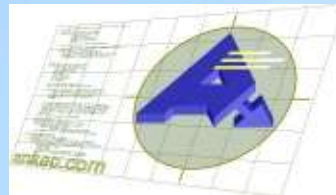


Signature et chiffrement

Jean-Marc Boursot



<http://www.ankeo.com>

© Ankeo 2004 - reproduction interdite

Ankeo

- Société de conseil spécialisée en sécurité informatique et réseau
- Audit, conseil en sécurité
- Firewalls, tests de vulnérabilités, veille technologique, etc.
- Conseil, ingénierie en logiciel libre

Contexte

Echanges par voie informatique: la plupart se font en clair.

- Envoi et retrait du courrier électronique sans aucune sécurité à la base
- Web (sauf web sécurisé)
- FTP, etc.

Pourquoi?

Des problèmes se posent:

- Comment être sûr que mon interlocuteur est bien celui qu'il prétend être et comment est-il sûr que c'est bien moi?
- Comment s'assurer qu'on n'interceptera pas des données sensibles?
- Des données parmi celles que je reçois ont-elles été altérées, modifiées ou perdues?

Quelles solutions?

Augmentation du niveau de sécurité sur les transactions:

- confidentialité des échanges: chiffrement
- identification des acteurs: signature
- intégrité des données: signature et chiffrement

Avec 3 acteurs indispensables: expéditeur, destinataire, tiers certifieur (CA)

Principes de sécurité

« *La sécurité n'est pas un produit mais un processus...* »
(Bruce Schneier - *Counterpane Security*)

Signatures et chiffrement sont des travaux de :

- **prévention et protection**

Eviter les problèmes de données révélées ou falsifiées: elles sont cryptées donc inaccessibles et infalsifiables, elles sont signées donc authentifiées.

- **détection**

La signature dépend des données signées donc permet de détecter une attaque ou une altération.

Éléments annexes

- Penser la sécurité de manière plus globale: à quoi servent des barreaux sur un mur de papier?
- Les mauvais systèmes de chiffrement et de signature.
- La protection de la vie privée?
- Les effets de bords (virus, etc.).
- Un vrai problème: trop peu de gens s'inquiètent de la sécurité

En conclusion

- **Avantages**

- mise en oeuvre facile, rapide et peu coûteuse
- niveau de sécurité élevé
- plusieurs types de signature/chiffrement

- **Inconvénients**

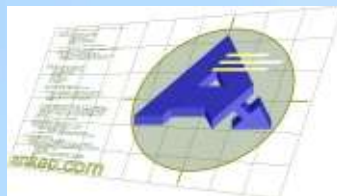
- pas toujours évident à utiliser
- prérequis parfois lourd (PKI)
- accusé de réception, datation

A intégrer dans une politique de sécurité plus large.

On demande plus au monde informatique qu'au monde réel (et on en obtient plus).

Signature et chiffrement

Jean-Marc Boursot



Présentation disponible à l'adresse:
http://www.ankeo.com/res_doc.phtml

© Ankeo 2004 - reproduction interdite