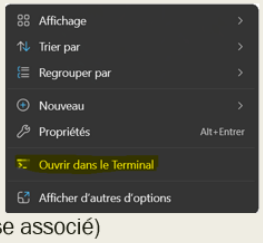
# Extraction de la clé publique du Certificat d'authentification logiciel Entité

Ce modop est utilisable a priori pour tous les types de certificats répondant aux exigences du FNC-RF, quelle que soit l'Autorité de Certification qui l'a produit.

Il faut extraire la clé publique (certificat **.CER en base64**) du fichier .P12 (en utilisant le mot de passe associé).

Un exemple ci-dessous pour extraire le .CER en base64 :

- A partir du dossier où est copié le fichier .p12, cliquer sur le menu contextuel (via clic droit) « **Ouvrir dans le Terminal** » :




- **Etape n°1** : import du fichier **.pem** (sans la clé privée) à partir du fichier **.p12** (et mot de passe associé)
  - Entrer la ligne de commande « **openssl pkcs12 -in certificat.p12 -clcerts -nokeys -out certificat.pem** »

| *Option* | *Signification* |
|---|---|
| -in certificat.p12 | Fichier d'entrée au format PKCS#12 |
| -clcerts | Ne garder que le certificat de l'entité (exclut les certificats CA) |
| -nokeys | Ne pas extraire la clé privée |
| -out cert.pem | fichier PEM contenant le certificat |

  - Entrer le mot de passe associé au certificat « certificat.p12 »

```
Enter Import Password:
```

**Etape n°2** : import du fichier **.cer** à partir du fichier **.pem** (sans la clé privée) importée à l'étape précédente

- Entrer la ligne de commande « **openssl x509 -in certificat.pem -outform PEM -out certificat.cer** »

| *Option* | *Signification* |
|---|---|
| x509 | Indique que l'on travaille avec un certificat X.509 |
| -in certificat.pem | Spécifie le fichier d'entrée contenant le certificat au format PEM créé à l'étape précédente |
| -outform PEM | Définit le format de sortie en PEM (Base64) * |
| -out certificat.cer | Spécifie le fichier de sortie pour le certificat converti. |

*** Import du fichier .cer (encodé en Base64) effectué ! ***

À noter que, lors de la configuration de **votre serveur de synchronisation sur votre MISP local de Production**, c'est le **.PEM** (**clé publique + clé privée**) que vous devez charger en tant que certificat client (**Client certificate file) :**

Note : pour exporter la clé privée en PEM (décryptée) à partir du fichier.p12 (et mot de passe associé), entrer la ligne de commande suivante : **openssl pkcs12 -in fichier.p12 -nocerts -nodes -out key.pem**