
2. **Viewing and co-editing documents:** documents can no longer be sent to OnlyOffice via the servers for collaborative editing.
3. **Videoconferencing:** the current solution (BigBlueButton) offers encryption in transit, but not end-to-end encryption. However, videoconferences are not stored once they have ended.

Thank you!

Whaller - contact@whaller.com