PKI Authority Integration

1. Description Technique

Le domaine **PKI Authority Integration** du moteur Gankpo gère la connexion fluide entre le système asynchrone hors-ligne de signature cryptographique native (Ed25519) et les écosystèmes hiérarchiques de la **PKI Institutionnelle (X.509)**, souvent pilotée par Active Directory, OpenLDAP ou Keycloak.

La passerelle Gankpo assure une **vérification croisée** stricte des certificats. Lorsqu'un fichier GKP est présenté à un utilisateur possédant un certificat institutionnel, Gankpo intègre par conception le concept de **"Resolution Logic"** (Binding V3) liant le rôle déclaré du signataire à l'authenticité vérifiable d'un Anchor certifié de l'Organisation.

2. Intégration de l'Identité du Signataire (Resolution Logic)

Lors de la signature ou de la lecture d'un acte officiel, Gankpo applique une validation triangulaire pour s'assurer que le porteur d'une clé privée est bien *habilité* institutionnellement.

Cette implémentation exploite le `SignerIdentity Envelope (SIE)` :

- **Gankpo Profile Data** : `displayName`, `email`, `role`, `organizationName`.
- **PKI Certificate Data** : `subject_name`, `serial_number`, `fingerprint` issue d'un magasin local (Keychain macOS ou Windows CNG) ou distant.
- **Resolution Engine (`gkp_core`)** : Lance une fonction de scoring (`consistency_status`) :
  - `Match` complet (ADN Certificat == Profil Gankpo).
  - `Partial` (Nom ou rôle validé sur la chaîne X.509 locale sans lien direct externe).
  - `Mismatch` ou `Unknown` (Interdiction catégorique du workflow de signature Ordered institutionnel).

```
sequenceDiagram
    participant User as Signataire Gankpo
    participant Reader as Gankpo Suite / Reader
    participant PKI as Système PKI (OS/HSM)
    participant Core as Trust Engine

    User->>Reader: Lance la demande de signature (GKP)
    Reader->>Core: Décode le Manifest (Allowlist GKP)
    Core->>Reader: Retourne Identité Requise (ex: "Directeur")
    Reader->>PKI: Demande le Certificat (X.509 ou Ed25519 Local)
    PKI-->>Reader: Certificat
    Reader->>Core: Validation de Correspondance (Binding V3)
    Core-->>Reader: Scellement OK (Conforme)
```

3. Trust Registries et Federation

L'intégration PKI Gankpo va plus loin en adoptant le modèle décentralisé :

- **Federation Layer** : Les autorités gouvernementales et institutionnelles publient une `PKI / Trust Anchor` (clé asymétrique de registre central) intégrée par Gankpo dès la phase d'Onboarding.
- Tout document "Scellé" (`action_type == "seal"`) avec une clé inconnue du Trust Register local ne bénéficiera jamais du label `Vérifié d'État` .

4. Composants Architecturaux de Sécurité X.509

- **Extraction X.509 (`x509_parser`)** : Validation pure d'ASN.1 / DER pour sécuriser le traitement (`no_panic`).
- **Vérification de Trust Store** :
  - Le `gkp_core` interroge dynamiquement le magasin système :
  - **macOS (`security-framework`)**
  - **Windows (`schannel` via `rustls-native-certs`)**
  - **Linux (`openssl` local root)**
- Le rejet cryptographique est **absolu**. Un certificat révoqué côté Windows cassera l'intégrité de l'enclave Gankpo locale lors de la signature.

5. Exemples d'Injection dans le GKP

Une signature validée par la passerelle PKI injecte dans le Ledger (`records`) un `identity_envelope` et un bloc ASN.1 :

```
{
  "records": [
    {
      "signer_id": "fpr:D8E2B2A2...",
      "signature_hex": "b3ad3f3...",
      "action_type": "sign",
      "pki_cert_der": "MIIB...",
      "identity_envelope": {
        "resolved_name": "Prefecture de Zio",
        "consistency": "match"
      }
    }
  ]
}
```

Ce modèle fusionne la souplesse de GKP (P2P et Asynchrone) avec la rigidité juridique de X.509.