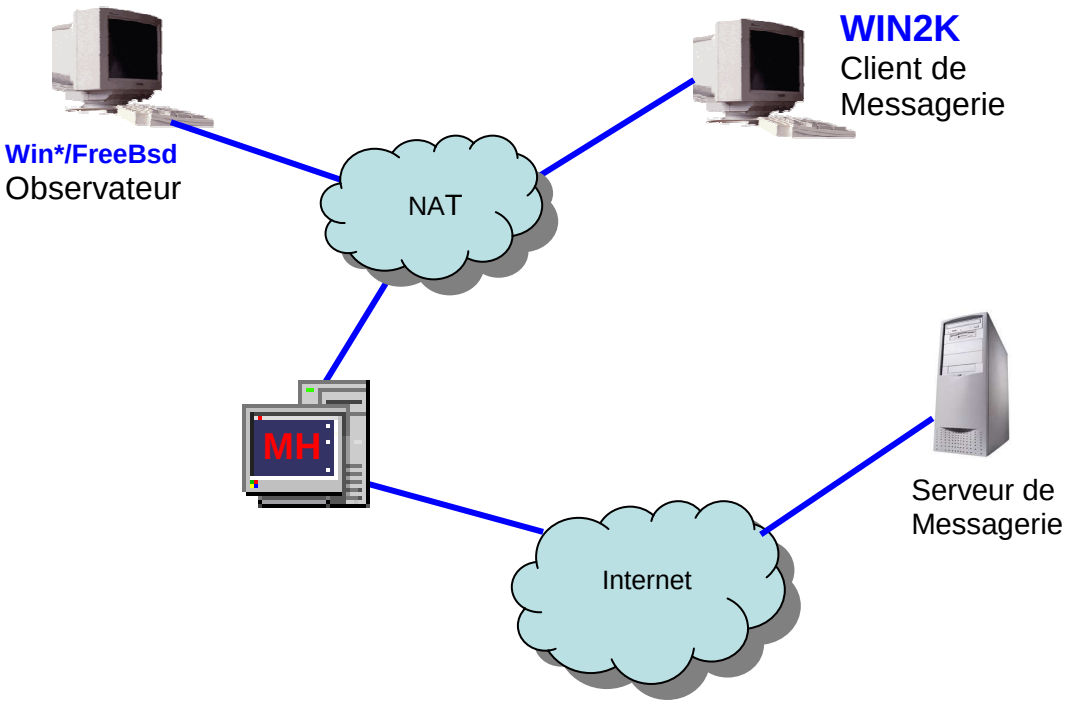
TP1 : La Messagerie Sécurisée

But du TP : Obtenir et utiliser un certificat lors d'échanges de messagerie sécurisée



L'objectif du TP est de mettre en oeuvre un échange sécurisé de messagerie, permettant d'une part l'authentification de l'émetteur et la vérification de l'intégrité d'un message, puis d'autre part la confidentialité de l'échange.

Etape A : Configuration du client de Messagerie

- Lancer la machine WIN2K
  - Configurer le client de Messagerie (Outlook Express installé déjà sur la MV ou Thunderbird à installer) pour interroger le serveur de messagerie de l'Université.
  - Protocole pop3, serveur entrant mailserver.u-strasbg.fr, serveur SMTP iutsud.u-strasbg.fr, compte <votre compte ENT>
  - **ATTENTION** : configurer les Propriétés Avancées « Conserver une copie sur le serveur » avant de relever votre courrier sous peine de supprimer tous les messages dans votre Boîte de réception sur le serveur.

Etape B : Obtention et installation du certificat

Contacter le serveur d'une Autorité de Certification et faire la demande d'un certificat personnel pour la messagerie électronique (provisoire et gratuit pour une durée de validité limitée).

- Vous donnerez comme identification votre adresse de messagerie @eturs.
- Suivre les indications et installer le certificat.

Vérifier et donner les caractéristiques du certificat. Est-il accessible sous IE/Firefox ? Est-il utilisable sous OutlookExpress/Thunderbird ? Comment est-il stocké et quelle est la sécurité du stockage ?

Etape C : Emission et réception d'un courrier signé

- Echanger des messages signés
- Que propose le client de messagerie ?
- Comment mémoriser le certificat de l'émetteur ?

Etape D : Observateur réseau

- Installer et configuer une MV *Observateur* , y installer une sonde (*tcpdump* ou *wireshark*). Montrer qu'il est possible de capturer le trafic issu de votre client de messagerie et de plus de reconstituer tout le flux (login, mot de passe, contenu des messages…)
- Vérifier le contenu d'un message signé : format MIME, contenu, signature

Etape E : Emission et réception d'un courrier crypté

- Que faut-il obtenir au préalable pour envoyer une courrier crypté ?
- Vérifier le contenu d'un message crypté, capturé par l'observateur
- Envoyer un courrier crypté et signé…

Etape F : Exportation du certificat

- Exporter le certificat
- Quels sont les formats proposés ? Comment pouvez vous l'installer sur un autre poste ?

Dossier à rendre :

Vous rédigerez étape par étape un dossier dans lequel vous consignerez les résultats obtenus à chaque étape, (copies d'écran, trames, schémas), vous donnerez également le détail des mécanismes de clés mis en œuvre et les réponses aux questions. En conclusion, donner votre avis sur l'apport des certificats pour la messagerie et votre sentiment sur l'évolution de la messagerie sécurisée.

Mode de rendu :
Le dossier comportera un résumé de TP0. Il sera nommé S51_TP1_<Nom>.pdf (ex : *S51_TP1_Muller.pdf*). et sera envoyé par mail signé avec nom de l'émetteur en clair (et si possible chiffré : *S51_TP1_Muller.zip → Dominique.Grad@urs.u-strasbg.fr*) le vendredi 14/12/07 au plus tard.