الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي - 08 ماي 1945 – بسيدي بلعباس
Ecole Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbes

MEMOIRE

En vue de l'obtention du diplôme d'**ingénieur d'état**

Filière : **Informatique**

Spécialité : **Ingénierie des Systèmes Informatiques (ISI)**

Thème

Implémentation d'un schéma de Signature électronique

Présenté par **:**

- Mlle ROUANE Amina Wafa
- Mlle HARRIR Naima

Soutenu le : **25/07/2019** Devant le jury composé de :

- M Feraoun Mohamed Kamel	Président
- Mme ANANI Djihed	Encadreur
- M Meddah Ishak Hibat Allah	Examinateur
- Mme Souyah Amina	Examinateur

Abstract

Every day in the world, billions of people exchange billions of digital documents, whether professional or private; but how many of them really engage their authors?

In fact: much less, and this is normal because the need to engage is justified when the documents have a value, whether financial, legal or sentimental. Indeed, to sign is to engage, to affirm one's identity in a chosen context.

Beyond the now widely used technical act, the electronic signature is a strong act that seals an agreement and relates to the digital identity of the signer (s). It is this strong link between the document and the natural or legal person that gives value to the document and establishes a relationship of trust between the parties who exchange the signed documents.

To be able to use this e-signature it is necessary to improve security by guaranteeing the following security pillars: authentication, confidentiality, integrity and non-repudiation.

The PKI (Public Key Infrastructure) presents an adequate solution addressing all these security functions and meeting the needs of organizations.

A PKI public key infrastructure is a set of procedures, physical and software components, used in the management of electronic certificates, these certificates allow to perform operations such as encryption and e-signature, the objective being to guarantee the confidentiality, authentication, non-repudiation and integrity of information.

In this thesis, we will present generalities on computer security and cryptography then we treat the public key infrastructure PKI and its policies that govern it and also we deal with the mechanism of signing and electronic verification, then we present some literature works that are interested in securing electronic transactions, and in the end we will implement a PKI and develop our solution called "WAQIE" which represents an application to exploit the PKI and secure the electronic exchanges within the company.

Keywords: Security, Electronic Transactions, Electronic Signature, PKI.

Résumé

Chaque jour dans le monde, des milliards de personnes échangent des milliards de documents numériques, qu'ils soient professionnels ou privés ; mais combien d'entre eux engagent vraiment leurs auteurs ?

En fait : nettement moins, et c'est bien normal car le besoin de s'engager se justifie lorsque les documents ont une valeur, qu'elle soit financière, juridique ou sentimentale. En effet, signer c'est s'engager, c'est affirmer son identité dans un contexte choisi.

Bien au-delà de l'acte technique désormais largement répandu, la signature électronique est un acte fort qui scelle un accord et liée à l'identité numérique du (des) signataire(s). C'est ce lien fort entre le document et la personne physique ou morale qui donne la valeur à l'acte et permet d'établir une relation de confiance entre les parties qui échangent les documents signés.

Pour pouvoir utiliser cette signature il faut une amélioration de la sécurité en garantissant les piliers de sécurité suivants : l'authentification, la confidentialité, l'intégrité et la non-répudiation.

La PKI (Public Key Infrastructure) présente une solution adéquate adressant toutes ces fonctions de sécurité et répond aux besoins des organisations.

Une infrastructure à clé publique PKI est un ensemble de procédures et de composants physiques et logiciels, utilisés dans la gestion des certificats électroniques, ces certificats permettent d'effectuer des opérations telles que le chiffrement et la signature électronique, l'objectif étant de garantir la confidentialité, l'authentification, la non répudiation et l'intégrité des informations.

Dans le cadre de notre mémoire nous allons présenter des généralités sur la sécurité en informatique et la cryptographie puis on traite l'infrastructure à clé publique PKI et aussi on traite le mécanisme de la signature et la vérification électronique, puis nous présentons des travaux de la littérature qui sont intéressés à la sécurisation des transactions électronique, et à la fin nous allons implémenter une PKI et développer notre solution appelée "WAQIE" qui représente une application pour exploiter la PKI et sécuriser les échanges électroniques au sein de l'entreprise.

Mots clés : *Sécurité, transactions électronique, Signature électronique, PKI.*