# TP relatif à PKI

Principe de fonctionnement de PKI

Quatre technologies définissant le concept de PKI :

1/ Confidentialité

2/ Intégrité

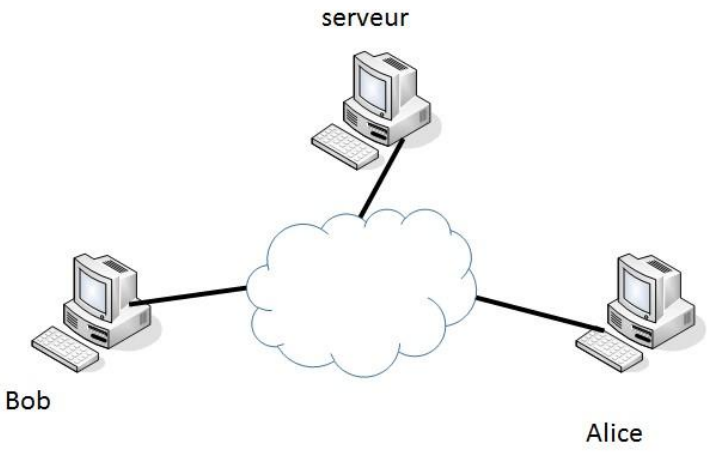
3/ Non-répudiation / signature numérique

4/ Authenticité

Ce TP permet dans un premier temps de mettre en évidence le fonctionnement de la confidentialité en utilisant le chiffre asymétrique (clé publique-privée).

Chaque correspondant génère au logiciel

Schéma réseau :




| Hostname | OS | IP | Masque | DNS |
|---|---|---|---|---|
| IIS | 2016 + AD | 192.168.1.3 | 255.255.255.0 | 192.168.1.3 |
| Pc1 | W7 | 192.168.1.1 | 255.255.255.0 | 192.168.1.3 |
| Pc2 | W7 | 192.168.1.2 | 255.255.255.0 | 192.168.1.3 |

I) Cloner les trois postes en full, configurer les IP et serveur DNS comme c'est indiqué sur le schéma réseau ci-dessus. Puis tester la connectivité entre les postes par ICMP.

II) Installer les services IIS (HTTP – ftp ) sur le poste serveur 2016. Tester le fonctionnement des deux services.

III) Sur le serveur (attention aux modifications)

- Créer deux comptes clients : Alice et Bob. (normalement il n'y a pas à faire)
- Créer deux dossiers c:\pki\public\bob et c:\pki\public\alice
- Créer deux dossiers c:\pki\prive\bob et c:\pki\prive\alice

- Tout le monde peut accéder aux répertoires c:\pki\public
- Seuls les propriétaires peuvent accéder leur propre répertoire.

IV) Télécharger le logiciel PGP4Win puis l'installer sur les postes Alice et Bob

- Générer un trousseau de clés publique-privée pour chacun entre eux
- Chacun dépose sa clé publique dans le répertoire publique correspondant
- Chacun chiffre un fichier avec la clé publique de l'autre, puis le déposer public de l'autre.

  c:\pki\public
- Chacun récupère le document chiffré, et déchiffre avec sa propre clé privée.

***V)*** Mettre le serveur DNS en place afin que l'accès au serveur ftp passe par l'url et non par l'IP, par exemple ***alice.uk*** et ***bob.fr***