

Offline Verification Architecture

1. Concept de Vérification Isolée ("Air-Gapped")

L'architecture de l'écosystème Gankpo repousse les limites de la confiance numérique en permettant la validation complète de l'authenticité d'un document GKP sans aucun appel réseau vers des serveurs distants.

2. Métadonnées Auto-portées (Self-Containment)

Dès l'origine (« Original »), l'ensemble du matériel cryptographique nécessaire à la vérification est placé dans le conteneur GKP :

- Les clés publiques des signataires (`Ed25519` ou certificats `X.509`).
- La charge utile complète (`payload`).
- Les structures `metadata.json` incluant les rôles, numéros et horodatages.
- Les enregistrements (Records) de type `Traitling Signatures` rattachés récursivement.

Il n'est donc pas nécessaire de consulter un annuaire de confiance pour **prouver les mathématiques** d'une signature.

3. Protocole Hachage et Validation Cryptographique

1. **Extraction** : Le lecteur (Gankpo Reader / Suite) désarchive le paquet de surface.
2. **Comparaison de l'Empreinte (Hashes)** : Le payload cible (PDF, CSV, etc.) produit une nouvelle empreinte via `Blake3`. Elle doit être strictement identique au `hash_hex` consigné dans le metabloc GKP.
3. **Vérité de la Signature** : Chaque signature contenue dans `signatures/` est soumise à la comparaison Ed25519 / RSA (par module PKI local) avec l'empreinte Blake3 de la version scellée du document et la clé publique stockée.
4. **Vérification de la Chaîne (Chaining)** : Si des signatures en cascade existent (Parapheurs), le vérificateur recalculera le `prev_record_hash` sur les entêtes pour s'assurer qu'aucune validation ne fut re-séquencée.

4. Exceptions Nécessitant Connectivité

Bien que le modèle "Offline" fournisse la garantie à 99% d'absence d'altération du fichier, quelques vérifications de registre public requièrent du réseau :

- Le contrôle de **révocation** en direct (Vérifier qu'un `ProtectedShare` ou que le GKP original n'a pas été abrogé par le créateur).
- L'interrogation des listes de certificats révoqués (CRLs/OCSP) pour les Sceaux institutionnels.