Université Paris Diderot
L3 informatique
Sécurité 2017-2018

TP Sécurité
Clef: point de vue utilisateur

1 Génération de clefs et de certificats

L'outil *keytool* permet de gérer les clefs et les certificats qui sont stockés dans un *keystore*.

Exercice 1.— Générer un fichier *keystore* contenant une paire de clefs DSA et une paire de clefs RSA (`keytool -genkeypair....`).

Exercice 2.— Visulaliser le contenu de votre keystore (utiliser l'option verbeuse (`-v`)).

Exercice 3.— A partir de votre keystore, exportez un certificat auto-signé contenant la clef publique DSA et un certificat auto-signé contenant la clef publique RSA.

2 Création d'une archive jar contenant une application

Exercice 4.— Ecrire une application java qui prend 2 arguments un fichier et 0 ou 1. Appelé avec l'argument 0 l'application écrit votre nom dans le fichier donné en premier argument. Appelé avec l'argument 1 l'application affiche le fichier donné en premier argument sur la sortie standard.

Exercice 5.— Créer une archive jar (`monjar.jar`) contenant le .class de l'application. Quel est le contenu du fichier MANIFEST.MF de votre archive?

Exercice 6.— Pouvez vous exécuter votre application sous la forme `java -jar monjar.jar fic 1`? Si non faites en sorte que cela le soit (modifiez le fichier MANIFEST.MF).

3 Signer et verifier une archive

Exercice 7.— En utilisant `jarsigner`, à partir de votre archive, créez deux archives signées: l'une utilisant la clef DSA de votre keystore et l'autre la clef RSA.

Que contiennent, dans chaque cas, le fichier MANIFEST.MF et le fichier signature (c'est le .SF) ?

Exercice 8.— Prenez une archive signée par un autre étudiant. Pouvez vous l'exécuter (java -jar ..)? Verifiez la validité de la signature (`jarsigner -verify -verbose -certs nom-du-jar-signe`)

Exercice 9.— Prenez les certificats de ce même étudiant et importez les dans votre keystore. Vérifiez à nouveau la validité. Quelle est la différence avec la vérification précédente?

4 Politique de sécurité

Exercice 10.— Que donnera l'exécution de l'archive signée si on a un security manager (`java -Djava.security.manager -jar rsamonjar.jar`)?

Exercice 11.— Installer avec *policytool* une politique de sécurité qui vous permettra d'utiliser votre application pour lire et écrire dans des fichiers et qui vous permettra d'utiliser l'application de l'autre étudiant seulement pour lire (et refusera l'écriture).