Fiche 8

Utilisation de l'e-mail sécurisé : chiffrement, signature

Sommaire

À propos de la signature électronique

Données de base

Sans entrer dans le détail de la cryptographie, le principe de signature électronique nécessite la délivrance d'une bi-clé constituée d'une clé publique et d'une clé privée. Cette dernière doit absolument rester secrète et à la seule connaissance de son détenteur (sauf pour le chiffrement). A l'inverse la clé publique peut être divulguée, en général assortie d'autres renseignements, le tout étant contenu dans ce que l'on a coutume d'appeler un certificat électronique.

Certificat électronique

Il s'agit d'un document sous forme électronique attestant du lien entre les données de vérification de signature électronique telles que les clés publiques et un signataire. Equivalent d'un passeport dans le monde physique, le certificat électronique joue véritablement le rôle de pièce d'identité électronique.

Valeur juridique d'un e-mail signé : voir supra fiche 4

Signature et chiffrement d'un e-mail

Un exemple concret d'utilisation : l'e-mail sécurisé

- **Les pages qui suivent présentent un exemple d'utilisation du certificat dans le cadre de la signature et du chiffrement des e-mails**

- **Le scénario que nous avons déroulé est très simple:**
  - Un émetteur prépare un message, le signe et le chiffre, et l'envoie à un destinataire.
  - Le destinataire, à son tour, reçoit le message, l'ouvre, valide la signature de l'émetteur et déchiffre le message.

- **Ce scénario est basé sur une infrastructure de messagerie traditionnelle.**
  - Les utilisateurs sont munis de certificats sur leur poste de travail. Ces certificats sont publiés dans l'annuaire de messagerie.

Ce que garantissent la signature et le chiffrement d'e-mail

- **La signature d'un e-mail à l'aide d'un certificat électronique :**
  - Permet d'authentifier l'émetteur du message ;
  - Permet de se prémunir contre l'éventualité d'une répudiation du message et de ses pièces jointes par son émetteur ;
  - Garantit que le message et ses pièces jointes n'ont pas été altérés entre le moment où il a été émis et le moment où il est ouvert par son destinataire.

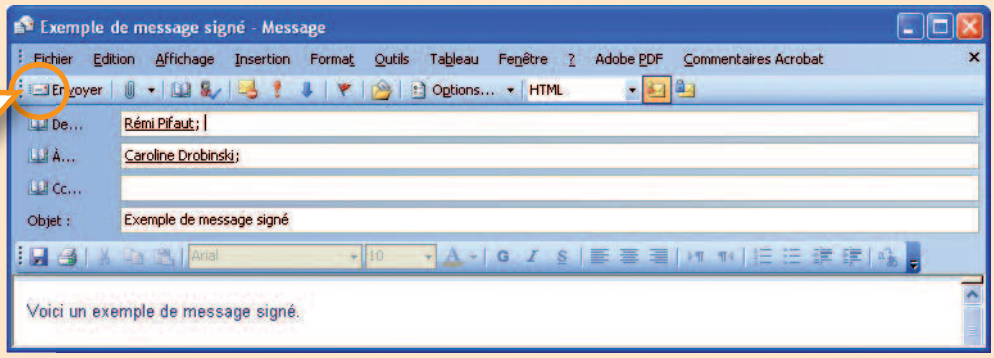
- **Le chiffrement d'un message permet de garantir la confidentialité totale des informations échangées (message et pièces jointes).**

Démonstration : envoi d'un e-mail signé

- **Pour illustrer la signature d'e-mails, le scénario suivant est présenté :**
  - Un émetteur prépare un message, le signe et l'envoie à un destinataire ;
  - Le destinataire reçoit le message, l'ouvre et vérifie la signature de l'émetteur.

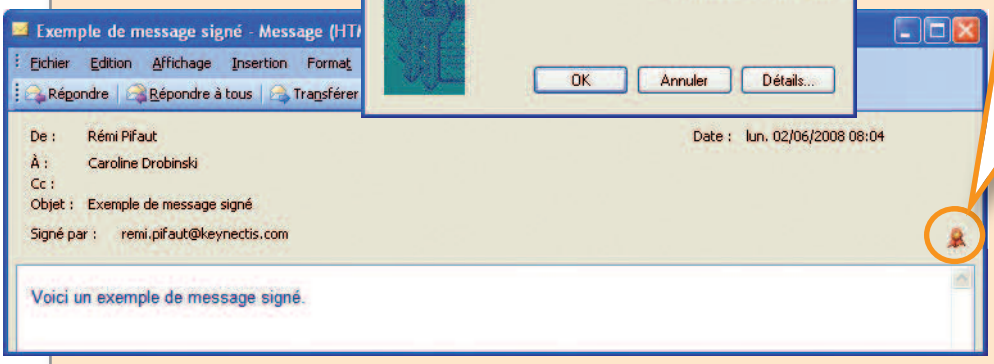
- **Ce scénario est basé sur une infrastructure de messagerie traditionnelle**
  - L'émetteur est muni d'un certificat électronique sur son poste de travail. (voir page ci-contre)

L'émetteur écrit son e-mail puis clique sur l'icône de signature d'e-mail de son logiciel de messagerie ;
Lors de l'envoi du message, le logiciel de messagerie va demander à activer la clé privée présente sur le poste de l'émetteur.
Dans le cas où la clé privée est sécurisée par utilisation d'un mot de passe, une nouvelle fenêtre apparaît.

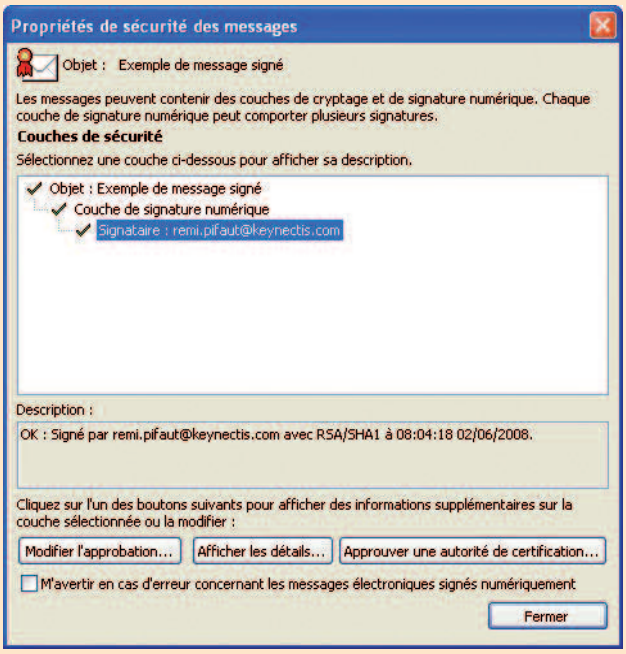


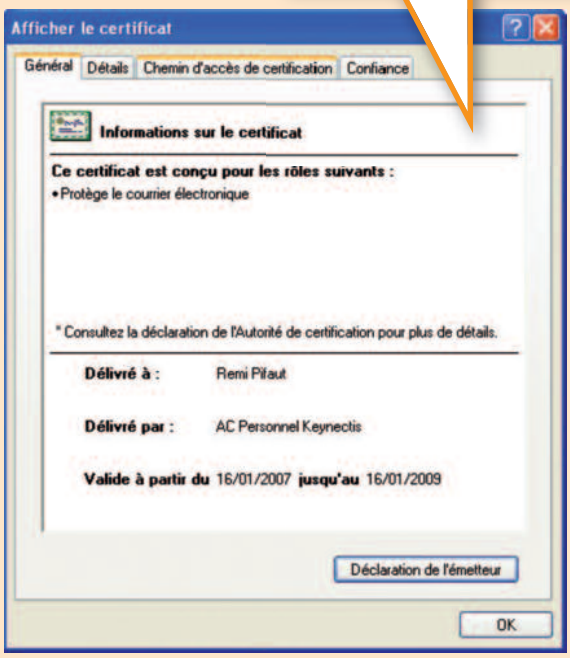
Sur correspondance du mot de passe entré, le message est alors signé de manière transparente par le logiciel de messagerie de l'émetteur.

Lors de la réception de l'e-mail, le destinataire est averti que l'e-mail a été signé. Ceci se traduit par l'apparition d'un certificat présent dans l'e-mail.



En cliquant sur l'icône représentant un certificat, le destinataire peut voir le détail du certificat qui a signé l'e-mail et vérifier aussi la signature de l'e-mail.





Démonstration : envoi d'un e-mail chiffré

- **Pour illustrer le chiffrement d'e-mails, le scénario suivant est présenté**
  - Un émetteur prépare un message et l'envoie en le chiffrant à un destinataire
  - Le destinataire reçoit le message, le déchiffre et l'ouvre

- **Ce scénario est basé sur une infrastructure de messagerie traditionnelle**
  - L'émetteur est muni d'un certificat électronique sur son poste de travail Il est important de préciser que ce certificat électronique ne peut en général pas être le même que celui utilisé pour signer. La contrainte essentielle de tout processus de chiffrement consistant à gérer les clés dans le temps, il est clair que ces dernières devront être détenues au minimum par deux personnes distinctes, contrairement à la clé privée utilisée dans le cadre de la signature électronique qui doit absolument rester secrète et à la seule connaissance de son détenteur.

(Voir page ci-contre)

Exemples d'applications d'un e-mail signé

La messagerie se différencie de la navigation web par la persistance des messages transmis. Cette persistance permet en particulier d'aller plus loin dans les fonctions de sécurité et de confiance que la messagerie peut véhiculer.

À titre d'exemple :

- l'authentification interactive est remplacée par une signature électronique authentifiant l'envoyeur et scellant en intégrité le message et ses pièces jointes ;

- le cryptage (chiffrement) de connexion est remplacé par le chiffrement persistant des messages, permettant ainsi de les conserver sous cette forme confidentielle protégée sur la durée. Bien entendu, cette potentialité s'accompagne de nécessaires précautions dans la gestion des clés : si l'utilisateur perd ses clés, il peut être gênant qu'il ne puisse déchiffrer ses anciens e-mails, des systèmes de back up de clés (aussi appelés séquestre et recouvrement de clés) peuvent alors être mis en place.

Ces propriétés ouvrent des possibilités nouvelles à l'utilisation de l'e-mail, non plus seulement comme facilitateur de communication mais comme véritable vecteur de dématérialisation d'échanges sensibles ou engageants. On a pu ainsi observer l'apparition de nouveaux services comme :

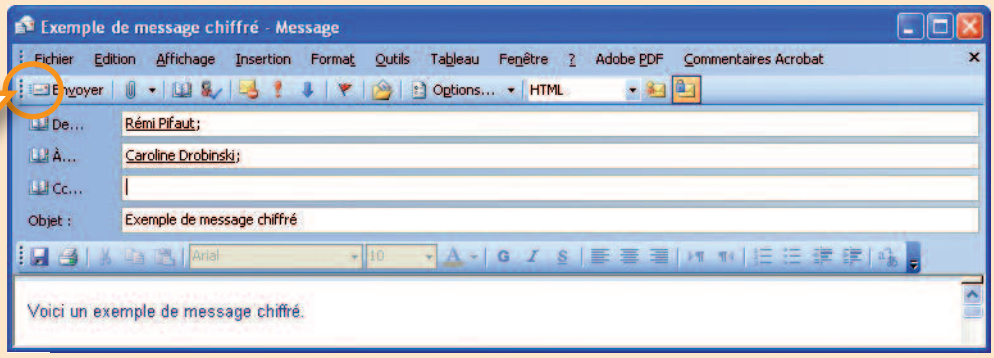
- la soumission électronique d'offres aux marchés publics, protégée en authenticité et en confidentialité ;
- l'échange d'actes administratifs authentiques (par exemple les délibérations communales soumises au contrôle de légalité du préfet) ;
- l'échange d'informations sensibles inter sites dans les entreprises (Pharmacie, Automobile, Aéronautique, Défense) ;
- la transposition en électronique du courrier recommandé avec accusé de réception, aujourd'hui proposé par La Poste et d'autres, et utilisé notamment par les professions du droit (avocats, notaires, greffiers, ...).

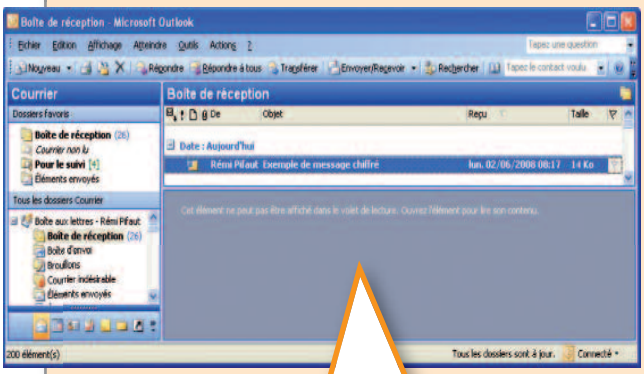
Utilisation de l'e-mail sécurisé : chiffrement, signature

L'émetteur écrit son e-mail puis clique sur l'icône de chiffrement d'e-mail de son logiciel de messagerie.

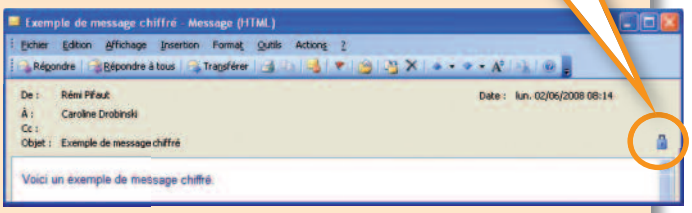
Lors de l'envoi du message, le logiciel de messagerie va demander à utiliser la clé publique contenue dans le certificat du destinataire afin de chiffrer l'e-mail.

L'e-mail est alors chiffré de manière transparente par le logiciel de messagerie de l'émetteur.





Une icône de chiffrement indique simplement que le message a été reçu chiffré.



Lors de la réception de l'e-mail, le destinataire reçoit un e-mail chiffré. Ceci se traduit notamment par le fait que le mail n'est pas lisible en l'état dans la zone de prévisualisation d'Outlook. Pour pouvoir lire l'e-mail, il faut l'ouvrir.

Pour lire le mail, le destinataire doit activer sa clé privée (utilisée pour déchiffrer l'e-mail) pour que le message puisse s'afficher en clair.

En cliquant sur l'icône représentant un cadenas, le destinataire peut avoir des détails sur le chiffrement de l'e-mail et sur le certificat utilisé pour le chiffrement.