Sphères chiffrées de bout en bout

Technologie native Cryptoner

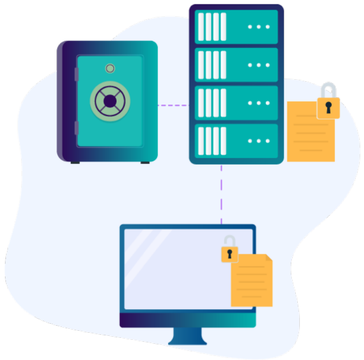
Whaller

Cryptoner

Whaller propose un système de chiffrement de bout en bout natif des messages et fichiers partagés dans les sphères.

Ce système de chiffrement, baptisé « *Cryptoner* » est une innovation majeure : elle s'inspire des solutions de messageries SKRED et OLVID, mais appliquée à un environnement collaboratif plus complexe, et accessible via navigateur.

C'est la première solution web de chiffrement de bout en bout d'une digital workplace sans déportation des secrets côté serveur.



Chiffrement côté serveur

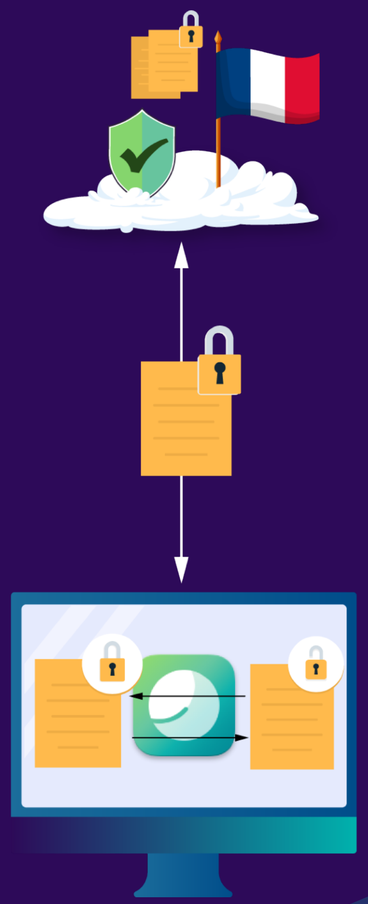
Architecture classique de chiffrement de bout-en-bout

type : Seald, Tanker

Architecture « Cryptoner » par Whaller :

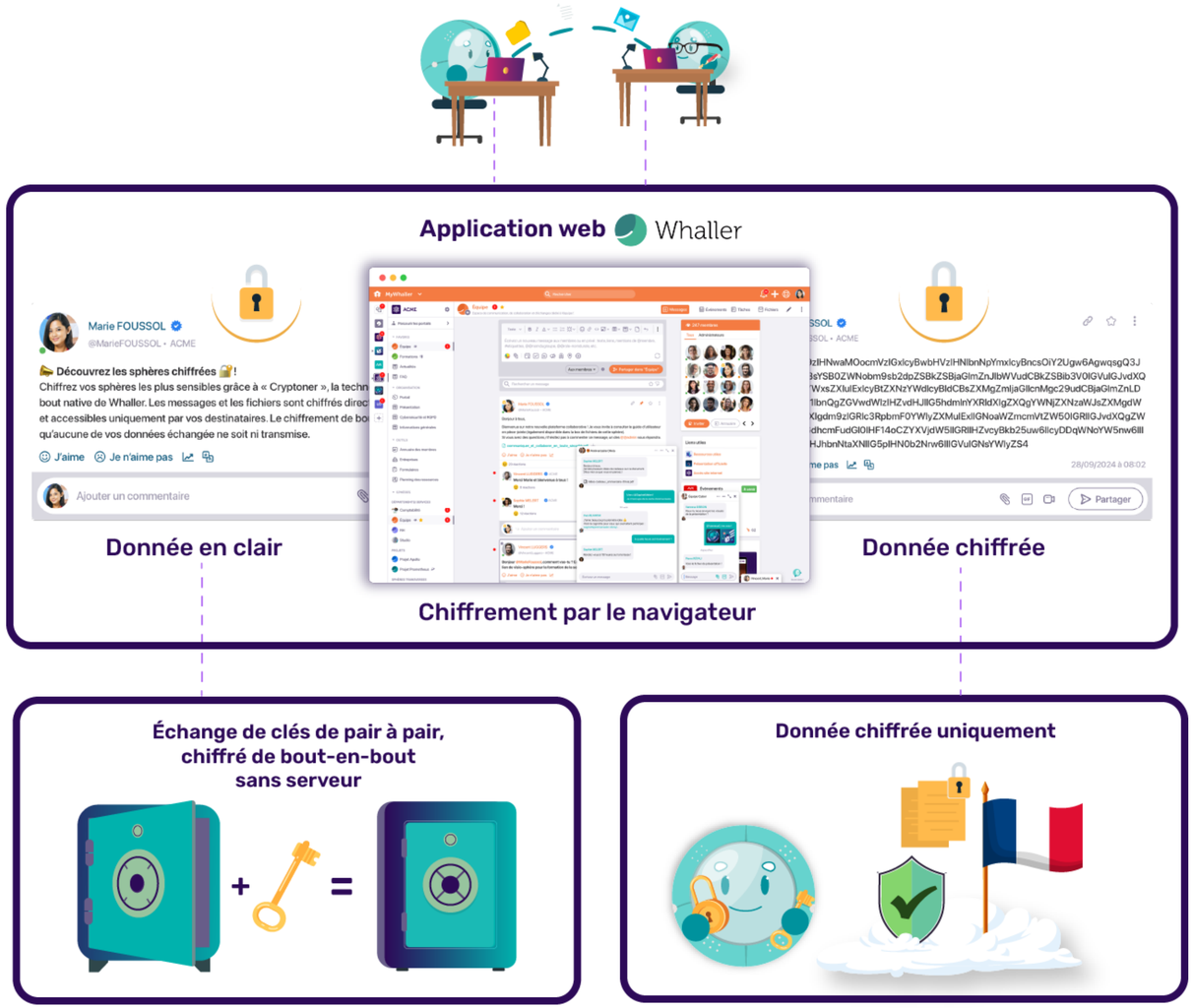
gestion des secrets de pair à pair, côté client.

Les sphères chiffrées



- Le créateur d'une sphère peut décider, au moment de la création d'une sphère, de chiffrer l'ensemble de ses futurs échanges et fichiers
- Ainsi, dans un réseau, le client peut disposer de sphères chiffrées et non chiffrées
- Whaller assure un chiffrement de bout en bout réel : aucun secret n'est déporté en backend, les données sont chiffrées
- Les données sont indéchiffrables pour un administrateur système ou un attaquant qui aurait réussi à s'introduire sur les infrastructures
- Seuls les membres d'une sphère chiffrée peuvent déchiffrer ses contenus

Schéma fonctionnel simplifié



Secrets : le cœur du chiffrement de bout en bout

Définition : Les secrets sont des clés symétriques utilisées pour chiffrer et déchiffrer les messages ainsi que les fichiers échangés au sein d'une ou plusieurs sphères Whaller.

Génération du secret de sphère :

Une clé symétrique AES-256 est générée de manière aléatoire sur l'appareil du premier membre de la sphère (l'utilisateur qui a créé la sphère) à l'aide d'un générateur de nombres aléatoires cryptographiquement sécurisés. Algorithme : AES (Advanced Encryption Standard) avec une longueur de clé de 256 bits.

Stockage sécurisé :

Dérivation de clé (PBKDF2) : Le secret est chiffré avec une clé dérivée d'un code PIN défini par chaque utilisateur, pour chaque sphère.

Transfert pair à pair :

Pour partager le secret d'une sphère avec d'autres membres de cette sphère, Whaller utilise des clés asymétriques éphémères : RSA-OAEP (4096 bits).

👉 En savoir plus sur les mécanismes et algorithmes cryptographiques utilisés.

Transfert pair à pair (« cérémonie ») : une sécurité renforcée

Qu’est ce que c’est ?

- **Transfert sécurisé du « *Secret* » :** le Secret (clé de chiffrement des données) est échangé directement de manière pair à pair, c’est-à-dire de navigateur à navigateur, entre les utilisateurs du même réseau Whaller. Ce processus élimine tout intermédiaire, réduisant considérablement les risques d’interception ou de compromission des données.
- **Clés publiques/privées :** le transfert pair à pair s’effectue de façon chiffrée grâce à la création temporaire d’une paire de cela publique/privée qui est effacée une fois la transaction effectuée.
- **Stockage sécurisé :** Le Secret ainsi que les clés ne sont jamais stockées sur un serveur, mais exclusivement en local sur l’appareil de l’utilisateur, garantissant ainsi une confidentialité maximale.

Génération, sauvegarde et hydratation du secret.

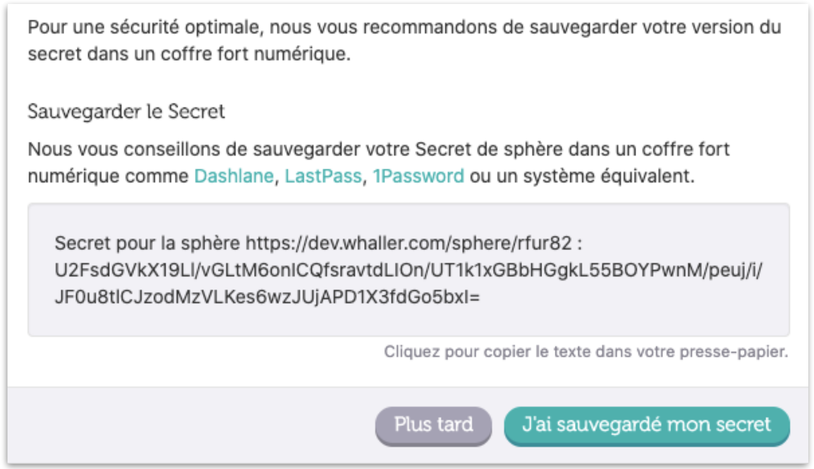
Un secret est généré soit par sphère, soit pour toutes les sphères chiffrées d'une organisation.

Ce secret est généré lors de la première activation d'une sphère chiffrée par qui que ce soit.

Ce secret doit absolument être sauvegardé par l'utilisateur (le client) dans un endroit sûr (chiffré et protégé par un mot de passe) et répliqué.

Le secret est ensuite transmis à l'ensemble des utilisateurs de pair à pair. Pour cela, il faut que lors d'une première connexion à une sphère chiffrée, un autre utilisateur soit connecté en même temps.

Les utilisateurs peuvent avoir connaissance du secret, et le sauvegarder.



Périmètre de chiffrement et limitations

Données protégées par le chiffrement de bout en bout :

- **Messages et commentaires : t**ous les textes saisis par les utilisateurs au sein des sphères sont chiffrés.
- **Fichiers partagés : l**es pièces jointes aux messages et commentaires sont chiffrés.
- **Box de fichiers :** tous fichiers stockés dans la box de fichiers sont chiffrés.

Limitations techniques à prendre en compte :

Le chiffrement de bout en bout offre une sécurité maximale pour vos données critiques, mais il implique certaines restrictions fonctionnelles.

1. **Recherche dans le contenu :** Les messages et les documents ne peuvent pas être recherchés par leur contenu en raison du chiffrement, seule la recherche par nom de fichier reste disponible.
2. **Visualisation et co-édition de documents :** Les documents ne peuvent plus être transmis à OnlyOffice via les serveurs pour une édition collaborative.
3. **Visioconférence :** La solution actuelle (BigBlueButton) propose un chiffrement en transit, mais pas de chiffrement de bout en bout. Cependant les visioconférences ne sont pas stockées une fois terminées.

Merci !

Whaller - contact@whaller.com