République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre de Recherche en Information Scientifique et Technique

Mémoire en vue de l'obtention du diplôme de
Post-Graduation Spécialisée en Sécurité Informatique

Thème

Conception et Déploiement d'une PKI pour sécuriser la messagerie électronique

Réalisé par:

- HADDADJI Samir
- MEHADA Issam

Encadré par :

- Dr. NOUALI Omar

Soutenu devant le juré composé de :

- Dr. BESSAI Fatma Zohra	Maitre de Recherche, CERIST	Présidente
- Mr. KHOUATMI Fouad	Attaché de Recherche, CERIST	Examinateur
- Mr. SAIDI Ahmed	Chargé d' Etudes, CERIST	Examinateur

-Promotion 2012/2013-

Remerciements

Nous remercions, en premier lieu, Dieu le tout puissant de nous avoir donné le courage et la puissance pour terminer ce travail.

Nous exprimons nos profonds remerciements et reconnaissances à **Monsieur NOUALI Omar** pour les nombreux conseils et orientations qui nous ont été très précieux au cours de la réalisation de ce travail.

Un merci tout particulier aux **membres de jury** d'avoir accepté de juger notre travail et nous avoir honoré par leur présence et pour nos enseignants de la PGS pour nous avoir enseigné, aidé et dirigé tout au long de cette formation.

Nous tenons à remercier nos responsables en l'occurrence **Mr. MALEK Lounes** et **Mr.MAAKOUF Zineddine** pour nous avoir donné l'occasion de suivre cette formation.

En fin, que tous ceux qui ont, de près ou de loin, contribué à l'élaboration de ce travail, particulièrement Messieurs : **GUERGUER Samir**, **MOKHTARI Hamid**, **SELMANI Haider**, **BOUCHAREB Farid**, **BOUKRICHE Mohamed-Amine**, **SADOUNE Ahmed**, **BOUKHOBZA Brahim**, **NIAR Hocine**, **DAHRIB Hakim, HADDAD Sofiane** et **TAFAT Adel**, trouvent ici l'expression de notre profonde reconnaissance.

Dédicaces

A mes chers parents qui ont sacrifié pour m'instruire, pour leur amour et leur soutien, c'est grâce à eux que Je suis devenu ce que je suis, à ceux que j'aime, particulièrement mes sœurs et frères, mon épouse et mes deux enfants Razane et Abderrahmane, je dédie ce modeste travail.

Samir

Dédicaces

A mes chers parents qui ont souffert pour m'éduquer et qui ont sacrifié pour m'instruire, c'est grâce à eux que je suis devenu ce que je suis. A ceux que j'aime, mon frère Sami et ma femme, je dédie ce modeste travail.

Issam

Résumé

La messagerie électronique est un moyen moderne d'échange d'informations offrant la possibilité d'augmenter la rapidité des communications, de diffuser massivement des informations, d'éliminer des opérations de paperasserie, par ailleurs la mise en œuvre d'une politique de protection de ce système est primordiale pour faire face aux multiples risques de sécurité des messages échangés.

L'exploitation des outils de cryptographie garantit les deux aspects de la sécurité des messages électroniques, à savoir, la confidentialité et l'intégrité, les deux autres aspects, à savoir, l'authenticité et la non-répudiation, nécessitent l'instauration d'une confiance au sein du système de messagerie à travers l'implication d'une tierce partie garantissant la correspondance et la concordance entre une identité électronique et l'identité réelle.

Une infrastructure PKI (Public Key Infrastructure) est la méthode la plus adaptée pour instaurer cette confiance et assure la sécurité des communications lors de l'échange de messages électroniques.

Microsoft Windows server permet l'intégration d'une PKI supportant les algorithmes et les outils cryptographiques les plus solides à l'aide de son service AD CS (Active Directory Certificate Services) et liant l'identité d'un utilisateur, d'un périphérique ou d'un service à une clé correspondante.

Sommaire

III. Conception de la PKI

IV. Mise en œuvre de la PKI