

Gankpo Security Architecture

1. Modèle de Signature Ed25519

L'épine dorsale de la plateforme repose sur la cryptographie asymétrique elliptique **Ed25519** (Edwards-curve Digital Signature Algorithm).

- **Avantages** : Très haute vitesse de signature et vérification (idéal pour le Edge Computing / Offline Verify), résistante aux attaques par canaux auxiliaires et à la falsification.
- **Vault/Wallet** : Les clés privées ne sont jamais exposées en clair sur le disque ; elles résident dans un *Software Vault* chiffré localement avec mot de passe selon un dérivé HKDF et AES-GCM (Zeroization après usage en RAM).

2. Le Hachage Cryptographique (Blake3)

Pour sceller le payload (le contenu visible des documents : PDF, images), Gankpo abandonne le SHA256 classique au profit de **Blake3**.

- **Avantages** : Extrêmement rapide sur de grands volumes de données tout en offrant un niveau de résistance aux collisions très largement supérieur à SHA-2. Il permet une validation instantanée même sur de très lourds GKP d'archives.

3. Conformité : Tamper Detection (Détection d'Altérations)

La modification unitaire d'un seul octet au sein d'un GKP (.gkp ou contenu protégé) est immédiatement sanctionnée :

- Les signatures vérifient la structure interne du `1_manifest` et du `metadata` .
- Les contrôles sur `fileKind` interdisent la dé-escalade d'une copie `PublicShare` pour qu'elle reprenne les attributs du statut d' `Original` .

4. Policy Enforcement (Application stricte des politiques)

La gouvernance s'applique dans un mode "Contract Strict" :

- **Prévention Anti-Spam de signatures** : L'approche modélisée ("Ordered" et "Threshold") rejette tout Sceau de la chaîne de possession si celui-ci ne correspond pas aux étapes de policy pré-calculées par le Trust Engine.
- **Isolation** : Les processus d'intégration du frontend (Tauri Invoke) ne peuvent exécuter le déverrouillage qu'en échange de la fourniture des clés et de tokens de sessions vivants (`runWithIdentityUnlock`), bloquant le phishing interne des mots de passe.