

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



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

Thème

LA SECURITE DES ECHANGES DE
DONNEES XML
(IMPLEMENTATION DE LA SIGNATURE NUMERIQUE
XML POUR UN FORMULAIRE EN LIGNE)

Elaboré par :

- BOUMARAF Ahmed.
- DAOUADI Dhiaeddine.

Encadré par :

- Mr. Dr NOUALI Omar.

- Mr DERHAB.A,
- Melle CHALLAL.Z,
- Mr KRINAH. A ,

Maître de Recherche A, CERIST
Attachée de Recherche, CERIST.
Chargé d'études, CERIST.

Président
Examineur
Examineur

-Décembre 2011-

Remerciements

Ce mémoire est le fruit d'un travail acharné au sein du CERIST et comme un tel travail nécessite la contribution de plusieurs personnes, nous profitons de cette occasion pour les remercier à travers ces quelques phrases.

Nous exprimons notre profonde gratitude au Directeur du CERIST et tous le staff technique du centre.

Nous tenons à remercier notre promoteur Monsieur NOUALI OMAR pour la confiance qu'il nous a témoigné en nous proposant ce sujet, sa disponibilité tout au long du projet, ses encouragements et sa patience. Les discussions scientifiques qu'il a su générer, ses remarques et ses suggestions nous ont permis de finaliser ce document..

Nous exprimons toute notre profonde gratitude et nous les remercions pour le personnel du service formation du CERIST.

Nous remercions les membres du jury pour avoir bien voulu juger notre travail.

SOMMAIRE

Résumé	
Introduction Générale.....	1

Chapitre 1 : Langage XML

1. Introduction.....	4
2. Présentation du XML.....	4
3. Structure d'un document XML.....	6
4. Document Type Definition.....	7
5. Parseurs.....	9
6. Avantages de XML.....	10

Chapitre 2: Signature Numérique

1. Introduction.....	11
2. Présentation de la signature numérique.....	11
2.1. Définition de la signature numérique.....	11
2.2. Propriétés de la signature numérique.....	12
2.2. 1. Authentification.....	12
2.2. 2. Intégrité.....	12
2.2. 3. Non répudiation.....	12
3. Principe cryptographique de la signature.....	13
3.1. Cryptographie à clé secrète.....	13
3.2. Cryptographie à clé publique.....	14
3.3. Fonction de hachage.....	15
3.4. Principe de la signature numérique.....	16
4. Certificat numérique.....	18
4.1. Présentation des certificats de clés publiques.....	18
4.1.1. Types de certificats.....	18
4.1.2. Normes et standards.....	19
4.1.3. Support Physique.....	19
4.2. Infrastructure à clé publique.....	20
4.2.1. Composantes de la PKI.....	18
4.2.2. Services offerts par la PKI.....	18
4.3. Applications de la signature électronique.....	25

Chapitre 3: Signature XML

1. Introduction.....	27
2. Structure de la signature XML.....	27
2.1. Élément <SignedInfo>.....	28
2.2. Élément <SignatureValue>.....	29
2.3. Élément <KeyInfo>.....	29
2.4. Élément <Object>.....	29
3. Types de signatures.....	30
3.1. Signature enveloppante.....	30
3.2. Signature enveloppée.....	30

3.3. Signature détachée	31
4. Format de la signature XML.....	32
4.1. XMLDsig.....	32
4.2. Signature électronique avancée en XML (XADES)	33
5. Signatures Multiples.....	37
5.1. Co-Signature.....	37
5.2. Contre -Signature.....	37

Chapitre 4: Implémentation

1. Introduction.....	38
2. Application de signature de formulaire.....	38
2.1. Contexte de l'application	38
2.2. Scénario de l'application.....	39
3. Environnement de développement.....	41
4. Java API XML Digital Signature.....	42
5. Applet Java pour génération de XML Digital Signature	43
5.1. Avantages des Applets.....	44
5.2. Les droits des applets	44
5.3. Applet formulaire	45
5.3.1. Processus de signature.....	46
5.3.2. Processus de validation de la signature	51
6. Environnement matériel.....	52
7. Développement des composantes fonctionnelles.....	53
7.1. Composante gérant l'interaction avec le signataire	53
7.1. 1. Exprimer son consentement à signer.....	53
7.1. 2. Introduction de la clé de signature	54
7.1. 3. Interrompre le processus de création de signature	54
7.2. Composante de génération de la signature XML.....	55
7.2.1. La génération de l'élément <Reference>	55
7.2.2. La génération de l'élément <SignatureValue>	55
7.3. Composantes de d'envoi de la signature	56
7.4. Les composantes de vérification de la signature.....	56
8. Interaction client Serveur	57
Conclusion générale.....	59
Bibliographie	