Whitepaper

1. Concept Métier

Locksy est un gestionnaire de mots de passe moderne et ultra-sécurisé. Il permet aux utilisateurs de stocker et gérer leurs identifiants, notes et cartes bancaires dans un coffre chiffré, accessible uniquement par eux. Le serveur n'a jamais connaissance des clés de chiffrement, garantissant une confidentialité totale.

2. Donnée Critique

La donnée critique que nous protégeons est l'ensemble des mots de passe des comptes utilisateurs. À cela s'ajoutent des informations sensibles comme les cartes bancaires, les notes sécurisées ou encore les documents. Ces données sont considérées comme hautement confidentielles et doivent rester inaccessibles à toute personne autre que l'utilisateur.

Failles possibles : Pour la protection contre le bruteforce il faut être vigilant sur le calibrage d'Argon d'autant qu'un attaquant pourrait lancer un bruteforce hors ligne.

3. Schéma de Chiffrement

Inscription :

- L'utilisateur saisit son mot de passe maître.
- Un salt aléatoire unique est généré côté client.
- Le mot de passe + salt passent dans Argon2id (fonction de dérivation de clé mémoire dur).
- Cela produit une clé locale.
- Le serveur stocke uniquement : email, salt, et le hash Argon2id du mot de passe.
- La clé locale n'est jamais transmise au serveur.

Connexion :

- Le serveur renvoie le salt associé à l'utilisateur.
- Le client régénère la clé locale avec Argon2id (mot de passe + salt).
- Cette clé locale sert à déchiffrer les données chiffrées reçues du serveur.
- Le serveur ne fait que vérifier le hash pour authentifier l'utilisateur, sans jamais voir la clé ni les données en clair.

Chiffrement des données sensibles :

- La clé locale dérivée est utilisée pour générer une clé maître.
- Cette clé maître chiffre toutes les données sensibles avec AES-GCM côté client.

- Le serveur ne stocke que des blobs chiffrés (BYTEA), jamais les données en clair.

4. Preuve Zero-Knowledge

- La clé locale est toujours calculée côté client et n'est jamais envoyée au serveur.
- Le serveur ne stocke que des hashs et des blobs chiffrés.
- Même en cas de compromission du serveur, les données restent inexploitables sans le mot de passe maître de l'utilisateur.

5. Le Schéma de Chiffrement