pam_pkcs11

Module PAM d'authentification via une librairie PKCS #11

Module PAM pour faire de l'authentification au moyen d'un certificat X509 au travers d'une librairie PKCS #11. Pour la vérification des certificats utilisateurs, le certificat de l'autorité stocké localement et la CRL en ligne ou locale sont utilisés. Les modules PKCS #11 doivent remplir les prérequis de RSA Asymmetric Client Signing Profil. Pour permettre au propriétaire d'un certificat de se connecter, pam_pkcs11 utilise des modules appelés des mappers, qui effectuent des mappages cert-to-login.

Configurer le package

1. créer le répertoire de base /etc/pam_pkcs11/
2. Copier ${base}/etc/pam_pkcs11.conf.example dans /etc/pam_pkcs11/ et le renommer en /etc/pam_pkcs11/pam-pkcs11.conf
3. créer /etc/pam_pkcs11/crls/ et /etc/pam_pkcs11/cacerts/. Le répertoire tools/ fournis un outil pkcs11_make_hask_link qui peut être utilisé pour créer les fichiers de hash pour chaque fichier certificat et crl valide.
4. Choisir un ou plusieurs mappers à installer, les configurer.
5. Éditer et configurer /etc/pam.d/xxx
6. Utiliser pkcs11_inspect et pklogin_finder pour voir si vous pouvez lire le certificat et effectuer un mappage correct
7. tester un login.

Configurer pam_pkcs11

la configuration de pam-pkcs11 se fait en 2 étapes :

1. configurer pam-pkcs11
2. Configurer les options PAM.

Vous devez connaître

- quel module PKCS #11 vous allez utiliser, et son fichier
- quels mappers vous voulez et comment le créer et l'éditer
- Les fichiers de l'authorité de certification et le fichier de révocation
- Une liste d'utilisateurs autorisés à se connecter, et leur certificats correspondant.

Spécifier la CRL et la CA

pam-pkcs11 a besoin d'une liste d'authorité de certification reconnue pour valider l'utilisateur. Celà s'applique également à la CRL :

1. Créer les répertoire ca_dir et crl_dir en accord avec le fichier de configuration
2. Copier les certificats de la CA au format DER ou PEM

3. Créer un hash link vers les certificats CA, fournis avec pkcs11_make_hash_link. Noter que openSSL doit être installé :
   cd /etc/pam_pkcs11/cacerts
   /usr/bin/pkcs11_make_hash_link
4. Répéter la procédure pour la CRL
5. Sélectionner la stratégie de vérification de certificat (cert_policy)

NOTE : Du à des limitations de librairie OpenSSL, les certificats de la CA doivent résider dans le système de fichier local.

Un fichier de map a la syntaxe suivante :

Certificate1 data -> login1

Certificate2 data -> login2

Certificate3 data -> login3

Ce fichier est parsé du début àla fin et la première occurence qui match est retournée.

Configuration PAM

Configurer les fichiers pam.d

auth sufficient pam_pkcs11.so ...

OPTIONS

debug mode debug

err_display_time Secondes à attendre après un message d'erreur pour lire le message

config_file Spécifier le fichier de configuration (défaut : /etc/pam_pkcs11/pam_pkcs11.conf)

nullok Autorise les mots de passe vide

use_first_pass Ne demande pas le mot de passe à l'utilisateur, mais le prend depuis le PAM_items.

try_first_pass Ne demande pas le mot de passe à l'utilisateur à moins que PAM_(OLD)AUTHOK ne soit pas mis.

use_authok Comme try_first_pass mais échoue si le nouveau PAM_AUTHOK n'a pas été précédemment mis.

pkcs11_module=<file> Nom de fichier du module PKCS11 (défaut : /etc/pam_pkcs11/pkcs11_module.so)

slot_num=<nb> Numéro de slot à utiliser (défaut = 0 = utiliser le premier slot disponible)

ca_dir=<path> Répertoire contenant les certificats CA (défault : /etc/pam_pkcs11/cacerts/)

crl_dir=<path> Répertoire contenant la CRL (défault : /etc/pam_pkcs11/crls/)

cert_policy=none, ca, signature, crl_online, crl_offline, crl_auto Spécifier la stratégie de vérification par défaut.

Utiliser la fonction d'auto-détection de LOGIN

Depuis pam-pkcs11-0.4.2 pam-pkcs11 peut déduire le username depuis le certificat utilisateur sans utiliser le login prompt.

Quand pam_get_user() retourne null ou une chaîne vide, pam-pkcs11 va alors utiliser la fonction 'find' du mapper au lieu du match normal. Si le finder retourne un succès, le username est définit avec pam_set_item(PAM_USER) et PAM_AUTH_OK est retourné.

Il y'a 2 manières d'utiliser cette fonctionnalité :

a. Patcher gdm et login pour détecter la présence d'un carte et retourner null comme nom d'utilisateur

b. Utiliser une version non patchée et entrée un espace pour login et entrée pour gdm.