

# Secure Exchange Engine Specification

## 1. Définition et Objectifs

Le **Secure Exchange Engine** orchestre la protection cryptographique et la gouvernance d'accès des documents GKP (en particulier pour la création et la consommation de `ProtectedShare` et pour les requêtes de signatures à distance).

## 2. Politiques Modulables (Policies)

L'Engine repose sur l'attachement d'un `policy.json` cryptographiquement inviolable.

### 2.1. `secure_exchange_policy`

Applicable aux configurations de partages :

- Contrôle strict via **mots de passe / indices de déchiffrement** avec clés dérivées HKDF (Version 4).
- Limite d'accès temporelle par paramètre `expires_at_iso`.
- Paramétrage de visibilité ciblée aux seuls destinataires disposant des mots de passe.

### 2.2. `signature_request_policy`

Dédiée au circuit de validation asynchrone (Multisignature) :

- Indique si la policy est de type `Threshold` (N signataires sur M requis) ou `Ordered` (circuit de rôles : e.g. Rédacteur -> Manager -> Seal Institutionnel).
- Bloque dynamiquement toute tentative d'approbation si le rôle de l'identité qui déverrouille le vault ne correspond pas à l'étape attendue (ex: "Sceau (Seal) ajouté trop tôt" est automatiquement bloqué).

### 2.3. Gestion des `access_counter`

L'outil "Gankpo Tracking" trace activement pour l'auteur de la politique :

- Le nombre total d'ouvertures ou d'interactions réussies.
- Si le nombre dépasse le paramètre optionnel `max_accesses`, le Share peut se refermer ou se bloquer via appel API (sur les portails de type Viewer).

## 3. Comportements Répressifs

Le moteur applique des restrictions directes :

- **Expiration de Copies** : Un GKP exporté en `PublicShare` ou `ProtectedShare` peut être déclaré obsolète en local si sa date système franchit le champ `expires_at_iso`.
- **Verrouillage sur Altérations** : Si le client détecte que le manifeste n'est pas cohérent avec le GKP crypté, le document est frappé d'une violation grave et les clés dérivées refusent le déchiffrement, garantissant qu'aucun document altéré ne peut être "sauvé".
- **Limitations de copie** : Un `Share` ne peut plus jamais redevenir un `Original`, rendant impossible (technologiquement) la retransmission infinie de copie de copie, forçant l'usage de la source unique.