GKP Developer Guide

Pour les intégrateurs systèmes, ESN ou services publics souhaitant traiter, signer, ou valider programmatiquement un conteneur GKP, ce guide détaille l'accès bas niveau au format.

1. Comment lire un conteneur GKP (.gkp)

Un fichier `.gkp` est structurellement un ZIP standard.

- De-zippez l'archive par n'importe quelle librairie (exemple : `unzip -q document.gkp`).
- Examinez le dossier `./payload`. Vous possédez le fichier source du document en forme non chiffrée (s'il s'agit d'un GKP non protégé) ou chiffré avec AES en cas de `ProtectedShare`.

2. Comment vérifier la signature cryptographique

1. **Calculez le Hash du Payload :** Avec l'algorithme `BLAKE3`, produisez un hex string de `/payload/*`.
2. **Obtenez le PublicKey :** Ouvrez `metadata.json` -> `issuer.public_key`.
3. **Parsez le Sign-Bloc :** Accédez au répertoire `/signatures/primary.sig` (ou via CBOR pour `version == V4`).
4. **Validité Mathématique :** Alimentez le hachage BLAKE3 et le Primary.sig dans votre implémentation standard de vérification *Ed25519*. **Si isValid == True**, alors le document n'a subi aucune modification.

3. Interpréter les Métadonnées GKP (Manifest & Metadata)

- **`kind` :** Inspectez toujours si le Fichier est "Original", "PublicShare" ou "ProtectedShare". Rejetez l'opération si un utilisateur tente de signer un "Share", ce privilège est réservé à l'"Original".
- **`gkp_number` :** Correspond au tracking de l'entité gouvernementale (Format : `GKP-1-<pubkey_slice>-YYYYMM-NNNN`).
- **Documents Multisignes :** Si `signatures/` contient `append_0.sig`, `append_1.sig`, analysez le payload du CBOR (Trail records). Vérifiez dans les métadonnées de chacun l'attribut `RecordType`. Les Types `Countersignature` sont les ajouts humains, les `Seal` sont formellement des sceaux automatiques (PKI ou CA Server).

4. Résolution d'erreur fréquente : Sceau Professionnel & PKI

Lorsqu'il figure un `pki_certificate` en base64 dans le sous-bloc ou une annotation `remote:uid`, remplacez l'instance Ed25519 standard par un module de validation X.509 pour vous brancher sur l'OCSP gouvernemental ou privé afin de valider le Certificat.