TP1 : La messagerie sécurisée

Olivier DOSSMANN

2007-12-10

Table des matières

1 Avant le TP1 ...

...il y a eu le TP0 !

1.1 Résumé rapide

Dans ce TP0 nous avons mis en place et utilisé des machines virtuelles :
- Sous FreeBSD
- Sous Windows 2000 (Win2K)

Le principe était simple : nous familiariser avec chacun des systèmes.

Il en résulte que l'utilisation, bien que similaire à celle des produits GNU / Linux, de FreeBSD s'est avérée plus compliquée que prévue, mais pas insurmontable. De bons coups de *man* ont permis de se documenter sur les possibilités du systèmes, et la plupart des commandes disponibles sous GNU / Linux, telles que *df -h* pour l'affichage de l'espace libre/occupé sur les partitions/disques/points de

montages, étaient fonctionnelles.
En revanche la configuration du réseau se faisant dans le fichier */etc/rc.conf*, nous avons buté dessus un bon moment.

Concernant l'utilisation de Win2K, rien de spécial n'est à dire, le système présente une couche graphique omniprésente, il suffit simplement de savoir cliquer au bon endroit au bon moment pour tomber par inadvertance (ou pas) sur la bonne fenêtre. De là des options de configurations en tout genre permettent à l'utilisateur d'agir sur le système, rien de trop spécial.

1.2 Conclusion

Nous concluons de ce premier TP0, que le temps et les ressources matérielles n'ont pas permis de finir entièrement, que l'utilisation de systèmes connus est forcément plus simple, et que nous nous enfermons dans des habitudes qui ne devraient être. Voilà pourquoi changer souvent de système permet de changer d'air, et de respirer le bon air frais de la liberté d'utilisation.
A noter que nous sommes intrigués par l'installation d'un serveur apache sur un système BSD, espérons que cette année nous permettent (niveau temps surtout) de parvenir à une telle installation, et, qui sait, à installer une surcouche SSL par dessus pour permettre l'utilisation de certificats sur le protocole de transfert hyper texte (ou HTTP).

2 Introduction à la messagerie sécurisée

La messagerie instantanée est aujourd'hui un facteur prédominant dans l'échange d'informations au sein des entreprises.
A cet effet, et sachant que la vie de l'entreprise passe aussi par des secrets et des techniques de fabrication, de déploiement, de développement ou même par simple mesure de précaution pour protéger sa vie privée, il est utile de pouvoir "cacher" les données confidentielles, de peur qu'elles soient vues par une tierce personne. Une personne non habilitée à lire ce genre document.

Ainsi nous verrons étapes par étapes, les problèmes et les solutions qui résultent de l'utilisation d'un logiciel de messagerie courriel.

3 Le client de messagerie courriel

3.1 Installation

Nous étions sur des machines virtuelles Windows 2000 (Win2K), ainsi l'utilisation d'Outlook Express 5 semblait tout à fait appropriée pour ce genre d'exercice. Nul besoin, donc, d'installer un client de messagerie.

3.2 Configuration

Sous Outlook Express, la première utilisation entraîne le lancement d'un assistant permettant la configuration d'un compte POP/IMAP. Ce sont des comptes qui permettent la récupération d'une boîte courriel auprès d'un serveur courriel, par exemple le serveur de notre Fournisseur d'Accès Internet (FAI).

Nous utiliserons le serveur courriel de l'IUT pour la récupération des courriers, et le serveur courriel d'un FAI pour l'envoi du courrier (le TP ayant été effecté à l'extérieur de l'enceinte du bâtiment informatique).
Pour ce faire nous avons les caractéristiques suivantes :

- Nom du compte : *Compte Personnel*
- Adresse courriel : *Olivier.Dossmann@eturs.u-strasbg.fr*
- utiliateur : *3dossmanno*
- mot de passe (utilisé seulement pour le TP) : *blankoworld*
- serveur pop : *mailserver.u-strasbg.fr*

Est à ajouter qu'il faut configurer le client courriel pour laisser les messages sur le serveur (en somme faire une copie de ces derniers). Ceci évite de perdre ses courriel simplement par mise en route d'un TP.

4 Les certificats

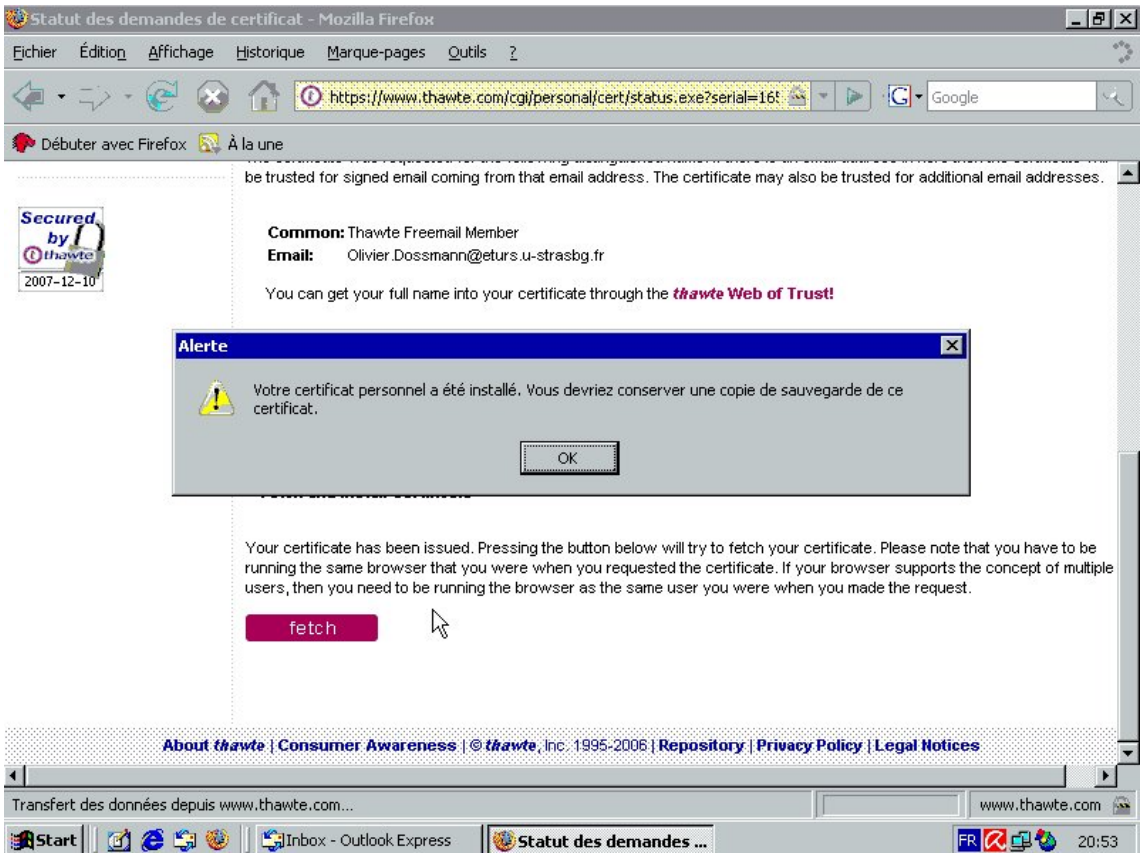
Parmi les solutions possibles (quoique restreintes), l'une des plus commode est l'utilisation de certificats.

Un certificat est un document numérique que nous obtenons sur Internet, ou bien à des agences spécialisées. Nous ne reprendrons pas le cours qui explique cela bien mieux que nous. Cependant nous nous attèlerons à l'obtention et l'installation d'un certificat dans un client courriel afin de tester la certification.

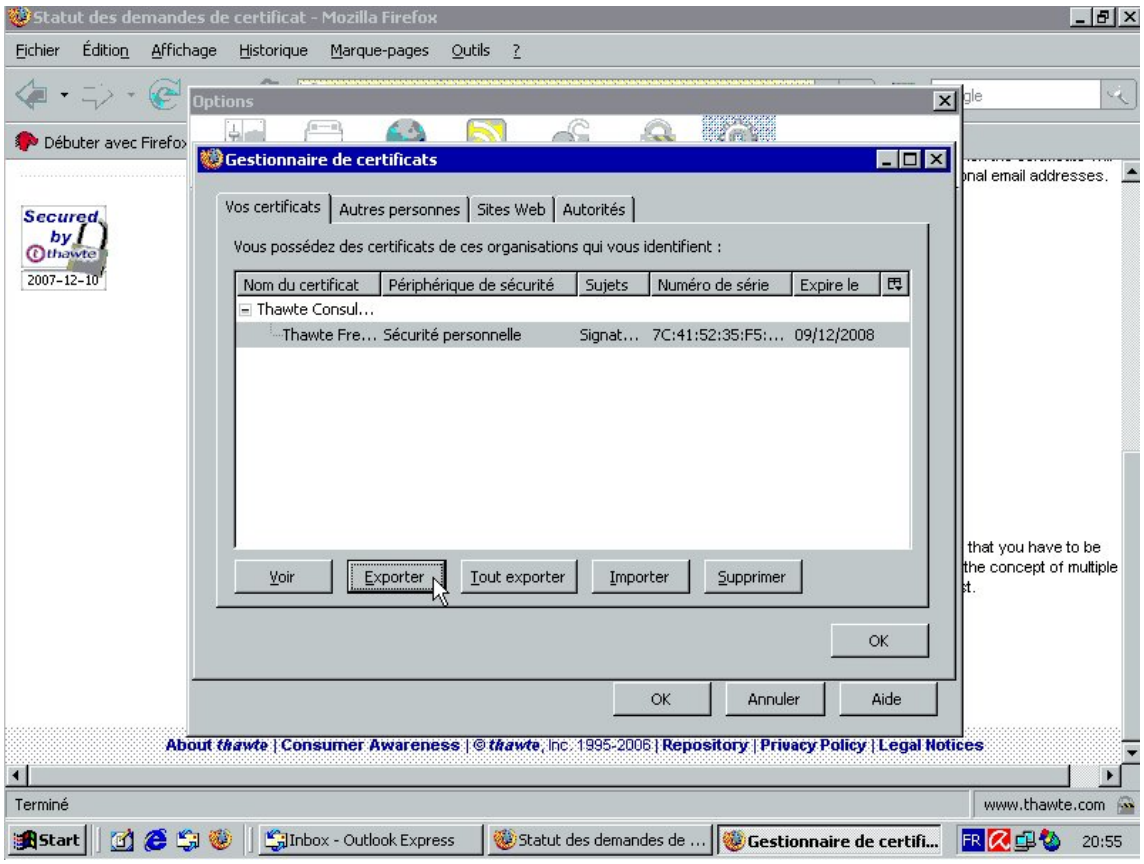
4.1 Obtention d'un certificat

Là encore, plusieurs sites permettent d'obtenir un certificat, nous avons choisi le site Thawte.com qui propose des certificats personnels gratuits.

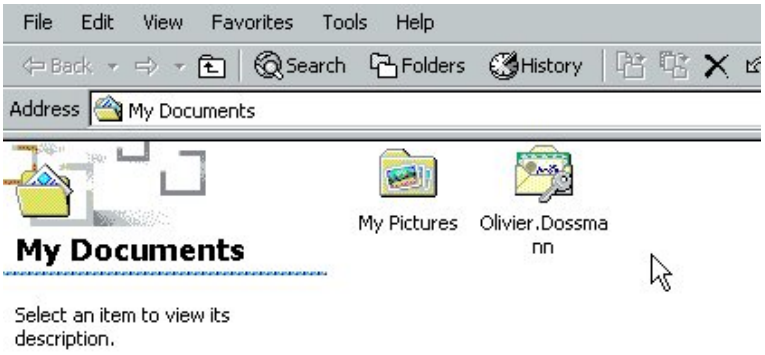
La première étape consiste à s'enregistrer sur le site et à répondre à tout un tas de questions ; après quoi nous reçevons un courriel nous confirmant l'acceptation de notre demande.
Ce courriel contient un lien qui redirige vers la page permettant l'obtention réelle du certificat.



Nous récupérons donc le certificat à l'aide du navigateur Web (ici Mozilla/Firefox), puis nous l'exportons.



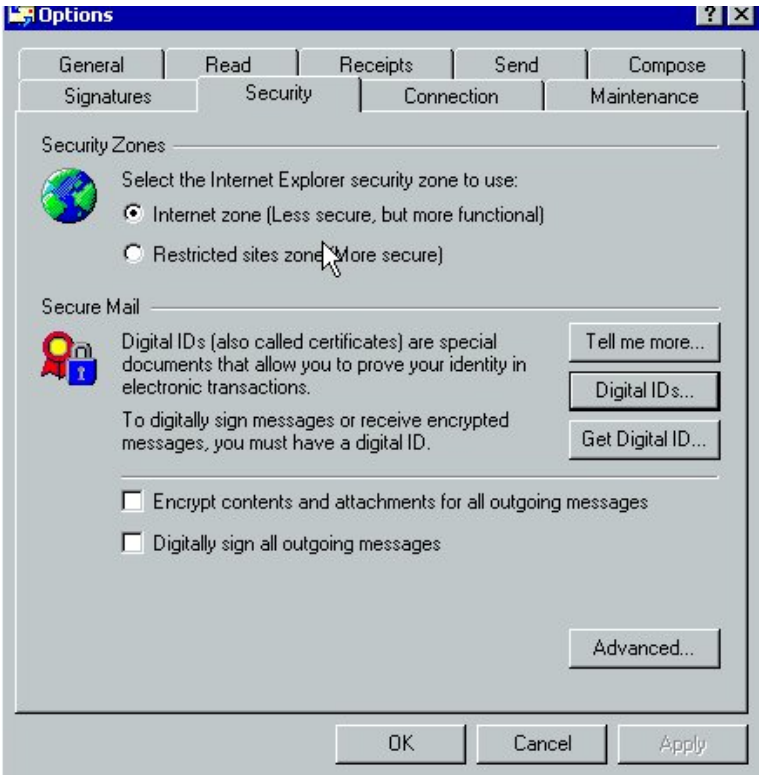
Il permet l'enregistrement d'un fichier portant l'extention *p12* et se nommant *Olivier.Dossmann.p12* que nous enregistrons volontairement dans le dossier *My Documents*.



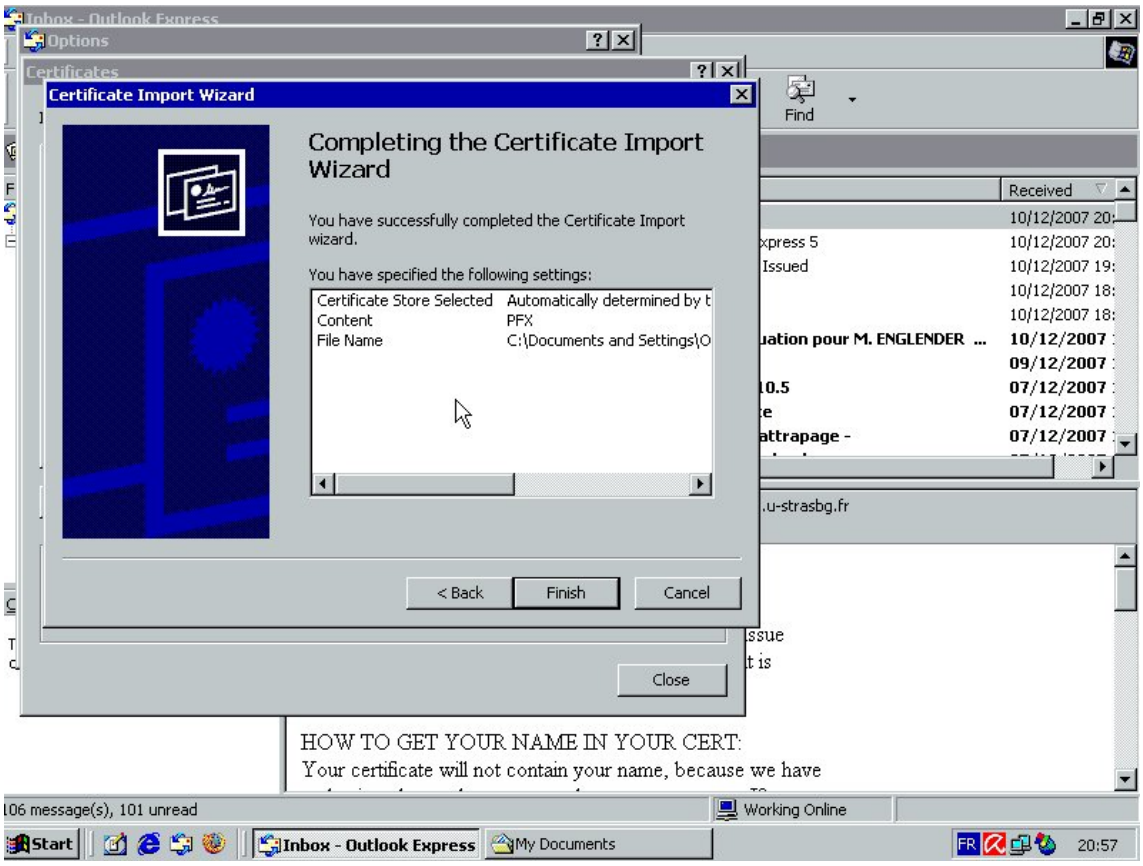
Voyons désormais comment utiliser ce certificat.

4.2 Installation du certificat dans Outlook Express 5 sur Win2K

Le certificat récupéré, il faut pouvoir l'utiliser dans notre logiciel de courriel. Pour cela nous ouvrons Outlook Express 5, sur Windows 2000 (Win2K). Nous allons sur Outils > Options, puis dans l'onglet Sécurité. Il ne reste plus qu'à cliquer sur le bouton *Identificateurs numérique* (aussi appelé *Digital IDs*.



Un assistant nous guide tout au long du processus d'importation.



Désormais notre certificat est installé sur Outlook Express 5 !

Nous pouvons également cocher la case *Signer automatiquement l'ensemble de mes messages*.

4.3 Caractéristiques du certificat

Le certificat se compose de plusieurs choses.
D'une part nous avons une clé privé et une clé publique, ce sont donc des clés asymétriques de chiffrage.

D'autre part nous avons des informations sur l'identité de la personne possédant le certificat.
Et finalement nous avons une hiérarchie de certification, c'est à dire des liens de confiance qui s'établissent par le biais de tierces personnes. C'est un système très particulier. Ici, par exemple (chez thawte.com), il faut obtenir pas moins de 50 points de confiance pour établir une confiance de base.

Le certificat, si le désire en venait à vouloir l'exporter, ou le "voler", est protégé par mot de passe. Ainsi nous avons beau avoir le certificat de quelqu'un, sans la phrase de passe, impossible de l'utiliser pour envoyer du courriel.

4.4 Les certificats et l'environnement bureautique

Le certificat est avant tout installé par le navigateur Web utilisé, mais aussi dans le logiciel de messagerie courriel, selon type de système d'exploitation et programmes compatibles.
Sous Mozilla Firefox, que nous avons utilisé pour le TP1, il faut récupérer le certificat en procédant de la manière suivante :

- Aller dans le menu *Outils* > *Options*
- Choisir l'icône *Avancé*
- Choisir l'icône *Chiffrement*
- Presser le bouton *Afficher les certificats*
- Séléctionner le fichier à exporter
- L'exporter en cliquant sur le bouton *exporter*

Le fichier s'enregistre au format **PKCS#12**, avec l'extension *.p12*, comme expliqué auparavant. Il ne reste plus qu'à le transférer sur l'ordinateur et dans le logiciel que nous voulons à l'aide de copies ou encore d'imports. N'importe quel logiciel ayant le support pour les clés PKCS#12 pourra utiliser notre certificat personnel, contenant à la fois la clé privée et la clé publique - Attention !, l'export demande si nous voulons oui ou non exporter la clé privé avec la clé publique. Si c'est pour un usage personnel, il faut confirmer, sinon le refus permettra d'avoir simplement un certificat susceptible d'être partagé à d'autres, avec les données sur l'utilisateur et sa clé publique.

Nous pouvons également utiliser le certificat sur un client courriel, c'est d'ailleurs le but de ce TP et l'origine du besoin de chiffrement.

5 Utilisation des certificats sous le client courriel

Après avoir fait les manipulations données dans les paragraphes suivants, attachons nous à l'utilisation des certificats sous un client de messagerie, et, la fois là, sur Outlook Express 5 (installé sur une machine Win2K). Nous verrons dans un premier temps l'envoi de message signés, puis dans un second temps la réception de ceux ci, et l'enregistrement du certificat de quelqu'un d'autre.

5.1 Envoi de messages signés

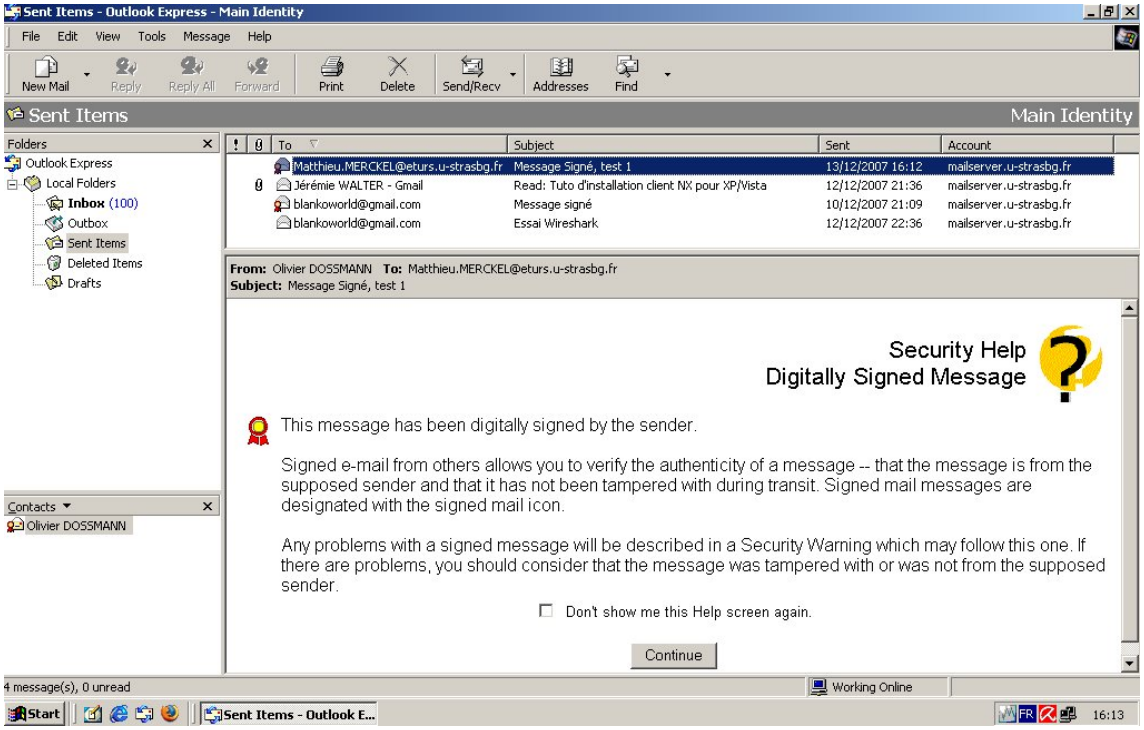
Sous Outlook Express 5, dans la configuration de la Sécurité, nous avions dit pouvoir activer la signature de chacun des courriels que nous envoyons.
Ainsi chaque mail envoyé sera signé automatiquement, c'est à dire proposera en pièce jointe un fichier contenant à la fois notre clé publique de chiffrage (dont nous reparlerons plus tard), mais aussi l'ensemble des données nous concernant.

NB : La personne qui écrit ce document ne sais pas encore totalement si les données nous concernant sont récupérées et mises à jour régulièrement par interfacage Web et par connexion au site Thawte, où si les données sont brutes, c'est à dire écrites au moment de l'envoi du certificat et non modifiées par la suite (sauf si le possesseur renvoie un courriel certifié mis à jour).

De cette manière nous envoyons des courriels signés, contenant certificat et clé publique ; ce courriel est reçu par le destinataire qui pourra alors enregistrer (et vérifier par la même) ledit certificat.

5.2 Récéption de messages signés

De beaux messages apparaissent quand nous reçevons un courriel signé.



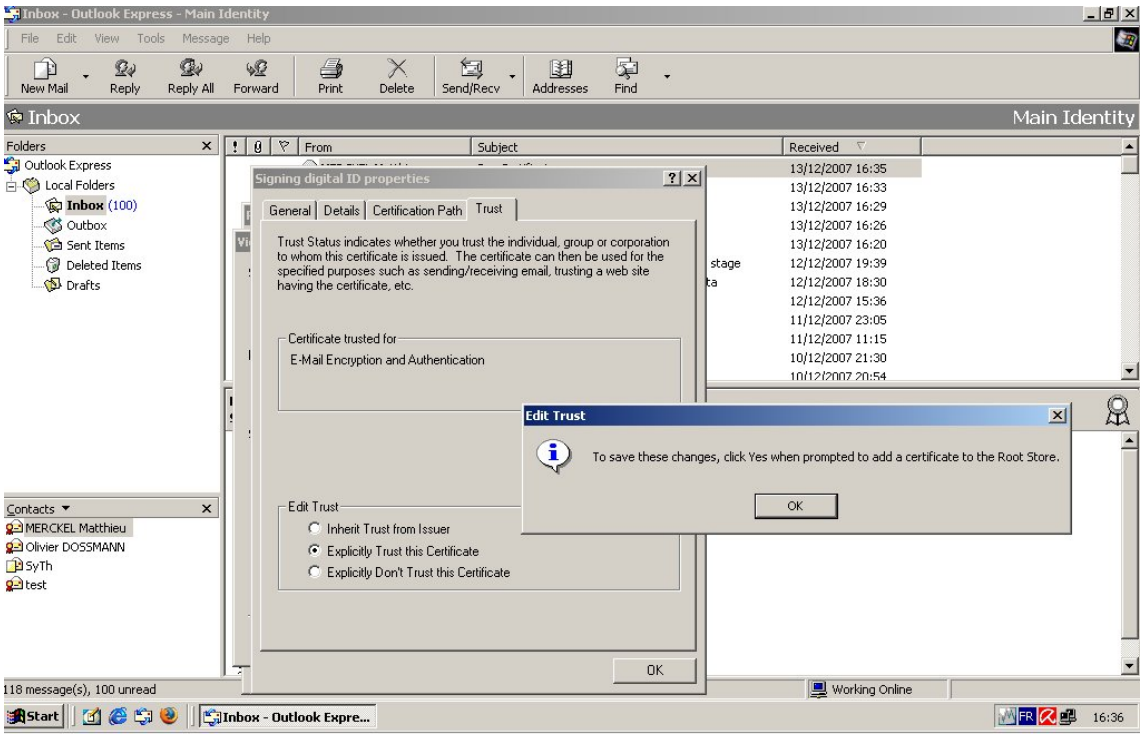
Il propose l'ouverture ou non du fichier.
Le certificat permet donc la certification de l'identité d'une personne, c'est la couche authentification. Et plus la confiance est haute en cette personne (par Thawte), et moins nous *hésitons à ouvrir le document*. C'est une mesure de précaution à prendre au minimum dans les entreprises internationales, ce qui assure au moins l'identité de l'émetteur.

Par ailleurs il est possible d'enregistrer le certificat reçu.

5.3 Enregistrement du certificat étranger

Une fois les règles de confiance (*trust*) vérifiées, nous pouvons enregistrer le contact dans notre Carnet d'adresses, mais également enregistrer le certificat de la personne ainsi que sa clé publique.

Pour enregistrer le certificat, il suffit de cliquer en haut à droite du message, sur le *médaillon* iconifié de Outlook Express 5. Une fenêtre de propriétés apparaît, dans laquelle nous séléctionnons les certificats de l'émetteur, puis nous demandons la fenêtre de propriétés le concernant. Dans cette boîte de détails, nous choisissons l'onglet *Confiance* (en anglais Trust).
En cochant sur le second bouton radio, nous disons à Outlook qu'un désir de confiance envers cet émetteur émane de nous. Le client courriel répond par une boîte de dialogue : "Voulez vous réellement faire confiance à cet émetteur, et par la même de son certificat ?". La réponse OK permet de copier le certificat, et la clé publique livrée avec, dans les certificats *Autres* de notre carnet de certificats.



Il suffit de vérifier par la suite, dans Outils > Options, Onglet Sécurité, Identificateurs numériques, puis dans l'onglet "Autres". Nous pouvons alors voir les détails du certificat.

L'utilisation semble aisée, et le client courriel est un bon programme, mais les protocoles utilisés sont ils aussi sécurisé que ça ?

6 Observation

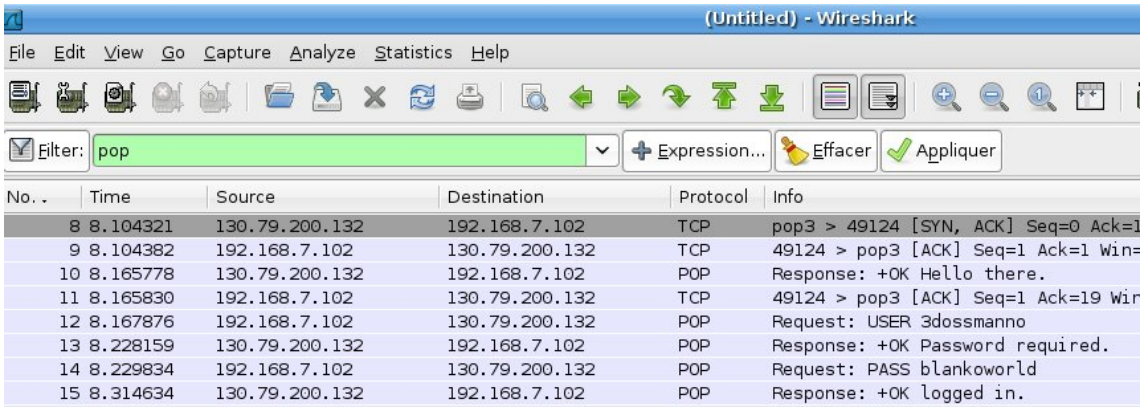
Afin de vérifier ce qu'il peut transiter sur le réseau, nous avons descendu le très connu logiciel Wireshark, nouveau nom donné à Ethereal, nom encore plus connu. Pour en dire deux mots, c'est un aspirateur (sniffer) réseau. Il va lire les paquets qui transitent sur le réseau tout en permettant de procéder à des méthodes de filtrages sur les paquets reçus (ceci pour une meilleure lisibilité humaine des choses).

Nous passerons donc par deux phases : l'écoute, et l'étude du résultat.

6.1 Ecoute du réseau

Après avoir installé le programme, il suffit simplement d'aller dans le menu *Capture* > *Interface* puis de séléctionner l'interface sur laquelle écouter pour permettre au logiciel de commencer sa phase de récupération des paquets provenant de la carte réseau.

L'utilisation de filtre est une bonne idée. Pour cela il faut aller dans l'encadré situé à droite du bouton *filter :*, puis de taper **pop** et finalement de valider en appuyant sur la touche [Entrée].
Il en résulte l'image suivante :



Il faut alors étudier le résultat des trames.

6.2 Etude du résultat

Comme nous le voyons sur l'impression d'écran fournise ci dessus, l'utilisateur POP et son mot de passe transitent à travers le réseau en clair. C'est un problème, puisque toute personne sachant récupérer des trames ou des paquets comme nous le faisons peut utiliser ses informations contre nous, pour nous nuire (comme le font une très grande majorité des hommes sur cette Terre, mais ceci est une autre histoire).

Pour remédier à ce problème, nous pouvons utiliser un chiffrage SSL pour le cryptage des données de connexion et de la récupération des courriers. C'est en général ce qui est utilisé lors d'envois de courriels par SMTP qui requiert SSL.

6.3 Etude d'un message signé

D'autres méthodes dans Wireshark permettent de récupérer entièrement l'ensemble des paquets composants un message courriel. Il faut utiliser le menu *Analyse*, puis *Follow Stream* (de mémoire) pour permettre l'affichage de trames.

Nous obtenons quelque chose comme :

```
1
2  RETR 114
3
4  +OK 5963 octets follow.
5  Return-Path: <olivier.leval@eturs.u-strasbg.fr>
6  Received: from iutsud.u-strasbg.fr (ms2.u-strasbg.fr [130.79.200.142])
7            by baal.u-strasbg.fr (8.14.0/jtpda-5.5pre1) with ESMTP id lBDFTYwl051948
8            for <olivier.dossmann@eturs.u-strasbg.fr>; Thu, 13 Dec 2007 16:29:34 +0100
                 (CET)
9  Received: from WinMV3oleval (pintade.u-strasbg.fr [130.79.81.2])
10 .by iutsud.u-strasbg.fr (Postfix) with SMTP id 430F81FD41
11 .for <olivier.dossmann@eturs.u-strasbg.fr>; Thu, 13 Dec 2007 16:29:34 +0100 (CET)
12 Message-ID: <002201c83d9c$f6494a90$8b00a8c0@WinMV3oleval>
13 From: "test" <olivier.leval@eturs.u-strasbg.fr>
14 To: <olivier.dossmann@eturs.u-strasbg.fr>
```

```
Date: Thu, 13 Dec 2007 16:29:32 +0100
MIME-Version: 1.0
Content-Type: multipart/signed;
.protocol="application/x-pkcs7-signature";
.micalg=SHA1;
.boundary="----=_NextPart_000_001C_01C83DA5.57620940"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1807
X-MimeOLE: Produced By Microsoft MimeOLE V6.
00.2800.1807

This is a multi-part message in MIME format.

------=_NextPart_000_001C_01C83DA5.57620940
Content-Type: multipart/alternative;
.boundary="----=_NextPart_001_001D_01C83DA5.57620940"


------=_NextPart_001_001D_01C83DA5.57620940
Content-Type: text/plain;
.charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable


------=_NextPart_001_001D_01C83DA5.57620940
Content-Type: text/html;
.ch
arset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2800.1578" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV> </DIV></BODY></HTML>

------=_NextPart_001_001D_01C83DA5.57620940--

------=_NextPart_000_001C_01C83DA5.57620940
Content-Type: application/x-pkcs7-signature;
.name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="smime.p7s"

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIII7jCCAnYw
ggHfoAMCAQICEBlVPIBik5ELFvtKepnGXvAwDQYJKoZIhvcNAQEFBQAwYjELMAkGA1UEBhMCWkEx
JTAjBgNVBAoTHFRoYXd0ZSBDb25zdWx0aW5nIChQdHkpIEx0ZC4xLDAqBgNVBAMTI1RoYXd0ZSBQ
ZXJzb25hbCBGcmVlbWFpbCBJc3N1aW5nIENBMB4XDTA3MTIwNjE1MjEzNVoXDTA4MTIwNTE1MjEz
NVowUjEfMB0GA1UEAxMWVGhhd3RlIEZyZWVtYWlsIE1lbWJlcjEvMC0GCSqGSIb3DQEJARYgb2xp
dmllci5sZ
XZhbEBldHVycy51LXN0cmFzYmcuZnIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
ALS299kAVgliXHIJN4ga8hdluWerpcJuQd9U2FHauBNahXic2zME0lQnfOFckEhlL39yso+azbL4
JbHPL9k+XyCi9WGnlwUUHsBfVdjARfaIMucOyPYKNhSwugGjcrWcgj5A4ryenuoj6JuFxiKxsv9g
kwvceQkQDvwAlNpSf7mzAgMBAAGjPTA7MCsGA1UdEQQkMCKBIG9saXZpZXIubGV2YWxAZXR1cnMu
dS1zdHJhc2JnLmZyMAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQEFBQADgYEATnIqdSVfguKKz5RV
```

```
VpnSlO5ZJTirSHHqMvO6F+L3j8VGY0Ttq/rbVSSrKSU
h9gF/VLGe7ZN16cJ5LslldA1GtDEqZSNf
tHsW5pZ+o+3+sQhQl2hWY5gsJvsuwpK3zhJL6cMwa24dfHVwn6qDsjbYpF8d0r22HIF1vMFoieSA
uIowggMtMIIClqADAgECAgEAMA0GCSqGSIb3DQEBBAUAMIHRMQswCQYDVQQGEwJaQTEVMBMGA1UE
CBMMV2VzdGVybiBDYXBlMRIwEAYDVQQHEwlDYXBlIFRvd24xGjAYBgNVBAoTEVRoYXd0ZSBDb25z
dWx0aW5nMSgwJgYDVQQLEx9DZXJ0aWZpY2F0aW9uIFNlcnZpY2VzIERpdmlzaW9uMSQwIgYDVQQD
ExtUaGF3dGUgUGVyc29uYWwgRnJlZW1haWwgQ0ExKzApBgkqhkiG9w0BCQEWHHBlcnNvbmFsLWZy
ZWVtYWlsQHRoYXd0ZS5jb20wHhcNOTYwMTAxMDAwMDAwWhcNMjAxMjMxMjM1OTU5WjCB0TELMAkG
A1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMRowGAYD
VQQKExFUaGF3dGUgQ29uc3VsdGluZzEoMCYGA1UECxMfQ2VydGlmaWNhdGlvbiBTZXJ2aWNlcyBE
aXZpc2lvbjEkMCIGA1UEAxMbVGhhd3RlIFBlcnNvbmFsIEZyZWVtYWlsIENBMSswKQYJKoZIhvcN
AQkBFhxwZXJzb25hbC1mcmVlbWFpbEB0aGF3dGUuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQDUadfUsJRkW3HpR9gMUbbqcpGwhF59LQ2PexLfhSV1KHQ6QixjJ5+Ve0vvfhmHHYbqo925
zpZkGsIUbkSsfOaP6E0PcR9AOKYAo4d49vmUhl6t6sBeduvZFKNdbnp8DKVLVX8GGSl/npom1Wq7
OCQIapjHsdqjmJH9edvlWsQcuQIDAQABoxMwETAPBgNVHRMBAf8EB
TADAQH/MA0GCSqGSIb3DQEB
BAUAA4GBAMfskn5O+PWWpWdiKqTwTRFg0G+NYFhhrCa7UjVcCM8w+6hKloofYkIjjBcP9LpknBes
RynfnZhe0mxgcVyirNx54+duAEcftQ0o6AKd5Jr9E/Sm2Xyx+NxfIyYJkYBz0BQb3kOpgyXy5pwv
Fcr+pquKB3WLDN1RhGvk+NHOd6KBMIIDPzCCAqigAwIBAgIBDTANBgkqhkiG9w0BAQUFADCB0TEL
MAkGA1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMRow
GAYDVQQKExFUaGF3dGUgQ29uc3VsdGluZzEoMCYGA1UECxMfQ2VydGlmaWNhdGlvbiBTZXJ2aWNl
cyBEaXZpc
2lvbjEkMCIGA1UEAxMbVGhhd3RlIFBlcnNvbmFsIEZyZWVtYWlsIENBMSswKQYJKoZI
hvcNAQkBFhxwZXJzb25hbC1mcmVlbWFpbEB0aGF3dGUuY29tMB4XDTAzMDcxNzAwMDAwMFoXDTEz
MDcxNjIzNTk1OVowYjELMAkGA1UEBhMCWkExJTAjBgNVBAoTHFRoYXd0ZSBDb25zdWx0aW5nICChQ
dHkpIEx0ZC4xLDAqBgNVBAMTI1RoYXd0ZSBQZXJzb25hbCBGcmVlbWFpbCBJc3N1aW5nIENBMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDEpjxVc1X7TrnKmVoeaMB1BHCd3+n/ox7svc31W/Ia
dr1/DDph8r9RzgHU5VAKMNcCY1osiRVwjt3J8CuFWqo/cVbLrzwLB+fxH5E2JCoTzyvV84J3PQO+
K/67GD4Hv0CAAmTXp6a7n2XRxSpUhQ9IBH+nttE8YQRAHmQZcmC3+wIDAQABo4GUMIGRMBIGA1Ud
EwEB/wQIMAYBAf8CAQAwQwYDVR0fBDwwOjA4oDagNIYyaHR0cDovL2NybC50aGF3dGUuY29tL1Ro
YXd0ZVBlcnNvbmFsRnJlZW1haWxDQS5jcmwwCwYDVR0PBAQDAgEGMCkGA1UdEQQiMCCkHjAcMRow
GAYDVQQDExFQcml2YXRlTGFiZWwyLTEzODANBgkqhkiG9w0BAQUFAAOBgQBIjNFQg+oLLswNo2as
Zw9/r6y+whehQ5aUnX9MIbj4Nh+qLZ82L8D0HFAgk3A8/a3hYWLD2ToZfoSxmRsAxRoLgnSeJVCU
YsfbJ3FXJY3dqZw5jowgT2Vfldr394fWxghOrvbqNOUQGls1TXfjViF4gtwhGTXeJLHTHUb/XV9l
TzGCAdkwggHVAgEBMHYwYjELMAkGA1UEBhMCWkExJTAjBgNVBAoTHFRoYXd0ZSBDb25zdWx0aW5n
IChQdHkpIEx0ZC4xLDA
qBgNVBAMTI1RoYXd0ZSBQZXJzb25hbCBGcmVlbWFpbCBJc3N1aW5nIENB
AhAZVTyAYpORCxb7SnqZxl7wMAkGBSsOAwIaBQCggbowGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEH
ATAcBgkqhkiG9w0BCQUxDxcNMDcxMjEzMTUyOTMyWjAjBgkqhkiG9w0BCQQxFgQU6PAOGi5oQCK+
XZaX9Cl25e0tCigwWwYJKoZIhvcNAQkPMU4wTDAKBggqhkiG9w0DBzAOBggqhkiG9w0DAgICAIAw
DQYIKoZIhvcNAwICAUAwBwYFKw4DAgcwDQYIKoZIhvcNAwICASgwBwYFKw4DAh0wDQYJKoZIhvcN
AQEBBQAEgYBonBaoKXhWJfm/ULh0EuXNCzuBUcMQrKLno1apSIyFi
mttXAnLC4nLJihKW7d3OS0w
fHvESK9p9EL7pAY5EXGFbYTuvudHHtktWuDkp6RGmB68HAhT3Am6/A6WrwFNcAQLhJxwxBDT+W7x
aPsbHi70aHlFke6aQP2mU6d4v/9mHQAAAAAAAA==

------=_NextPart_000_001C_01C83DA5.57620940--

.

QUIT
```

Nous distinguons donc les champs suivants :

- Return-path : Désigne l'adresse à laquelle le courrier de réponse (s'il y a lieu) sera adressé
- Received : Deux champs *Received* renseigne le serveur SMTP d'envoi (iutsud.u-strasbg.fr), le serveur qui a traité le courriel (ici baal.u-strasbg.fr), et le destinataire (nous-même). Le second champ *Received* donne l'émetteur du courriel (ici c'est M. LEVAL Olivier).
- Message-ID : Ce doit être l'identifiant de session lors de l'envoi du courriel vers le serveur, ou quelque chose de similaire.
- From : Contient une information supplémentaire sur l'émetteur, à savoir son adresse courriel et la dénomination qu'il se donne. Il a d'ailleurs très poétiquement choisi de se nommer "*test*".
- To : Désigne le destinataire du message ; comme quoi on peut reçevoir du courriel qui ne nous est pas destiné, tout comme cela

arrive avec le courrier papier.
- Date : La date pardi !
- MIME-Version : la version MIME utilisé pour construire le message
- Content/Type : Type du contenu du message. Nous trouvons ici que c'est un message signé avec une clé de type PKCS#7 et sûrement une clé publique en SHA1.
- X-Priorité : La priorité du message, ici 3.
- X-MSMail-Priority : Le mode de priorité, ici *normal*.
- X-Mailer : Logiciel de courriel utilisé (sûrement une chaîne de caractère créée de toute pièce par le logiciel en question. Nous retrouvons le logiciel de courriel Outlook Express 6.0 et des poussières.
- X-MimeOLE : Aucune idée de ce que cela peut signifier.

Par la suite une phrase affirme que le courriel est en plusieurs morceaux. Nous en trouvons un en format HTML, un morceau de texte, des espaces vides, et finalement le nom d'un fichier et un très très gros morceau de caractères désignant sûrement la signature du courriel.

Grâce à cette étude du courriel, nous comprenons qu'un message contient bien plus d'informations que nous le pensons. Et qu'une tierce personne ayant l'oreille sur le réseau pourrais avoir beaucoup d'informations sur les flux d'échanges entre deux points du réseau, comme par exemple la discussion courriel entre deux entreprises.
Peut être y a - t - il un moyen plus sûr que d'envoyer qu'une signature ?

7 Chiffrage

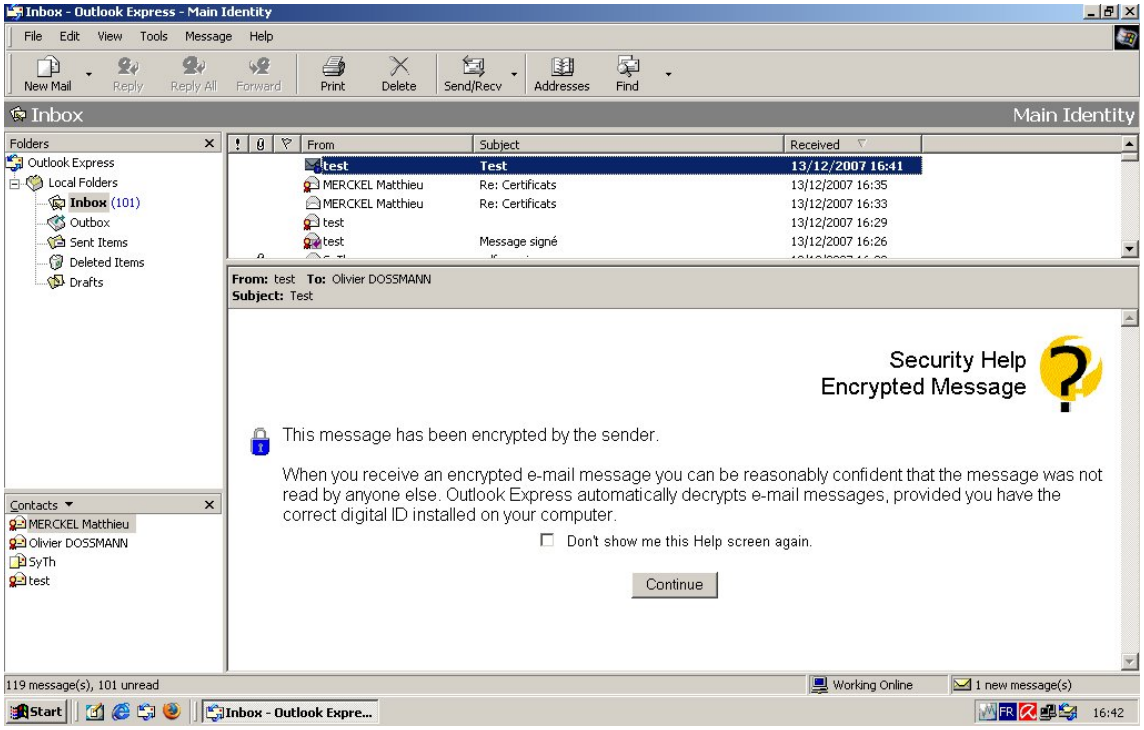
Oui cela existe, et cela se nomme le **chiffrage** ! Jusque là nous parlions sûrement de cryptage, car nous n'arrivions pas à décrypter un message codé. Cependant, et dans le cas précis que nous allons voir, il faut bel et bien utiliser le terme chiffrage, car le message chiffré est prévu pour être déchiffré par une personne, c'est à dire la bonne personne, celle détenant à la fois une clé privée et un mot de passe.

Le certificat que nous avons si généreusement reçu de *Thawte* contenait une clé privée. Une quéquoi ? Une clé privée ! En parallèle / complément d'une clé publique. C'est l'avantage des clés asymétriques : vous pouvez donner à tout le monde votre clé publique, tout en gardant votre clé privée. De la sorte seul vous pouvez déchiffrer les messages qui auront été chiffrés avec votre clé publique. Cela paraît "surnaturel", mais c'est ainsi que cela se déroule.

7.1 Envoi d'un courriel chiffré

Vous l'aurez compris, si vous envoyez un courriel chiffré avec votre clé publique, vous serez le seul à pouvoir le déchiffrer, ce qui est totalement inutile (pour ne pas dire idiot).
Voilà pourquoi il faut absolument récupérer le certificat de quelqu'un d'autre, certificat contenant sa clé publique, et donc permettant de chiffrer des messages à lui envoyer. Nous avons déjà vu comment récupérer un certificat transmis en pièce jointe d'un courriel, envoyons désormais un courriel chiffré à la personne qui nous a envoyé le courriel.

Pour cela il suffit simplement de cocher l'icône indiquant un cadenas bleu, lors de la rédaction d'un courriel. Le message, lors de l'envoi, sera chiffré. Si tout va bien, à l'ouverture du message, le destinataire reçevra un message de confirmation pour déchiffrer le courriel.



Après quoi il pourra lire le message que vous lui avez envoyé.

Procédez de même pour chiffrer et signer en même temps, il faut que les deux soient cochés et que les deux icônes apparaissent sous Outlook Express 5 (ou supérieur). Voyons désormais envoyer des courriels chiffrés et signés pour permettre à la fois de protéger le contenu de votre message et garantir au destinataire d'être sûr que vous soyez bien le bon émetteur. Par contre tout se fait donc lors de la récéption du PREMIER courriel contenant le certificat. C'est là que tout se joue selon nous !

7.2 Etude du message chiffré ET signé dans Wireshark

En procédant de la même façon que précédemment, nous avons capturé la trame résultant de la récéption d'un courriel chiffré ET crypté. Bien qu'étant long, peu parlant et bien trop indéchiffrable, il est bon que vous sachiez à quoi cela ressemble. Voici donc le message entier, en bon et due forme (ou presque !).

```
1  RETR 122
2
3  +OK 9036 octets follow.
4  Return-Path: <matthieu.merckel@eturs.u-strasbg.fr>
5  Received: from iutsud.u-strasbg.fr (ms1.u-strasbg.fr [130.79.200.141])
```

```
by baal.u-strasbg.fr (8.14.0/jtpda-5.5pre1) with ESMTP id lBDGMwMW079656
for <Olivier.Dossmann@eturs.u-strasbg.fr>; Thu, 13 Dec 2007 17:22:58 +0100 (CET)
Received: from test (dindon.u-strasbg.fr [130.79.81.1])
.by iutsud.u-strasbg.fr (Postfix) with ESMTP id BA8061FD41
.for <Olivier.Dossmann@eturs.u-strasbg.fr>; Thu, 13 Dec 2007 17:22:58 +0100 (CET)
Message-ID: <009001c83da4$6cd4dec0$9871a8c0@test>
From: "MERCKEL Matthieu" <matthieu.merckel@eturs.u-strasbg.fr>
To: "Olivier DOSSMANN" <Olivier.Dossmann@eturs.u-strasbg.fr>
References: <20071213155452.eahq1atz2sogwc4s@webmail.u-strasbg.fr>
Subject: Re: Certificats
Date: Thu, 13 Dec 2007 17:22:56 +0100
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime;
.smime-type=enveloped-data;
.name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="s
mime.p7m"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1807
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1807

MIAGCSqGSIb3DQEHA6CAMIACAQAxggKjMIIBDQIBADB2MGIxCzAJBgNVBAYTAlpBMSUwIwYDVQQK
ExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMSwwKgYDVQQDEyNUaGF3dGUgUGVyc29uYWwg
RnJlZW1haWwgSXNzdWluZyBDQQIQYC3CzxSOT8IB/9dwdiI58zANBgkqhkiG9w0BAQEFAASBgOro
Zwo6n2OUOSZ6uWJ3XcPFOJTTQ
ICmLH4UyPDaaGk07x0mj9Ac3e9QPK94OPaCGbkDkyIEEyB5vbD7
2DvebvXFDmuoHBWfl84LseMdyW7lI2ggl20b/x+IhOqgc42QP6CBOwASTPia3JTgT68khsxocX5K
UiLcWByc9xUCzWNsMIIBjgIBADB2MGIxCzAJBgNVBAYTAlpBMSUwIwYDVQQKExxUaGF3dGUgQ29u
c3VsdGluZyAoUHR5KSBMdGQuMSwwKgYDVQQDEyNUaGF3dGUgUGVyc29uYWwgRnJlZW1haWwgSXNz
dWluZyBDQQIQfEFSNfUCtjWgHXKzhQAH6jANBgkqhkiG9w0BAQEFAASCAQARaIo+jUvC9C0bpcJU
9GILdPQr2lpT305f0m33fgDEXRIf271gkHKoh0cslOfzrk+uwHQBZmNFlNeJ1erIt2SqicDNWuf6
8/1Kyy/5mxw8b0kjO5D8ekCgFRXHq70c1gP1wbyeOc4z9uJcd14YHjzxTPGOzih/QG23gFKByxar
L/6XG0y9z2GUjZM0MSEaMYX121NY5dabYJaBAuk77vnOoOSHoSsrMpN2fP20TfDqi+CSVIv6kWFY
KRU6pRSo99B5/0FGsBgJ5G+AV+BiYVY06UB4z28mHAybbi8B3I17zIDQSGO+CNiM/sUHW3YAQYVj
2Jac4BctiCx3UYsuQzS/MIAGCSqGSIb3DQEHATAUBggqhkiG9w0DBwQIOXI6oR8ML7aggASCBADi
lvz55Z1O9NXrttxkOeY7cdwGOqZ1jgpOO533OEN2uLPvsV3yETKlI9obcTUVai+dVoeBDV3hCbpT
F2h3k6JqCfZVVT+MrHOX2iXC6clPb+AmV7PAcLlMOGQxStoClrOWDbohIlj+XMwe8rYARa1ef2Yv
YxWOO9zL+pnTT3fxBtuEpK1mQTZn1pcoasCmm4LhPJJefWkQ/ClCYBKACd6dA3GzvQMJLLeMnxrb
TIBhsxLNsvD+yTMlyUK8lJHtGs45ZGT5rVe
CPrATxu6zA0sWjxMgQkZmJDvLYnZ4xX23EKJZvA5U
p+2z3DtOGYBumm3FHmE+bSkBNykMCfgjZ9veM6qKLfvp4z0Mk87rNkx1VU3BgQq4ooBKcW8Clszu
FF3bOOeRIsFKAftxpHrds/7xL73g5Co5JSAcZyj1gdMYEUF4kHDApLO0vNE2OkK7gRYB7hqmgsYj
+jAEo3aVYoHSF0ZG/Z3ue172rJUspqgbAYKmtuxjKTB2VfEX35RyxKXLZW9itAKlezfvKeS4nFlK
hvHxBQZE562n8w7cZrDtij7GoROhmlz8BjXH7RZiDWs3KtMqgA852F+HTtVKDK7nHJznQ8/6/VYf
cq6rsACzYzMfGovwFbomjoDMD3j5PbwwTGcNeZsbs/mLzH5w+Dmhwdtx8gNgnb+HvwPq1
6VJ/ogi
hxHgHBphc6PNBscRlZv5+vH7xBZn7VH9z0oSxkW2KfWVjRfJBphfxgkiCELxkQ0a2lokpYsogBTp
eUNzfhak6XzgIkUxi28EXr8RwQI0lab5U7sBDyo16I/rQg4ZUIjb7ldimxRklfVYcvFzT33dGbMC
PghSdkvVH5EcWIyv5eKJbFnQ1ENVVJ3caQnVSo4Lg6xWanwrzM7jLS83dyD9Gic/hIpQ6MKlUnGz
OZ37wmgF4tLe3XTW/lEN08qYWjUFLck08YnbvJOe+Q/N/ItKwcSZHvYcTkadca+mbsbZucQxFX2z
sNb39RoHGNpKcva7UaJ7awX6sGts0zdoCkHa4euloigVKcpKFyS0oRZXTEsCOfiCZ4C7aTkpoTI/
zyHUlaulLKo2VVzj4EBa0aqoknHAMiYY2m0Uni+0XsZfsTHuqlTZSn65dKMp2UZf0DAqF8Oz+i08
Qgr7EqkhaHVCLuKGbOj5NsUHHFB99LkiHoZa3p8gL0VlsAAvhykBnXMTirkkMsclDyO+tmYr+g8f
M364VZ8lDz+KelsFsF3NxubnTaDd2mk/xDVDNj37pEs8aLm3zoVQUhrKlcJvCjOot7NczE2bQzov
qpK4JIRyyDG46Q4oyEtb8AENusu8LOa2BL9ra/RZy/pHmiZIinfHSLbDyTgA8atfG0E4rIZHBIIE
ALCjnDbyyaQfWCXc3whxwMEtN9CwNCNzGFCj+FF+IbueUbNiw5pMLvKjLG61CPsO30TGzVgS7dz+
ImHBXLkWnDhxubJd6w86gPL382fqW9sqlKQum/xEP/DqVQYAmUbNFTxZdXWyccls3Gs6bgc/V1w0
Su6SAv1fxPsACn6ZyYjt/e2hHg8lLPkSNRhrgzjmw6flQn4GwgGlwzACi7PM96OFB94U6NwApzEd
```

```
ZrgOAZeHk1TuyukKeaXgoEuCyqMlPs1BCr6Zwx1pRq3/gbyOmxKWBpr4CTBzHCillhIEaUN0r/sG
I
HLLV/2gAxLDaU2aZuV4NHVV6k/Y8oNgxgNevz0cbM8QKQ6zgrfnNJAVsis4Kj3llyb8XiWmAgJZ
3FbPkSjuRncYAx6dTpIydZOy3o8NKyoSQFQcjbzNTPpAI8XD67NM8JYjMN/SEvi1AHNQMHIBoYlA
lRRysfk8d1b5mnKGZaze8wGgyJLa/bEb568wLXtTiIJrf/jGdH7yEvkm6paMGAVHwYpn9R9PWSXd
pX4Gnghk6EKkjqD1HpBUmW0iQGZvHbbDiQE7caxHsJdIoq2322fknXnBMytDRcpNaWwWudD0Pkcx
rEyZsHsGNrEXvKZQibvvXPJ8B0ebH37xT5IqXDjVexuB8dDliMw2ctJ2uaNS3B3gLjZZw9p/QBfC
ml1oJx3Ezp5KkRkGaA9TEWDVJkTqbT5OMEn
NOoSqukszJfkdtKsRkEU25CqqjdSIdLY5YkdKASv4
K39k7swczf/kZp9UHTF75Vf3yCJVtR99w0z4WWBwEikyLvASRJ+QG7VzO9HXABy013Kr2u+OCDoH
3qd+53fqfBoEScTRe+5+ORAh9QGnCrzoraxmxQSOLsuEpt1V0vbfhIeZXJtj/WS3DlrwUKaLDWUj
dcuB75ZuM7ksm/anutMP8zZzd0xQdyVN/1rRNEgvVxn/fNXYbbdWgNxPeZ78lk6NBzr+sSa1Wtwc
0K0FJhjWzAKiURQWuUhFfKmEarr6OlbfXrrJCP/H5UMX1ACMnVY8iyMnskWr77tFuCtKILiiFPOM
fyMXAGAfypb8K9kz2bo5qfRWpvB/ZMzYyWbLC5fRIbAxzCnFyuddJ+G7MndFr2bhVXO5Fyp9mjiZ
dXDOHpJ5erbh2H5Y3vD+epZY3D8GVM0NRVNz3MN9yTtHl8cU5R3h000TOnWRdyKuu8QdG/eVFj9e
m3TCG9QmaPCxVVlHr5KucjcIjZDVRMk8dY43/oElyKiYREjUuGm0FJPHlmwdYiT6VVvNaoZbjtiN
3Dg9BgAUPQM2cj7Ng+VxAbGMnVskjdzu+WL1ffXbVi2amcXFphxtHuxen4z5zbXYIiCiuOg2HZAE
ggQAanu70cWDykn5ErOYSgCbybH0SiTbL6Rt8PAKNm4degn2p200Aa9RSz5LPVY8llu3dgMiEBmZ
bFimG6bpW2JZjXxBB9x2jGNGs5mIR4+oDB716uMqs04/U395S+2UdDZwm6598J/wFAf4jpgNhonY
PFF3v3InxvRQ5NNU9zyjccqQeYxBarn2FadnVQ6yFL0s6eytOhUq9iyxD7fK5R0ZlA1crmmytNZy
MylFeYqVqzzSkCk5D5dQpFWMbHUAbhkalSvu32txchauUDpUEBM//QZbnI+xA8Va6PtHJF6mQ8zW
YgvK3lEWJPWG56Ee9jeeBRm0BeC6w469CkHx2SPv3acBw
j42sj9DNASC6tv4QoLrHMWyIVikn/Q4
/Ltz6Ms+S6PYkjwo9A5DEh0cPyx2FeV7D9ORH5Lbcsgjv0/fGaF26P/TaSnfG+6Ux1KiSmcHCJ8a
dw4zWmPx5YZxCPA+EB7OUBqUZkS52AlaqD3NnHfHkVsYWpI/F42Rzvh4c2yfOoSbKtB7CF1fABmq
6HcKgpQjCwacTkL/ulp8P5mcgymOfai4gWT2QT+AlOq+cVpv3HiuCvASer8sLKLzo7Td0B9ib5t1
1t8zspDzba32mFus7Gkx/NT1i1D3n1lhvF/x3KFuYvQjhpwxtW6XWxx3PHZR3ZOp0ozaV06N6HaY
SW/QL5usqhK87xbMx9w2sltKxC3UORf/Cow6upM1tcFn5de06oR2rEB+iu/rQ5vI9Vd1R4zcPWEb
Y
IbemmSlTuJsBGCV11i7268AaQsYjM74Q86XGPorEY7m1vWPWcdbD2/7NF33fwa1o/JHmSHVyY8q
jtoH5VxOt/fvNXg9AI+S28EPyVR2rJmp7vB16mVdvzz3xHB7+DJOvEuT0UxthW+7PF5Rx7Go8lRg
W8sv8tE7OGBHGQ/0gqG18k5Tr1wK5AKe6lQXzwavsLgbo4drSt/C2Im9Jm7moDy6zj8nzSeekheU
v0lgyTkAONf8UzPmX3OMoDqohu0drrqSh1N/g8OKTgtn6AwG23+kixgbZ5j8W6APZer9sb1+UgQs
3QNqqZIdOO4ycgiqLgW00kGmsuRY4SYaPIdbBM/lnW7QOmwgUxdTEc7YRl/hxOtweww//7rAiG1d
8+mxw5iZwntOGwJ3BcJhjWAWreXe/z26HBS+dyZEYnVoR1gY8+PFPFgwYMRgLxZnUDOZtvosZppW
Osmg1+94Fk4rKiKtd55hIKlTd2CDj4rVaqKrkpdgFoZ0Zt/VQH6taA3f35xbTgIilD40Wuuu9KMQ
61M0Goee/EqAXJRMEvAOM7OaYE7k5DNvsw/jc4LWGbNo5Nm42mHaXQoMkfpdeZcw3RTLz6hKH7B+
awSCBADYiYTJgSvbLMeUI5b1bUdxdGV8JQICF3ABXa3MTL/bOnjI0QoTCvrolO6ZnVhVRFuCZnFC
6u/JmjaQ/oMesVhx1D7A99FaUIqTZcHMNN1wC0o382REE6by5qly47SwTKMS62anK9XqC7+TsJv7
JTEd23tXMqKoIrWmKpp0W2OTBD9jiPILuvFtZnz4P9l62vUzwkz7spFLUeBlBKXp79goRHHcTKtU
7ZlJwsu94+Vtc82sF1j5kvddlVrXntj3OXZFNOBj6cOoefS+2OPBTww4kGzFF38Jeh9LL5PkM39N
YncsbrgceepJhG/TrMNYIbERnv610XQlGCkaTjWgO2qSsWwmatxiBAdaDPySxXET/CjIcKzE+5nu
eyqUQwp3BdO
5hy/kbdisGFF7X/DQHhlsBo2UfNS1pLbu85txZPRUWh6o25px6saHjWQAVs1M2K+e
y8JiDIunbpAKPnakv8OfGuh1vf8BMVXaxo77wpbtISq36vnkpBwhGL1XYDXq/UWmHL1ZynER9YWr
u1DOR2twj74qt5I0cjVSAJYnjOB4XqmYh0/egv9sjMkSOL0rAuCiaL7qR74EU9jt/ryFFh+wYEBN
BGbYZ/KLhW8sBMTkMlagEWIWWh/1U5wrWQ7H44OcECS5Pbx8+FOZOA81JyfXNGrxe/O051xyLJud
ykT75G+HmoUAyvi3meE+Ojd39/YA6hrKiqWVHB+DRLfyd3uoM0NJh8Mgb0a2b1rN4Xl24NKdzIwM
uqIDXiuFmtRsbkdA5mMcfoD48WTtmQ/c5TnfKq0Zpco+f
9xw6jOk0C1Ak0Nq8SunVXYWcHEwOsb4
/m3eLuatlDOcwkrGNYQC3Mbfj4OX6cGJf11w1yJjn9OovoYWHD/I7Otkmx3Piwxi6QFqLdS8Xca2
/gT2Sy58OJE8OO2WX6xslxbBz20zg0eOSqCQueP8AYZ8cK3cL237/72kzO2wSoX4q647r1zTcaGA
VCSoKDV4Ynh/SNxyGymku+XhTe54h3mJ5I0F4gzz3pDCwKGD2W+bNIK+QwZTcUFqiBz6n4IDGvDY
gW0lmxGLt6jP0BC0Fkd1YaNrCzXD4SlpKDj62CgIrYL45rFeJM9IMWvC6p7EI1BFz5LGhy6dYBfo
yXWU3z0mAx8+puTpYdvLuLplzJzHpDO69YJQjoNoR0aGecMdZUN559G5Ad0545kN6jWzr3RSxlMK
xmsddy8RAK08arCZPcpuWmA7TDDkSff/yq+FGPsR4u5+ClG69n47bhWTOebg6hQo/V4k0+1NUBu0
P+c3/9rQmJ/OVOHOYDxf4iBvAGa2z3u4ZAefsZFXCBUSL4IgI1oQrCh2e10uaZTF8a121fLWJRNG
49vKBIIDeHTZJuyrourrPAV2eI46gzsiqqzwCbnnTodaa6rPNc9fZ+FxSN6mSbWZ3c1cr8XYtKTp
TOPYhFSvYi9+Jy5ILBvV03WrIv0/6zUIa7QMU5y6+lspvFLUVq5LWLX64EymGXNjvlPjBPYEmcAj
C6jkLkFrT4ERZ3dqeQ2jk2ZMF2Ggywd/NzjEIxOGM1zva1m6N6RW5Zlx+gx9bJlG1rmaYcSsdXhj
YxKOum4NypoasQp/HR0gby+A96TPgCy6YKK6pWBiPOyiTmlCv8XSfOqUoEged60YOEQ1Ns3nvY5D
```

```
sNIXBTCHPb2X9JBB+lSWG7BHlj/0Gx5H/jRPgNJNLLEYL5HV9B6cM6BZah3d6NRc+BFNAnoSXFFZ
hGKa+QJNicO29wX3WL0oI8w1FRTVA14f49RUkbueVhDn9sIDKksP6MT
+vOjtOhOKed2t+hmW0mX0
F8s9S/pZ9MuolpxLTCSA+ReVzc5LbHnT+AzYf5GiDdRjqNDTG84qELolgnNHtwBoUjVsVZ8RTdqs
OXwDKySZiogypUQRopbRFhJA6wKw/0n3qq5ceEF5hmmpx11EFTUGYypwAHPbqY4JUxMjQNbV4Ni6
H41f5ySpk9o+bz0EKs0/m09QImcc4p1UnsWiA6nQlkkX4c23MxgTqM14zDp5kDOAsOYpm/ply+xw
phjLO8sP/3fFX8AXCndorGkn16gL4Y75dRrP70iZlEQM7S4nz9kT4g49v+f2GIb054TRh003SrSE
e4+pGtyl90a6FFX7UGWtjYSX1u2HBs5i/fHt6T0JvAWpIiPoQVhRONpn+mnPz2cbIHzy0Ztd/3Ry
1dJ09/BMkM1
wNRxQcqCx4ZAMZ8he5HFvdihlRYBJJQCY3r+SiYch4Hr36jlXao2nZHJX9xV+y2Nv
6f/kV/JZpWp5Ojn+4iSJgBkm2pugL0QXz3m8rdLOLAopzqHV0hCyyAE/oprvzL/mKvoMRKwHW8Tb
GSJa8vM7d/ZSiN2Xi2KVsifHDXZ/AdC1biIdPbp2AIqf2OSK6K/7XMSEZjCXmNwFusH6aWbhiQY9
PBGAqP+3skLuhaX9JXEa5SD4feeJ4aMMA9Bj9xbsIEE/mObVtQToWLsPEYcs9BKlkHjecCWIuRmw
kYN9aONMY27Vigse6C8jjDNltfZaUyHLyOkIKreTwa0WBXc5dcXmzAAAAAAAAAAAAAA=

.

QUIT

+OK Bye-bye.
```

Le message ne contenait qu'une phrase, nous vous laissons imaginer la suite lorsque nous écrivons tout un texte, envoyons des pièces jointes, etc ...

8 L'export de Certificats

Bien que nous l'avions déjà décrit auparavant, il faut savoir quelques petites choses sur les certificats.

Dans Outlook Express 5, le certificat personnel peut être exporté avec la clé privée, dans ce cas il se trouve au format **PKCS#12**, avec une extension *p12*. Il est également possible d'exporter ledit certificat avec la clé publique seulement.

Mieux encore, nous pouvons exporter et donc réutiliser les certificats de nos contacts. Ainsi il est possible d'exporter au format **x509** (normes établies pour les standards d'échanges de courriels avec un algorithme pour le chemin de certification, c'est à dire qu'on met en place des réseaux de confiance au travers d'autorités de certifications. Il y a donc une hiérarchie qui permet au réseau de confiance d'être sûr.

Il paraît cependant plus sûr de pouvoir donner son certificat en toute sécurité à quelqu'un. Pourquoi ne pas opter pour le certificat temporaire ? Nous utilisons un certificat, nous échangeons directement des courriels cryptés avec un second certificat (celui ci crypté cette fois), de sorte que notre destinataire reçoive notre certificat réel dans de bonnes conditions.

Autre solution : transport du certificat par clé USB, puis remise **en main propre** au destinataire. Ceci n'est possible que sur courte distance, ou alors avec des moyens sérieux de mettre en pratique le déplacement de la personne possédant la clé USB jusqu'à la seconde personne désirant la clé publique.

En tout cas l'utilisateur n'a plus qu'à importer le certificat à l'aide des outils adéquats (sur les interfaces graphiques il existe généralement un bouton *Importer*.

Nous arrivons aujourd'hui à des méthodes fiables, performantes et faciles pour obtenir, importer, exporter des certificats et des clés de chiffrage. Pourquoi ne pas en profiter ?

9 Conclusion

Ce TP01 sur la sécurité courriel montre bien que l'utilisation des méthodes de bases sont totalement inefficaces quant à l'utilisation correcte et sécuritaire d'un client de messagerie courriel.
Le protocole POP de base, sans la couche SSL qui va bien, est totalement dénué de sécurité. Il faut donc utiliser SSL dès que possible.
Mais ce n'est pas tout, car l'accessibilité aux technologies de certification et de chiffrage permettent de rendre sécuritaire la communication, que ce soit pas messagerie courriel que par messagerie instantanée, en ce sens que nous permettons ainsi, par l'utilisation desdits certificats, d'assurer l'identité de la personne, l'authentification de cette dernière, et par le chiffrage nous garantissons l'intégrité des données, mais aussi la non - répudiation.
La problématique qui se pose alors est celle ci : La sécurité de l'envoi de courriel est elle actuellement un facteur prédominant dans la vie de l'utilisateur de tout les jours ? Et si oui, les méthodes permettant de remplir toutes les conditions de sécurité sont - elles suffisamment simples pour permettre à n'importe qui de mettre en place un système sécurisé sur sa machine ?

Selon moi il y a plusieurs façons de répondre à ces questions. Tout d'abord je pense que les méthodes sont bien trop complexes à mettre en oeuvre pour une personne de base, même avec des explications (à moins que les explications mettent en jeu un tutoriel, des images et une documentations) ; tout en sachant aussi que le système est assez compliqué à expliquer à quelqu'un, il faut comprendre le fonctionnement pour bien se mettre en tête les notions qui sont mises en jeu. Les informaticiens que nous représentons sont normalement plus débrouillards et avons tout de même rencontrés des problèmes lors de l'évolution du TP. Qu'on se le dise, le chiffrement, c'est pas le moment (slogan qui pourrait être réutilisé plus tard !).

D'autre part j'estime qu'ayant visité le TP de part et d'autre, ayant mis en oeuvre sur Outlook Express ce que j'avais mis en place sur mon client de courriel Thunderbird (avec Enigmail) et sur mon client de messagerie instantanée **PSI** à l'aide de clés PGP (utilisation de GnuPG), la sécurité semble de plus en plus proéminente, et il faut faire attention à ne pas tourner tout cela à la paranoïa !
Seulement voilà, quand nous sommes en informatique, que nous commençons à y toucher de plus en plus, que nous travaillons fréquemment avec des entreprises, que nous sommes en concurrence avec d'autres équipes, d'autres solutions logicielles, il est évident que la sécurité prime, et qu'à ce moment là aucune méthode de protection n'est à délaisser !
Je crois sincèrement qu'à l'avenir je vais mettre un peu plus de sécurité dans mes échanges de données, kit à perdre des données dans le tas, à perdre des amis pour les obliger à faire des choses qu'ils ne peuvent pas mettre en place, mais au moins de vie privée il y aura. Rappelons à juste titre que les fournisseurs d'accès internet, pour la plupart, limitaient déjà leurs abonnés grâce aux routeurs CISCO par étude des trames envoyées sur ledit réseau, et que le seul moyen de contourner cela a été de chiffrer ses paquets. A savoir également que les grosses entreprises telles que celles liées à MSN et Live Messenger (pour ne pas les citer) enregistre et traitent des millions de données de texte privés par jour dans des buts statistiques (voire d'autres buts commerciaux) au détriment de la vie privée de l'utilisateur, même s'il a accepté qu'il en soit ainsi en validant un contrat qu'il n'a même pas lu. Il est également de fait que l'ensemble des données que nous tapons pour des recherches sur le si connu moteur Google n'arrange pas les choses. Je crois ne pas mentir en disant que finalement grâce à internet c'est tout un réseau public qui s'ouvre à nous, cette fameuse toile d'araignée, mais avec une pieuvre qui utilise ses ventouses pour aspirer le moindre petit morceau que nous lui donnerons à manger.

Finalement que dire de plus que ceci : nous ne pouvons faire que prévenir, pas forcément guérir. Ce sont des mots d'une personne ayant passé plus de 3 ans à aider les gens dans le sens de la sécurité et de l'utilisation correcte d'un ordinateur qui vous parle. Les résultats sont très faibles par rapport à l'énergie et le temps dépensé. Certes mes ressources ne sont pas celles des grosses entreprises, mais que faire contre des mégalopôles qui détruisent tout ce qui bougent et réduisent à néant tout sens pratique aux utilisateurs ? La sécurité est importante, mise en pratique par les entreprises et ceux qui veulent bien, pour le reste, j'ai presque envie de dire tant pis.