CRYPTOGRAPHIE
TP N°3

Objectif du TP : *Nous continuons les problèmes de chiffrement et de signatures "réels". Maintenant, les clefs publiques / privées devront être incluses dans des certificats dont le format est standard. Nous nous intéressons ici aux certificats #PKCS12 et X509 utilisés par ssl.*

ENONCE :

Lorsqu'on demande un certificat signée à une CA, celle ci vous fournit un fichier **PKCS#12** que vous pourrez utiliser dans vos logiciels : navigateur web, logiciel de messagerie, ... Les fichiers PKCS#12 auront pour extension **.p12**

La CA vous remettra également une pass phrase permettant de déchiffrer ce certificat (puisqu'il contient votre clef privée).

Le format PKCS#12 permet de rassembler:

- Paire de clé privée/publique
- Certificat X.509 de la clé publique de la paire
- Certificat X.509 signataire
- Chaine des certificats jusqu'au certificat ROOT (peut ne pas etre present).

Vous pouvez à partir de ce fichier récupérer le certificat public que vous allez distribuer. La plupart du temps, la CA vous fournira aussi ce certificat public, un certificat X509. Enfin, elle vous fournira son propre certificat public afin que vous puissiez le distribuer. Les certificats X509 ont pour extension **.cer**

Exercice 1 :
Créer une CA, ainsi que les certificats PKCS#12 et X509 pour Alice et Bob. Il vous faut en fait pour chaque personne : un certificat pour chiffrer à l'aide de RSA et un certificat pour signer avec DSA.

Pour cela, vous utiliserez l'utilitaire **CA.pl** qui se trouve quelque part sur vos machines. il y a une bonne manpage pour CA.pl, ce qui devrait vous permettre de faire tout cela.

Exercice 2 :
Utiliser le programme TestPKCS12 pour lire les certificats et vérifier que tout est bien en ordre.
- Utiliser le programme TestX509 pour lire les certificats x509 et vérifier que tout est bien en ordre.

Exercice 3 :
Modifiez les programmes du TP précédent (chiffrement et signature) pour que les clefs soient lues dans des certificats standards et pour que l'utilisateur se voit demander sa Pass Phrase quand il doit utiliser sa clef privée.
Notez qu'en fait, un message signé devrait contenir le message, la signature et le certificat X509 du signataire. Ceci existe sous le standard CMS/PKCS#7 mais ne sera pas fait en TP (pas eu le temps).