

République Algérienne Démocratique et Populaire

**MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE  
LA RECHERCHE SCIENTIFIQUE**

**CENTRE DE RECHERCHE SUR L'INFORMATION  
SCIENTIFIQUE ET TECHNIQUE**



Mémoire:

Pour l'obtention du diplôme de poste graduation spécialisé en  
sécurité informatique

Thème:

**Conception et réalisation d'un  
système de signature d'un document  
XML**

**Réalisé par :**

Mr KHEDROUCHE Farid

Mr OUNASSI Abdelhakim

**Encadré par :**

Mme BESSAI F.Z

Devant le jury: Mr NOUALI Omar

Président

Mme BENMEZIANE Souad Membre

Mme NOUALI Nedja Membre

**Décembre 2007**

## Sommaire

<b>Introduction Générale.....</b>	<b>6</b>
<b>Chapitre I : Le document XML.....</b>	<b>7</b>
I. Introduction.....	7
II. Eléments d'un document XML.....	7
II.1. Balisage .....	7
II.2. Les attributs .....	8
II.3. Les instructions de traitement.....	9
II.4. Les commentaires :.....	9
II.5. Les entités .....	9
III. Structure d'un document XML .....	10
III.1. En-tête .....	10
III.2. La racine.....	11
IV. Règles de mises en œuvre des balises .....	11
V. Exemple de structure simple .....	12
VI. La DTD (Document Type Définition) .....	12
VI.1. Limitations des DTD .....	13
VII. Les schémas XML.....	13
VIII. Mise en forme à l'aide de feuilles de style XSL (XSLT).....	14
IX. Les parseurs.....	14
<b>Chapitre II : La signature électronique .....</b>	<b>16</b>
I. Principe de la signature électronique .....	16
I.1. Algorithmes asymétriques.....	16
I.2. Fonction de hachage .....	17
II. Construction et vérification d'une signature.....	17
III. Horodatage .....	18

IV. Normes et standards .....	19
IV.1. XML Signature .....	20
IV.2. XML Advanced Electronic Signatures (XAdES) .....	20
<b>Chapitre III : La signature XML.....</b>	<b>21</b>
I. Introduction .....	21
II. Le W3C (World Wide Web Consortium) .....	22
II.1. Les Outils de Cryptage du W3C .....	22
III. XML signature .....	22
III.1. La spécification XML Signature.....	23
III.2. Fonctionnalités de XML Signature .....	23
IV. Présentation de concepts généraux.....	24
IV.1. Fonction de hachage et cryptographie à clé publique.....	24
IV.1.1. Hachage.....	24
IV.1.2. Chiffrement .....	25
IV.1.3. Vérification .....	25
V. Les algorithmes .....	26
V.1. Les algorithmes de hachage .....	26
V.2. Les algorithmes de chiffrement.....	27
VI. Certificats digitaux .....	27
VII. Types de signatures XML .....	28
VIII. Canonisation .....	30
IX. Algorithme Base64.....	30
X. La structure de la signature XML .....	31
XI. Syntaxe et traitement des signatures XML .....	32
XI.1. Introduction.....	32
XI.2. Syntaxe des signatures XML .....	32
XI.3. Les règles de traitements .....	38

XI.3.1. La génération principale.....	38
XI.3.2. La validation principale .....	39
XI.4. Les identifiants d'algorithmes et les exigences d'implémentation.....	40

## **Chapitre IV : Conception et réalisation d'un système de signature de documents XML.. 43**

I. Conception .....	43
I.1. La Canonicalization.....	43
I.2. La transformation .....	45
I.3. La production de la signature XML.....	47
II. Réalisation du système .....	49
II.1. Les clés .....	49
II.2. Exemple illustratif .....	51
II.3. Génération des trois types de signatures.....	51
II.3.1. Signature enveloppée.....	52
II.3.2. Signature enveloppante.....	54
II.3.3. La signature détachée .....	56
II.4. Signature d'une partie du document .....	57
II.5. Vérification de la signature.....	59
III. L'interface graphique .....	61
III.1. La signature : .....	62
III.2. La vérification de la signature .....	63
III.3. La gestion des clés .....	65
<b>Conclusion Générale .....</b>	<b>67</b>
<b>Bibliographie.....</b>	<b>69</b>
<b>Annexe .....</b>	<b>71</b>