



République Algérienne Démocratique et Populaire  
HIGHER INTERNATIONAL MANAGEMENT INSTITUT  
( HIMI )  
CENTRE DE RECHERCHE SUR L'INFORMATION SCIENTIFIQUE ET  
TECHNIQUE

Mémoire en vue de  
l'obtention du diplôme  
D'Ingénieur en Informatique

THEME

Conception et réalisation d'un système de  
signature XML

Etudié par :  
Mr BENHAMOUDA Hocine  
Mr MOUSSACEB Mohamed Amine

Promoteur :  
Mme BESSAI F/Zohra

ENCADREUR:  
Mr ZOUAOUI Hocine

Organisme d'accueil: CERIST

PROMOTION : 2007 / 2008



Introduction générale.....	2
----------------------------	---

## Présentation de l'organisme d'accueil

### CERIST en bref

1. Historique.....	3
2. Mission.....	3
3. Organisation de CERIST.....	4

## CHAPITRE I : Sécurité informatique et cryptographie

I.1 Introduction.....	5
I.2 Objectif de la sécurité informatique.....	5
I.2.1 Confidentialité.....	6
I.2.2 Intégrité.....	6
I.2.3 Disponibilité.....	6
I.3 Vulnérabilités, menaces et contre-mesures.....	8
I.3.1 Vulnérabilités.....	8
I.3.2 Type de menace.....	8
I.3.3 Contre-mesures.....	9
I.3.4 Exemple de menaces et vulnérabilités.....	9
I.3.5 Exemple de contre-mesures.....	10
I.4 Mécanisme de sécurité.....	12
I.4.1 Contrôle d'accès.....	12
I.4.2 Cryptographie.....	13
I.4.2.1 Chiffrement.....	13
a. Chiffrement symétrique.....	14
b. Chiffrement asymétrique.....	14
I.4.2.2 Fonction de Hachage.....	15
I.4.2.3 Authentification de l'origine des données et MAC.....	16
I.4.2.4 Signature numérique.....	16
I.4.2.5 Infrastructure à clé publique PKI.....	17
I.4.2.6 Algorithmes de cryptographie et de hachage.....	19
a. Data Encryption Standard (DES).....	19
b. Digital Signature Algorithm (DSA).....	20
c. Rivest Shamir Adelman (RSA).....	20
d. Fonction de hachage MD5.....	22
e. Fonction de hachage SHA-1.....	23
I.5 Conclusion.....	23

## CHAPITRE II : le Langage XML (eXtensible Markup Language)

II.1 Introduction.....	25
II.2 Avantage et raison du succès du langage XML.....	26
II.3 Objectif du langage XML.....	28
II.4 Description des Document XML.....	29
II.4.1 Structure d'un document XML.....	29
II.4.1.1 Anatomie d'un document XML.....	29
II.4.1.2 Balises, Eléments et Attributs.....	30
II.4.2 Règles syntaxique.....	31

II.4.3 Document bien formé et document valide.....	31
II.4.3.1 Document bien formé.....	31
II.4.3.2 Document valide.....	32
II.4.4 Arbre XML.....	32
II.4.5 Affichage de document XML.....	32
II.4.5.1 La liaison à des feuilles de styles.....	32
II.4.5.2 La liaison de données.....	33
II.4.5.3 Les scriptes.....	33
II.5 Document type définition et W3C XML Schéma.....	33
II.5.1 Document type définition.....	33
II.5.2 W3C XML Schéma.....	33
II.6 Conclusion.....	34

### CHAPITRE III : Signature XML

III.1 Introduction.....	35
III.2 Présentation de la signature XML.....	35
III.3 Forme d'une signature XML.....	39
III.3.1 Signature enveloppée.....	39
III.3.2 Signature enveloppante.....	39
III.3.3 Signature détachée.....	40
III.4 Les règles de traitements.....	40
III.4.1 Définition des transformations.....	40
III.4.2 Définition de la canonicalization.....	41
III.4.3 Génération de la signature.....	42
III.4.3.1 Génération de la référence.....	45
III.4.3.2 Génération de la signature.....	45
III.4.4 Vérification de la signature.....	46
III.4.4.1 Vérification de la référence.....	46
III.4.4.2 Vérification de la signature.....	46
III.5 Syntaxe de la structure de la signature.....	47
a. L'élément Signature.....	47
b. L'élément SignatureValue.....	47
c. L'élément SinedInfo.....	48
d. L'élément KeyInfo.....	50
e. L'élément Object.....	52
III.6 Conclusion.....	53

### CHAPITRE IV: Conception d'un système de signature XML

IV.1 Introduction.....	55
IV.2 Architecture globale du système.....	56
IV.2.1 Description de l'architecture du système.....	56
IV.2.2 Détermination des cas d'utilisation du système.....	58
IV.2.3 Diagramme des cas d'utilisation.....	59
IV.2.4 Description de l'interface graphique.....	60
IV.2.5 Description de l'interaction entre le système de l'interface graphique.....	61
IV.2.6 Description des modules et fonctionnalités du système.....	64
IV.2.6.1 Déroulement des cas d'utilisation.....	65
IV.2.6.2 Etapes d'assemblage et de génération de la signature.....	74

a. Assemblage de la signature.....	74
b. Les étapes de création de l'élément SigneInfo pour les trois types de signature...	74
c. Les étapes de création de KeyInfo.....	77
d. Génération principale de la signature.....	77
IV.2.6.3 Processus de vérification de la signature.....	78
IV.3 Conclusion.....	79

## CHAPITRE V: Réalisation d'un système de signature XML

V.1 Introduction.....	80
V.2. Description des API et outils utilisés.....	81
V.2.1 Présentation de l'API JSR 105.....	81
V.2.2 Présentation de l'utilitaire JAVA pour la création de clé et certificat « KeyTool ».....	82
V.2.3 Présentation de la bibliothèque Swing.....	84
V.3 Présentation des modules du système.....	85
V.3.1 Module signature.....	85
V.3.1.1 Classe Fonction.....	85
V.3.1.2 Classe SignatureDétachée.....	86
V.3.1.3 Classe SignatureEnveloppée.....	88
V.3.1.4 Classe SignatureEnveloppante.....	89
V.3.1.5 Liste des packages utilisés dans le module signature.....	89
V.3.1.6 Gestion des exceptions de la classe Fonction.....	90
V.3.2 Module vérification.....	90
V.3.2.1 Classe X509KeySelector.....	90
V.3.2.2 Classe VérifierSignature.....	90
V.3.2.3 Liste des packages utilisés dans le module vérification.....	91
V.3.2.4 Gestion des exceptions du module vérification.....	91
V.3.3 Le module générer Certificat.....	91
V.4 Présentation de l'interface graphique.....	91
V.4.1 La Classe Application.....	91
V.4.2 La Classe View.....	92
V.4.3 La Classe SignatureGUI.....	93
V.4.4 La Classe VérificationGUI.....	94
V.4.5 La Classe KeyToomGUI.....	95
V.4.6 La Classe SigneElementGUI.....	96
V.4.7 Fonctionnement des interfaces.....	97
V.4.8 Gestion des exceptions.....	97
V.5 Conclusion.....	98
Conclusion Générale.....	99
Bibliographie	
Annexe A	
Annexe B	
Annexe C	
Annexe D	
Annexe E	