Gankpo Trust Engine Architecture

1. Introduction

Le **Gankpo Trust Engine** est le pilier d'évaluation transactionnelle qui garantit la fiabilité, l'authenticité, et la conformité d'un document circulant sur la plateforme (Suite, Reader, Field). Plutôt qu'une simple vérification mathématique, il assure une modélisation dynamique du contexte transactionnel d'un GKP.

2. ChainOfCustody (Chaîne de Possession)

Le registre *ChainOfCustody* capture la généalogie exacte d'un conteneur GKP de sa création jusqu'à sa destruction/révocation.

1. **Événements horodatés & Signés :** Toute opération inter-organisationnelle (`Creation` , `Signature` , `Revocation` , `Submission`) n'est pas simplement journalisée en base de données, mais elle est attachée sous forme cryptographique à l'arbre interne du GKP.
2. **Pointeurs Hachés (PrevHash) :** Afin de garantir l'absence de falsifications rétroactives, l'événement N concatène l'empreinte de l'événement N-1 dans sa charge utile. La falsification ou la suppression de la "racine de confiance" invalide la chaîne.

3. TrustGraph (Graphe de Confiance)

Le Trust Engine projette chaque signature validée dans un *TrustGraph*, modélisant l'autorité (PKI ou locale) des signataires.

- Les identités individuelles (`Ed25519`) sont croisées avec les bases de "Binding V3" (Actor + Role + PKI Fingerprint).
- Lorsqu'une identité externe issue d'une fédération ajoute un sceau (Sceau Professionnel / Organisme), le TrustGraph injecte ses certificats (Chaîne de Confiance X.509) afin de légitimer les étapes de workflows.
- Si le certificat est compromis (CRLs / OCSP checks), le nœud du graphe devient "Répudié".

4. TrustScore (Score de Confiance)

Lors de la vérification (hors-ligne ou hybride), le moteur attribue un *Trust Score* (0 à 100) à l'interaction :

- **100 - Institutionnel Absolu :** Signature reconnue via une racine PKI certifiée (X.509 RSA/ECDSA), avec un Binding Acteur correct (Rôles institutionnels approuvés).
- **80-99 - Gankpo Vérifié :** Signataire présent dans l'annuaire unifié de Gankpo avec une clé `Ed25519` fiable.
- **50-79 - Gankpo Limité :** Signataire Gankpo vérifié mais contexte incertain (par exemple, alerte sur le TrustGraph de son entité).
- **0 - Invalide / Altéré :** Toute rupture mathématique (Blake3), perte de signature, ou répudiation explicite du document.

Ce calcul dynamique offre aux UI (e.g. Gankpo Reader) la possibilité d'afficher en temps réel le "niveau" d'assurance au citoyen ou à l'institution inspectrice.