Stage d'application àl'INSA de Rouen

Découvrir la PKI.

Du 22 avril 2002 au 9 août 2002
Cesi Normandie – MSII

José GONÇALVES
Promotion 2001 / 2002

REMERCIEMENTS

Ce stage n'aurait pu se faire sans la volonté et la collaboration de nombreuses personnes. J'exprime ma reconnaissance au personnel de l'Institut National des Sciences Appliquées de Rouen et plus particulièrement à Monsieur Philippe WENDER, responsable du Service Informatique et Réseaux, qui a fait preuve de pédagogie et àPhilippe SAVARY son assistant.

Je tiens aussi à citer Michael BEDIOU (stagiaire TSS Télécommunications et Réseaux) avec qui je m'entendais bien.

Enfin mes derniers remerciements iront à la secrétaire Marie-Claude GAUQUELIN dont la gentillesse n'est plus àdémontrer.

Je remercie chaleureusement ces personnes pour l'aide qu'elles m'ont apportée dans cette démarche rendue possible grâce àleur accueil et leur ouverture.

Résumé à l'attention du lecteur pressé

PKI (Public Key Infrastructure), en français **IGC** (Infrastructure de Gestion de Clés) ou **ICP** (Infrastructure à Clés Publiques) est un système de gestion de clés de chiffrement et de certificats qui constitue un cadre à l'usage des techniques de cryptographie.
Une PKI est donc une structure qui permet de gérer les certificats (l´identité numérique) et les clefs de chiffrement d´un ensemble d´utilisateurs (servant à la signature numérique et au cryptage). C´est une « couche de gestion » qui s´occupe de délivrer les certificats, assure leur valeur et leur validité, et permet à tout le monde d´utiliser la cryptographie.
La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Désormais, la cryptographie sert non seulement à préserver la **confidentialité** des données mais aussi à garantir leur **intégrité**, leur **authenticité** et le caractère **non-répudiable** des documents signés.

Une PKI intègre les moyens techniques et organisationnels pour produire et diffuser les certificats numériques. D'un point de vue organisationnel, elle s'appuie sur une Autorité de Certification, qui émet les certificats, et sur une ou plusieurs Autorités d'Enregistrement, qui valident les demandes de certificats. Il faut souvent y ajouter un serveur de révocation, qui permet de déclarer les certificats révoqués avant leur date d'expiration. Pour obtenir un certificat l'utilisateur adresse sa demande à l'autorité d'enregistrement. Si la demande est complète, conforme à la politique de certification et authentique, alors elle est transmise à l'autorité de certification qui produit le certificat puis transmet ce certificat à l'utilisateur et le publie dans l'annuaire. Si un deuxième utilisateur veut communiquer avec cet utilisateur, alors, il envoie une requête à l'annuaire et reçoit en retour le certificat de la personne qu'il veut contacter. Il contrôle ce certificat grâce à la clé publique de l'autorité de certification déjà en sa possession.

La sécurité de la PKI repose sur la sûreté de deux mécanismes :

- la vérification de l'authenticité de la demande de certificat (l'utilisateur devra certainement se déplacer physiquement pour se faire reconnaître)
- la distribution du certificat contenant la clé privée de l'utilisateur et la distribution initiale du certificat de l'autorité de certification car il permet de vérifier l'authenticité des certificats utilisateurs délivrés (établissement d'une confiance commune à un groupe de certificats).

Dans l'étude suivante « **Découvrir la PKI** » nous verrons que la fiabilité de l'IGC repose sur un cadre juridique qui règle, désormais de façon plus libérale, l'utilisation de la cryptographie. Nous verrons aussi que loin de s'attacher à un éditeur de logiciels chacun peut, grâce au Logiciel Libre, mettre en place son infrastructure privée. Nous comprendrons également que la PKI ne se substitue pas à la sécurité informatique mais en est un élément supplémentaire.

SOMMAIRE

ILLUSTRATIONS

TABLES