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

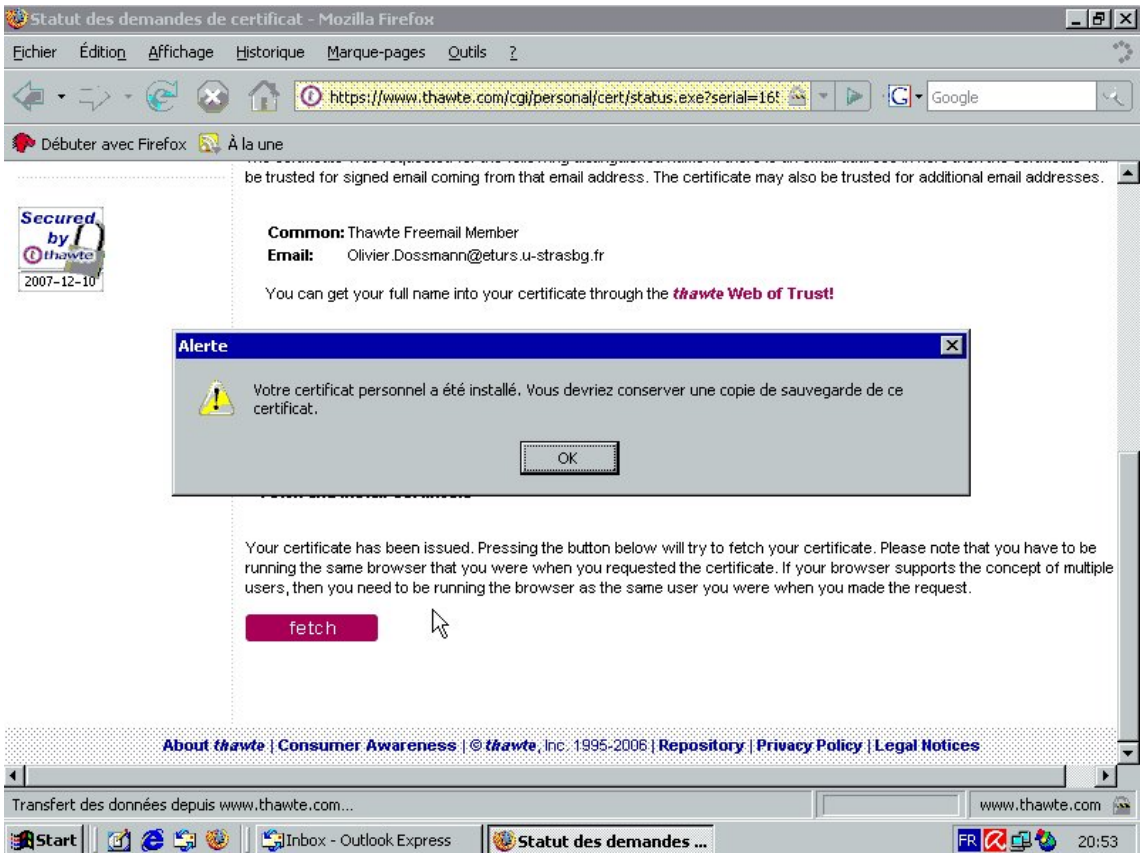
Parmi les solutions possibles (quoique restreintes), l'une des plus commode est l'utilisation de certificats.

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.

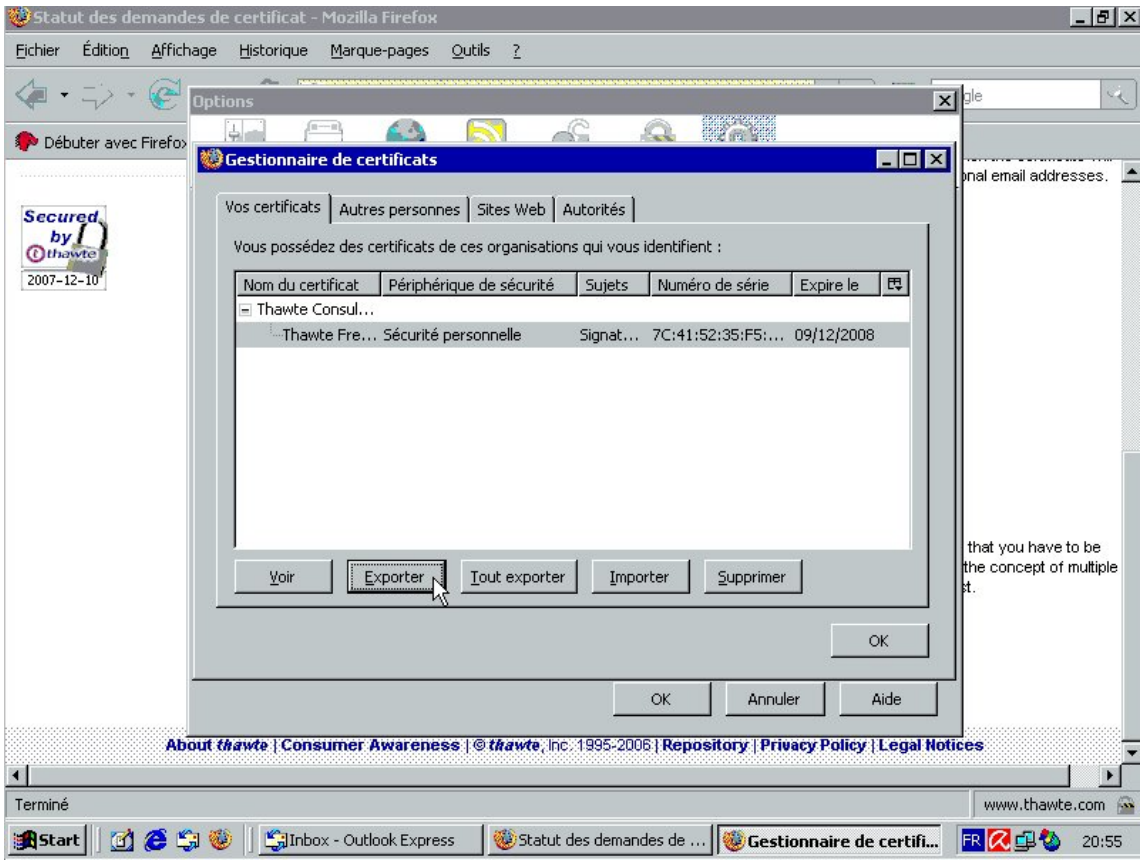
4.1 Obtention d'un certificat

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

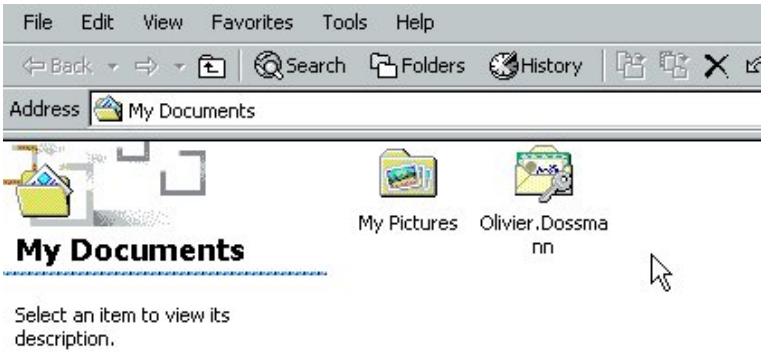
La première étape consiste à s'enregistrer sur le site et à répondre à tout un tas de questions ; après quoi nous reçevons un courriel nous confirmant l'acceptation de notre demande.
Ce courriel contient un lien qui redirige vers la page permettant l'obtention réelle du certificat.



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



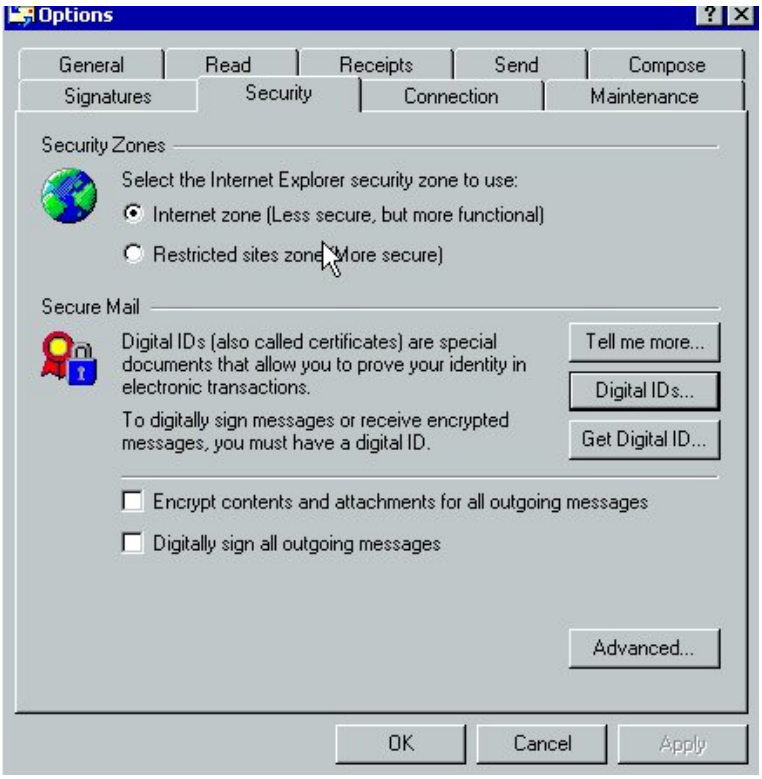
Il permet l'enregistrement d'un fichier portant l'extention *p12* et se nommant *Olivier.Dossmann.p12* que nous enregistrons volontairement dans le dossier *My Documents*.



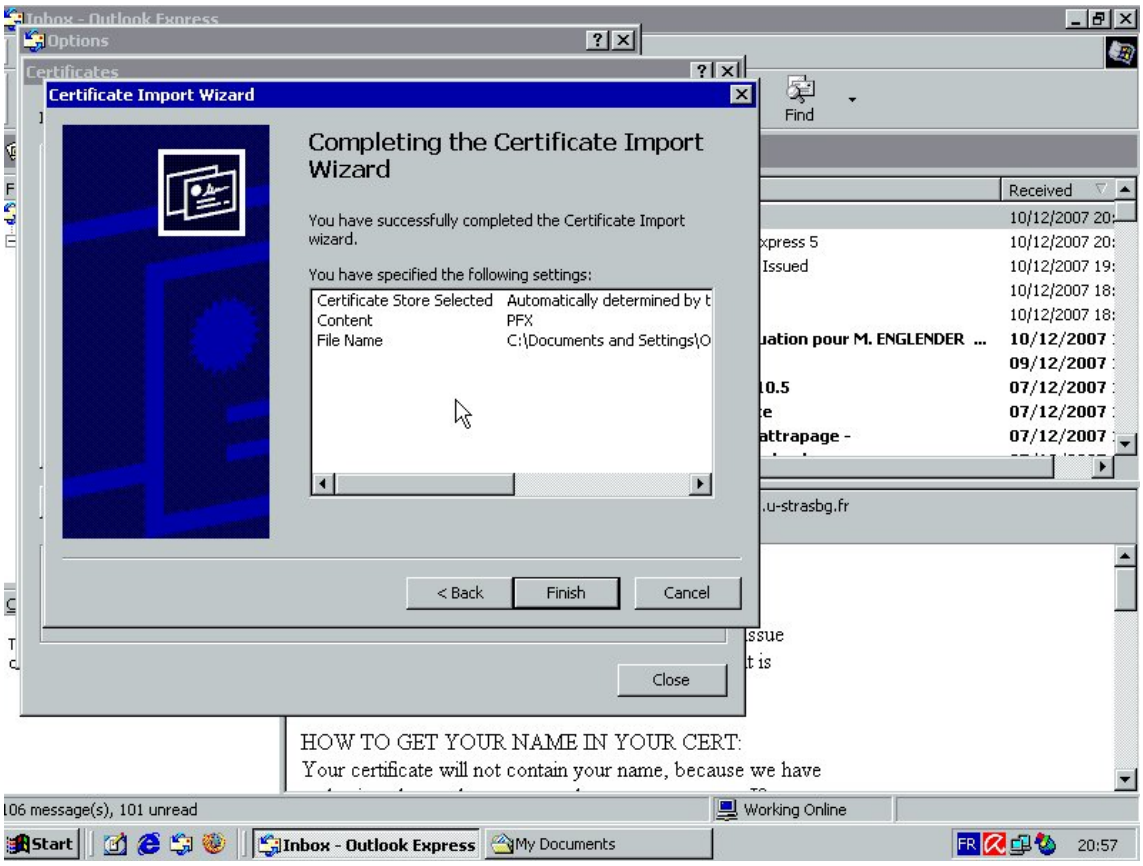
Voyons désormais comment utiliser ce certificat.

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

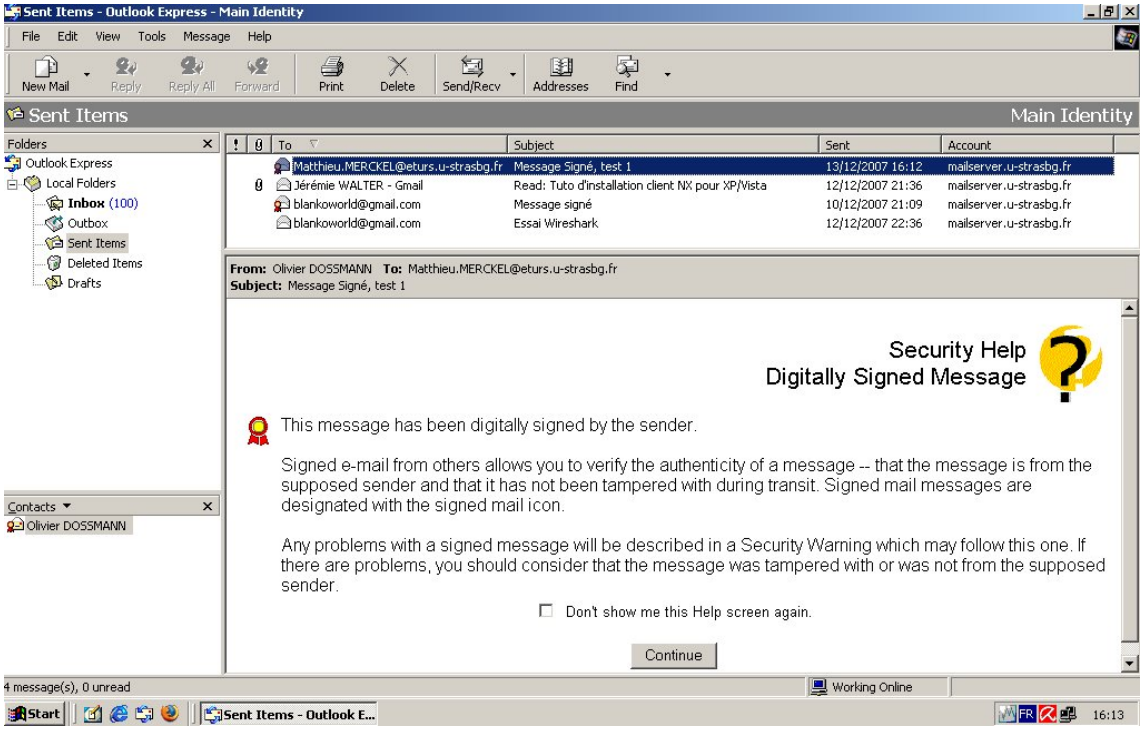
Sous Outlook Express 5, dans la configuration de la Sécurité, nous avions dit pouvoir activer la signature de chacun des courriels que nous envoyons.
Ainsi chaque mail envoyé sera signé automatiquement, c'est à dire proposera en pièce jointe un fichier contenant à la fois notre clé publique de chiffrage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



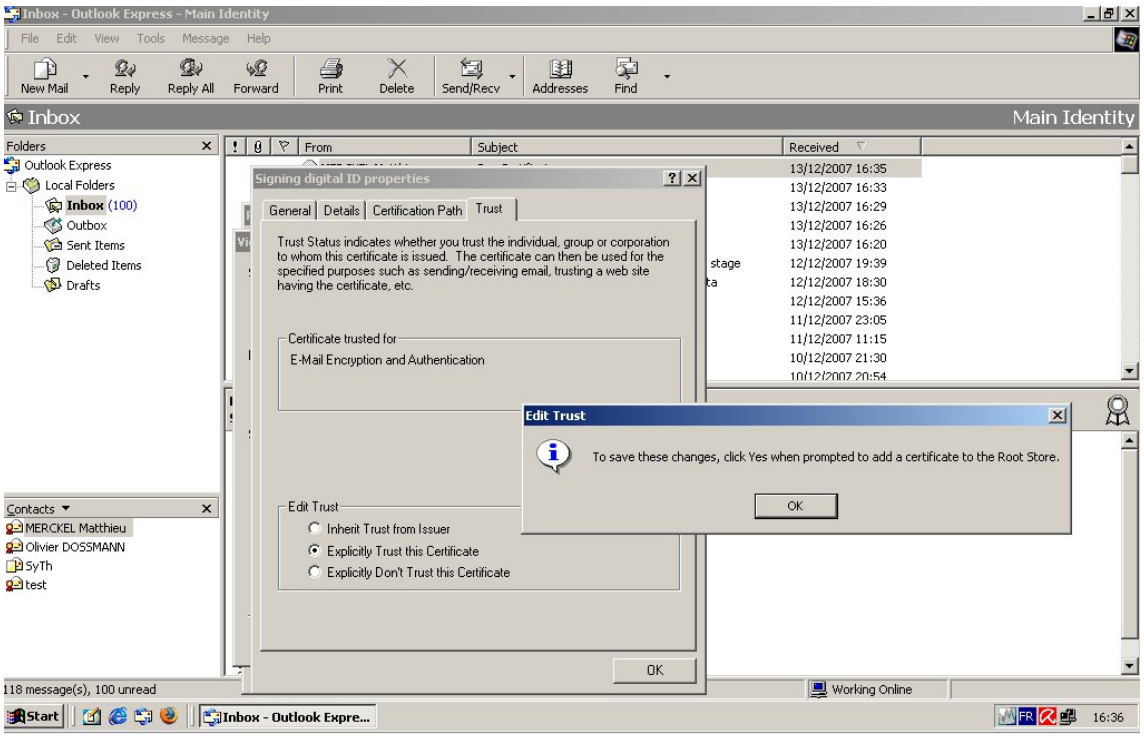
Il propose l'ouverture ou non du fichier.
Le certificat permet donc la certification de l'identité d'une personne, c'est la couche authentification. Et plus la confiance est haute en cette personne (par Thawte), et moins nous *hésitons à ouvrir le document*. C'est une mesure de précaution à prendre au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


Inbox - Outlook Express - Main Identity
File Edit View Tools Message Help
New Mail Reply Reply All Forward Print Delete Send/Recv Addresses Find
Inbox
Main Identity
Folders
Outlook Express
Local Folders
Inbox (100)
Outbox
Sent Items
Deleted Items
Drafts
From Subject Received
13/12/2007 16:35
13/12/2007 16:33
13/12/2007 16:29
13/12/2007 16:26
13/12/2007 16:20
12/12/2007 19:39
12/12/2007 18:30
12/12/2007 15:36
11/12/2007 23:05
11/12/2007 11:15
10/12/2007 21:30
Signing digital ID properties
General Details Certification Path Trust
Trust Status indicates whether you trust the individual, group or corporation to whom this certificate is issued. The certificate can then be used for the specified purposes such as sending/receiving email, trusting a web site having the certificate, etc.
Certificate trusted for
E-Mail Encryption and Authentication
Edit Trust
Inherit Trust from Issuer
Explicitly Trust this Certificate
Explicitly Don't Trust this Certificate
OK
Edit Trust
To save these changes, click Yes when prompted to add a certificate to the Root Store.
OK
Contacts
MERCKEL Matthieu
Olivier DOSSMANN
SyTh
test
118 message(s), 100 unread
Working Online
Start
Inbox - Outlook Expre...
16:36

6 Observation

7 Cryptage

Chiffré
chiffré ET signé