KORUM SECURE
korum-secure.com

Guide OpenSC PKCS#11 & PKCS#15

Ce guide est pour OpensSC, et montre comment utiliser les clés Epass2003 ou les cartes à puces A22CR et A40CR

La gamme ePass2003 de jetons PKI ainsi que ces deux modèles de cartes à puce peuvent être utilisées avec les utilitaires et bibliothèques OpenSC PKCS#11 et PKCS#15.

Initialisation de ePass2003 et/ou cartes à puce avec OpenSC.

Étapes

1. Effacez toute structure PKCS#15 existante sur le jeton :

   ```
   pkcs15-init -E
   ```

2. Créez la nouvelle structure PKCS#15 sur le jeton :

   ```
   pkcs15-init --create-pkcs15 --profile
   pkcs15+onepin --use-default-transport-key --pin 12345678 --puk
   entersafe
   ```

   Le code PIN et le code PUK peuvent être modifiés à vos valeurs préférées à cette étape.

3. Voilà ! Vous pouvez maintenant utiliser le jeton avec OpenSC.

Créer une paire de clés sur des jetons ePass2003 et cartes à puce à l'aide d'OpenSC

Vous devez initialiser le jeton/la carte à l'aide de la commande pkcs15-init avant de pouvoir créer des paires de clés. L'initialisation est abordée ci-dessus.

Étapes

1. Pour créer une paire de clés RSA sur le jeton, vous devez exécuter la commande suivante :

```
pkcs15-init --generate-key rsa/2048 --id 010203 --key-usage
sign,decrypt --auth-id 01 --label "MyKey"
```

Cela crée une clé avec l'ID « 010203 », mais vous pouvez le remplacer par un autre ID hexadécimal de votre choix.

2. Vous pouvez extraire la clé publique au format PEM à l'aide de la commande suivante :

```
pkcs15-tool --read-public-key 010203 > 010203-public.pem
```

3. C'est tout ! Vous pouvez désormais utiliser le jeton pour effectuer des opérations de chiffrement intégrées.

Chiffrement/déchiffrement avec les jetons ePass2003 à l'aide d'OpenSC

Vous devez initialiser le jeton/la carte et créer les clés de chiffrement avant de suivre les étapes de ce guide. Il vaudra donc réaliser les deux procédures précédentes avant de pouvoir commencer cette dernière

Étapes

1. En supposant que vous ayez exporté la clé publique dans le fichier ***010203-public.pem*** du guide précédent, vous pouvez chiffrer les données à l'aide de n'importe quel outil qui accepte une clé publique codée en PEM. Ici, nous utiliserons la boîte à outils OpenSSL comme exemple.
2. Ici, nous allons crypter un fichier à l'aide de l'outil **openssl rsautl** (***remplacez-INPUT_FILENAME*** par un fichier de votre choix) :

```
openssl rsautl -in INPUT_FILENAME -encrypt -pkcs -pubin -inkey
010203-public.pem -out encrypted.bin
```

Vous aurez maintenant vos données cryptées dans le fichier ***encrypted.bin*** lequel nous pourrons déchiffrer à l'aide de la clé privée intégrée au jeton
(remplacez ***OUTPUT_FILENAME*** par un nom de fichier de votre choix) :

```
pkcs15-crypt --decipher --key 010203 --pkcs1 --raw --input
encrypted.bin > OUTPUT_FILENAME
```

3. C'est terminé ! Vos données déchiffrées contenues seront dans ***OUTPUT_FILENAME***.

Cordialement,**SUPPORT :**

Si vous avez besoin d'assistance pour l'utilisation de nos produits, n'hésitez pas à nous contacter au contact@korum-secure.fr