

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre de Recherche sur l'Information Scientifique et Technique



*Mémoire pour l'obtention du diplôme de
Post Graduation Spécialisée en sécurité informatique*

Thème

Paiement électronique sécurisé Cas des achats sur Internet

Présenté par :

Mr. CHAIBI Abdelhamid

Mr. HADJ MOUSSA El-Hadj

Encadré par :

Dr. NOUALI Omar

Membres de jury :

Dr. TANDJAOUI Djamel

Président

Mme. BENMEZIANE Souad

Examineur

Melle. BENSALIA Hassina

Examineur

Promotion 2005-2006

Résumé

Dans ce mémoire, sont présentées les solutions les plus représentatives en matière de commerce électronique et de paiement sécurisé sur Internet. Une classification des moyens de paiement électronique est présentée : la carte bancaire, le chèque électronique et la monnaie électronique. Les différents protocoles de sécurité pour le paiement électronique sont ensuite détaillés (SSL, iKP, SET, 3D-Secure, SPA/UCAF).

Une solution de paiement sécurisé, permettant des achats en ligne, pour un site Web de e-commerce et finalement présentée.

Abstract

In this dissertation, the most significant solutions for electronic commerce and secure payment on Internet are presented. A typology to classify electronic payment systems is presented: the bank card, electronic check and electronic money. Then, the different protocols of electronic payment are detailed (SSL, iKP, SET, 3D-Secure, SPA/UCAF).

A secure payment solution, which allows a shopping online, for Web site of e-commerce, is presented.

Sommaire

Liste des figures	viii
Liste des tableaux	ix
Liste d'abréviations	x
Préface	01
Introduction	02
Chapitre I : Commerce électronique	03
1. Formes de commerce électronique	03
1.1. Livraison Offline	03
1.2. Livraison Online	03
2. Sécurité et commerce électronique	04
3. Paiement électronique	04
4. Caractéristiques d'un mécanisme de paiement électronique	05
Chapitre II : Techniques cryptographiques	10
1. Chiffrement symétrique	10
1.1. Data Encryption Standard	11
1.2. Triple DES	11
1.3. IDEA	11
1.4. Advanced Encryption Standard	12
1.5. RC4	12
2. Chiffrement asymétrique	13
2.1. Diffie – Hellman	13
2.2. RSA	14
3. Modes de chiffrement	14
4. Fonctions de hachage	15
4.1. MD5	15
4.2. SHA1	15
5. Signatures numériques	15
6. Code d'authentification des messages	16
7. PKI	17
7.1. Entités d'une PKI	17
7.2. Organisation d'une PKI	18
Chapitre III : Modes de paiement électronique	19
1. Systèmes de paiement par cartes	19
1.1. Carte magnétique	19
1.2. Carte à puce	20
1.3. Paiement par carte	21
1.3.1. Carte de débit	21
1.3.2. Carte de crédit	22
1.3.3. Carte de crédit EMV	22

Liste des figures	viii
Liste des tableaux	ix
Liste d'abréviations	x
Préface	01
Introduction	02
Chapitre I : Commerce électronique	03
1. Formes de commerce électronique	03
1.1. Livraison Offline	03
1.2. Livraison Online	03
2. Sécurité et commerce électronique	04
3. Paiement électronique	04
4. Caractéristiques d'un mécanisme de paiement électronique	05
Chapitre II : Techniques cryptographiques	10
1. Chiffrement symétrique	10
1.1. Data Encryption Standard	11
1.2. Triple DES	11
1.3. IDEA	11
1.4. Advanced Encryption Standard	12
1.5. RC4	12
2. Chiffrement asymétrique	13
2.1. Diffie – Hellman	13
2.2. RSA	14
3. Modes de chiffrement	14
4. Fonctions de hachage	15
4.1. MD5	15
4.2. SHA1	15
5. Signatures numériques	15
6. Code d'authentification des messages	16
7. PKI	17
7.1. Entités d'une PKI	17
7.2. Organisation d'une PKI	18
Chapitre III : Modes de paiement électronique	19
1. Systèmes de paiement par cartes	19
1.1. Carte magnétique	19
1.2. Carte à puce	20
1.3. Paiement par carte	21
1.3.1. Carte de débit	21
1.3.2. Carte de crédit	22
1.3.3. Carte de crédit EMV	22

Chapitre V : Cas pratique - Achat sur Internet	59
1. Etude de l'application	59
1.1. Environnement de l'application	59
1.2. Description de l'application	59
1.2.1. Mode anonyme	60
1.2.2. Mode utilisateur	60
1.3. Tâches à sécuriser	63
1.4. Servlet	64
1.5. Tomcat	64
1.5.1. Statut de développement	65
1.5.2. Installation	65
1.5.3. Arborescence des répertoires	65
1.5.4. Arborescence des sous répertoires du répertoire webapps	66
1.5.5. Fichiers de configuration	66
1.5.5.1. Le fichier <i>Server.xml</i>	66
1.5.5.2. Le descripteur de déploiement (<i>web.xml</i>)	66
1.5.5.3. Le fichier <i>tomcat-users.xml</i>	67
2. Choix du mode de paiement	67
2.1. Porte monnaie virtuelle	67
2.2. Caractéristiques de la solution	68
3. Choix du protocole de sécurité	68
4. Implémentation du protocole de sécurité	69
4.1. Architecture de l'application web	69
4.2. Configuration de l'application	70
4.2.1. Déclaration des servlets	70
4.2.2. Association des servlets à des URLs	71
4.2.3. Implémentation des contraintes de sécurité	72
4.2.3.1. Authentification des utilisateurs	72
4.2.3.2. Transport sécurisé des données	73
4.3. Configuration de SSL dans Tomcat	74
4.3.1. Outil Keytool	74
4.3.2. Génération d'un certificat auto-signé RSA	77
4.3.3. Activation du protocole SSL dans Tomcat	79
5. Règles supplémentaires de sécurité	83
 Conclusion et perspectives	 85
 Bibliographie	 86