pkcs15-init

Utilitaire de personnalisation de carte à puce

Il permet de créer des structures PKCS #15 sur les cartes à puce, créer des PIN et ajouter des clés et des certificats. Les détails de la structure est contrôlée par des profils.

Utilisation du PIN

Une carte OpenSC peut avoir un security officer PIN, et 0 ou plusieurs PIN utilisateurs. Généralement, un PIN est une séquence de chiffres, mais certaines cartes acceptent des caractères ascii. Le SO-PIN est spécial, il est utilisé pour protéger les métadonnées sur la carte, tel que la structure PKCS #15 elle-même. Le SO-PIN est optionnel. Pour chaque PIN, vous pouvez spécifier un PUK.

Modes opératoires

Initialisation

Première étape de la personnalisation de la carte, et va créer les fichiers de bases sur la carte. Pour créer une structure PKCS #15 (le PIN, le PUK et le SO-PIN sont demandés) :
pkcs15-init –create-pkcs15
Si la carte le supporte, vous pouvez également l'effacer avant avec –erase

Installation du PIN de l'utilisateur

Avant d'installer des objets, vous avez besoin d'au moins un PIN pour protéger ces objets (demande le PIN et le PUK) :
pkcs15-init –store-pin –id " nn
Où nn est un ID PKCS #15 en notation hexadécimal. Les valeurs communes sont 01, 02, etc.

Génération de clé

Pour générer une nouvelle clé et la stocker :
pkcs15-init –generate-key " keyspec " –auth-id " nn
Où keyspec décrit l'algorithme et la longueur de la clé à créer, tel que rsa/512. Actuellement seul RSA est supporté. nn est l'ID d'un PIN utilisateur
Cela va stocker la portion privée et publique de la clé. Par défaut, tente d'utiliser la fonctionnalité embarquée de la carte.

Télécharger la clé privée

Vous pouvez utiliser une clé par un autre moyen et la charger dans la carte. Doit être au format PEM, DER, et les certificats pkcs12 et pfx :
pkcs15-init –store-private-key key.pem –id 45 –auth-id 01

L'option –id sert pour définir 2 templates de clé. l'id 45 sert pour l'authentification et l'id 46 pour la non-répudiation.

Télécharger la clé publique

–store-public-key stocke la clé publique. Utiliser –format pour spécifier le format du fichier (PEM par défaut)

Télécharger un certificat

–store-certificat stocke le certificat. Le fichier est supposé être un fichier x.509 au format DER

Télécharger les fichiers pkcs#12

pkcs15-init –store-private-key key.p12 –format pkcs12 –auth-id 01

OPTIONS

–profil, -p Charge le profile général spécifié. Des options peuvent être spécifiées pour ce module en ajoutant un + entre chaque option. ex : pkcs15+onepin

–card-profile, -c Charge l'option de profile de carte spécifié.

–create-pkcs15, -C Crée un structure PKCS #15 sur la carte

–erase-card, -E Efface la carte avant de créer la structure PKCS #15

–generate-key, -G Dit à la carte de générer une nouvelle clé et de la stocker sur la carte, avec l'algorithme/longueur spécifiée

–store-private-key, -S Télécharge la clé privée sur la carte. Crée également un objet clé publique

–store-public-key, -P Télécharge la clé publique sur le certificat

–store-certificate, -X Stocke le certificat sur la carte

–so-pin, –so-puk, –pin, –puk Permet de spécifier les valeurs pour les opérations qui le nécessite

–passphrase Permet de spécifier la passphrase pour débloquer la clé privée

–verbose, -v mode verbeux

–options-file Lit les options additionnelles depuis le fichier spécifié. Ce fichier est supposé contenir une option longue par ligne. (Peut être spécifié plusieurs fois). ex :

pin frank
puk zappa