POC OpenXPKI

Cette page présente brièvemet une configuration d'esup-signature permetant l'utilisation d'un serveur OpenXPKI dans le but de demander des certificats à la volé au nom du signataire au moment de la signature des documents.

Installation d'OpenXPKI

L'installation à été réalisée sur le configuration suivante :

OS: Debian GNU/Linux 10 (buster) (x86-64)

Kernel: 5.10.0-10-amd64

Il faut tout d'abord suivre la documentation officiel d'OpenXPKI :

https://openxpki.readthedocs.io/en/stable/quickstart.html

Puis suivre les instructions suivantes :

- Changer le password du compte rob ici : /etc/openxpki/config.d/realm.tpl/auth/handler.yaml

- Supprimer du fichier /etc/openxpki/config.d/realm/democa/crypto.yaml les lignes suivante

```
# ratoken:
# label: Secret group for RA Token
# export: 1
# method: literal
# if you change this, you need to adapt the ratoken_update workflow!
# value@: credentials.token
```

- Décommenter dans la configuration apache (générée suite à l'installation d'OpenXPKI) les lignes suivante :

```
ScriptAlias /rpc  /usr/lib/cgi-bin/rpc.fcgi

https://<IP>/rpc/enroll
```

- Configurer un workflow de demande de certificat qui valide toutes les demandes sans contrôle humain. Fichier /etc/openxpki/config.d/realm /democa/workflow/def/certificate_enroll.yaml est à remplacer par le fichier suivant :

- De manière facultative, il est possible de régler la duré de validité des certificats (typiquement 24 heures) ici :

/etc/openxpki/config.d/realm/democa/enroll.yaml

- Et enfin il faut ajouter l'adresse de votre serveur OpenXPKI dans la configuration d'esup-signature (application.yml) :

```
open-x-p-k-i-server-url: http://10.0.131.23/rpc/enroll
```

⚠ Tous les utilisateurs auront la possibilité de signer à l'aide ces certificats auto générés