

Mostafa Hashem Sherif  
Ahmed Serhrouchni

commerce électronique

# La monnaie électronique

Systemes de paiement sécurisé

- ▶ La monnaie et les instruments de paiement
- ▶ Algorithmes de cryptage
- ▶ Protocoles SSL et SET
- ▶ Solutions de micropaiement
- ▶ Porte-monnaie électroniques et virtuels
- ▶ Sécurisation des cartes à puce

[www.editions-eyrolles.com](http://www.editions-eyrolles.com)

- ▶ Poursuivez votre lecture sur le web
- ▶ Consultez les mises à jour et compléments
- ▶ Dialoguez avec les auteurs

**E** Eyrolles

# Table des matières

<b>AVANT-PROPOS</b> .....	1
---------------------------	---

## **CHAPITRE 1 : QU'EST-CE QUE LE COMMERCE ÉLECTRONIQUE ?** ..... 3

<b>Définition et catégories du commerce électronique</b> .....	3
<b>Exemples d'applications</b> .....	4
Dans le commerce interentreprise .....	4
Dans le commerce grand public .....	5
Dans le commerce de proximité et de paiement sur automate.....	7
<b>Le cadre du commerce électronique</b> .....	7
Les banques.....	9
Clients .....	10
Fournisseurs .....	10
Nouveaux entrants et substituts.....	10
<b>Caractéristiques des systèmes de paiement dématérialisés</b> .....	11
<b>L'effet « Internet »</b> .....	13
<b>Technologies du commerce électronique</b> .....	17
Accès au réseau .....	17
Traitement informatique.....	22

## **CHAPITRE 2 : LA MONNAIE ET LES SYSTÈMES DE PAIEMENT** ..... 25

<b>Les mécanismes des monnaies classiques</b> .....	25
<b>Les instruments de paiement</b> .....	27
Espèces.....	29
Chèques.....	31
Virements.....	34
Avis de prélèvement.....	37
Titres interbancaires de paiement.....	39
Les effets de commerce.....	39
Les cartes de paiement .....	39
<b>Les systèmes de compensation bancaire</b> .....	42
États-Unis.....	43

Royaume-Uni.....	44
France.....	45
<b>Les monnaies et les instruments de paiement dématérialisés.....</b>	<b>46</b>
La monnaie électronique.....	46
La monnaie virtuelle.....	47
La monnaie numérique.....	48
Porte-monnaie et porte-jeton électroniques.....	48
Porte-monnaie et porte-jeton virtuels.....	49
Propriétés transactionnelles des monnaies dématérialisées.....	50
<b>Comparaison entre les instruments de paiement.....</b>	<b>53</b>
<b>Pratique de la monnaie dématérialisée.....</b>	<b>55</b>
Protocoles des systèmes de monnaie dématérialisée.....	55
Paiement direct au commerçant.....	58
Paiement via un intermédiaire.....	60
<b>Conclusion.....</b>	<b>62</b>

**CHAPITRE 3 : ARCHITECTURE ET ALGORITHMES DE SÉCURISATION..... 65**

<b>Sécurité des réseaux financiers ouverts.....</b>	<b>66</b>
<b>Modèle OSI de sécurisation cryptographique.....</b>	<b>68</b>
Le modèle de référence OSI.....	68
Services de sécurisation : définitions et emplacement.....	69
Services de sécurité de la couche réseau.....	70
<b>Réalisation des services de sécurité.....</b>	<b>72</b>
La confidentialité des messages.....	72
L'intégrité des données.....	75
L'identification des participants.....	83
L'authentification des participants.....	84
Non-répudiation.....	85
<b>Gestion des clés.....</b>	<b>86</b>
Contraintes de la sécurisation des clés.....	87
Échange de clés secrètes : Kerberos.....	89
Échange de clés publiques.....	92
<b>Gestion des certificats.....</b>	<b>94</b>
Description d'un certificat X.509.....	96
Itinéraire de certification.....	98
Procédures d'identification poussée.....	106
Révocation des certificats.....	108
Service de sécurité et citoyenneté.....	109
Exemple.....	110
<b>Lézardes des services de sécurisation.....</b>	<b>113</b>
<b>Annexe I : Notions de chiffrement symétrique.....</b>	<b>115</b>
Modes d'utilisation des algorithmes en bloc.....	115
Le DES.....	121
Triple DES.....	121
IDEA.....	122
AES.....	122
<b>Annexe II : Notions de chiffrement asymétrique.....</b>	<b>123</b>
RSA.....	123
Les standards PKCS.....	124

PGP .....	125
<b>Annexe III : Données comparatives .....</b>	<b>126</b>
Performance pour JSAFE 1.1 .....	126
Performance avec S/WAN .....	127
Performance avec BSAFE™ 3.0 .....	129
Performance pour BSAFE™ 4.1 .....	132
<hr/>	
<b>CHAPITRE 4 : LE COMMERCE INTERENTREPRISE ET L'EDI .....</b>	<b>133</b>
<hr/>	
<b>Composantes l'EDI .....</b>	<b>134</b>
Génération et réception des données structurées .....	136
Gestion de la diffusion .....	137
Gestion de la sécurité .....	138
<b>Exemples de systèmes EDI .....</b>	<b>138</b>
<b>Structuration alphanumérique des données .....</b>	<b>141</b>
ANSI X12 .....	142
EDIFACT .....	144
Comparaison structurelle entre EDIFACT et X12 .....	150
<b>Structuration de documents ou formulaires .....</b>	<b>151</b>
SGML .....	152
XML .....	153
Interface de XML avec l'EDI traditionnel .....	153
<b>Messageries de l'EDI .....</b>	<b>156</b>
X.400 .....	156
Internet (SMTP/MIME) .....	158
<b>Sécurisation de l'EDI .....</b>	<b>159</b>
Sécurisation de X12 .....	159
Sécurisation de l'EDIFACT .....	161
Propositions de l'IETF .....	168
Empilements protocolaire pour l'EDI .....	172
Interopérabilité de l'EDI sécurisé avec le protocole S/MIME .....	173
<b>Relation entre l'EDI et les virements bancaires (transferts électroniques de fonds) ..</b>	<b>174</b>
Virements par EDIFACT .....	178
Virements par X12 .....	179
<b>Intégration de l'EDI dans les processus .....</b>	<b>179</b>
<b>Normalisation de l'EDI .....</b>	<b>182</b>
<b>Évolution de l'EDI .....</b>	<b>184</b>
<hr/>	
<b>CHAPITRE 5 : LES PREMIERS TÉLÉPAIEMENTS PAR CARTE BANCAIRE ..</b>	<b>187</b>
<hr/>	
<b>Sécurisation sans cryptage : First Virtual .....</b>	<b>187</b>
Architecture du système .....	188
Inscription .....	188
Protocole d'achat .....	189
Compensation et acquisition .....	190
Sécurisation .....	190
Évaluation .....	191
<b>Les protocoles iKP .....</b>	<b>191</b>
Le protocole 1KP .....	194
Le protocole 2KP .....	197
Le protocole 3KP .....	199

<b>CyberCash</b> .....	200
Inscription .....	201
Achat par carte de crédit .....	201
Achat par carte de débit .....	202
Sécurisation .....	204
<b>Agora</b> .....	204
Inscription .....	204
Achat .....	204
Évaluation .....	208

## **CHAPITRE 6 : SÉCURISATION DES TÉLÉPAIEMENTS AVEC SSL** ..... 209

<b>Architecture</b> .....	209
<b>Les services de sécurisation de SSL</b> .....	212
L'authentification .....	212
La confidentialité .....	212
L'intégrité .....	213
<b>Les sous-protocoles de SSL</b> .....	213
Déroulement des échanges SSL .....	214
Calculs de paramètres .....	217
Le protocole Handshake .....	218
Le protocole ChangeCipherSpec (CCS) .....	228
Le protocole Record .....	228
Le protocole Alert .....	229
<b>Exemple de traitement de SSL</b> .....	231
Établissement d'une nouvelle session .....	232
Traitement des données des applications .....	237
Établissement d'une connexion .....	238
<b>Implémentations</b> .....	242
<b>Évaluation</b> .....	245
<b>Annexe 1 : Structures des messages du Handshake</b> .....	246
<b>Annexe 2 : Codage en langage C d'une application fondée sur SSL</b> .....	250
Code du côté client .....	250
Côté serveur .....	252

## **CHAPITRE 7 : SÉCURISATION DES TÉLÉPAIEMENTS AVEC SET** ..... 255

<b>Architecture</b> .....	256
<b>Sécurisation</b> .....	259
Algorithmes cryptologiques utilisés .....	260
La méthode de la signature duale .....	262
La certification .....	263
<b>Achat</b> .....	275
<b>Procédures facultatives</b> .....	284
<b>Implémentations</b> .....	285
<b>Évaluation</b> .....	287

## **CHAPITRE 8 : SOLUTIONS HYBRIDES À BASE DE SET** ..... 289

<b>C-SET et E-Comm</b> .....	290
------------------------------	-----

Architecture de C-SET .....	291
Inscription .....	293
Distribution du logiciel de paiement .....	294
Achat .....	295
Sécurisation .....	297
Interopérabilité SET/C-SET .....	298
<b>Architecture hybride SSL/SET .....</b>	<b>300</b>
Architecture du modèle hybride SET/SSL .....	302
Achat .....	304
Évaluation .....	307

## **CHAPITRE 9 : MICROPAIEMENTS ET COMMERCE DE PROXIMITÉ .....**

<b>Caractéristiques des systèmes de micropaiement .....</b>	<b>310</b>
<b>Chipper® .....</b>	<b>311</b>
<b>GeldKarte .....</b>	<b>313</b>
Inscription et chargement de valeur .....	313
Paiement .....	315
Sécurisation .....	317
<b>Minipay .....</b>	<b>318</b>
<b>Mondex .....</b>	<b>318</b>
Chargement de valeur .....	320
Paiement .....	320
Sécurisation .....	321
Expériences pilotes .....	321
<b>P-CARD .....</b>	<b>321</b>
<b>PAYCHIP .....</b>	<b>322</b>
Inscription et chargement de valeur .....	323
Paiement .....	323
Sécurisation .....	323
<b>Proton .....</b>	<b>324</b>
Chargement de la valeur .....	325
Paiement .....	325
Applications internationales .....	325
<b>Comparaison entre les principaux porte-monnaie .....</b>	<b>326</b>

## **CHAPITRE 10 : MICROPAIEMENTS À DISTANCE .....**

<b>NetBill .....</b>	<b>329</b>
Inscription et chargement de valeur .....	330
Achat .....	330
Compensation .....	334
Évaluation .....	335
<b>CyberCoin .....</b>	<b>335</b>
<b>KLELine .....</b>	<b>336</b>
Inscription et chargement de valeur .....	337
Achat et paiement .....	337
Compensation .....	339
Évaluation .....	340
<b>Millicent .....</b>	<b>340</b>

Sécurisation.....	342
Description du scrip .....	342
Inscription et chargement de valeur .....	343
Achat.....	345
Évaluation .....	346
<b>PayWord.....</b>	<b>347</b>
Inscription et chargement de valeur .....	348
Achat.....	349
Compensation .....	351
Charge de traitement .....	351
Évaluation .....	352
<b>MicroMint .....</b>	<b>352</b>
Inscription et chargement de valeur .....	353
Achat.....	353
Compensation .....	353
Sécurisation.....	354
Évaluation .....	355
<b>Comparaison entre différents systèmes de télémicropaiement .....</b>	<b>356</b>

**CHAPITRE 11 : LA MONNAIE NUMÉRIQUE ..... 359**

<b>Principes de base.....</b>	<b>359</b>
Non-traçabilité du débiteur.....	360
Non-traçabilité du créancier.....	363
Non-traçabilité réciproque du débiteur et du créancier .....	364
Description des coupures numériques .....	365
Détection du faux monnayage (la dépense multiple).....	367
<b>DigiCash (Ecash).....</b>	<b>369</b>
Inscription et chargement de valeur .....	370
Achat et paiement.....	371
Compensation .....	372
Livraison .....	372
Évaluation .....	373
<b>NETCASH.....</b>	<b>373</b>
Inscription et chargement de valeur .....	373
Achat.....	374
Extensions de NetCash.....	375
Évaluation .....	377

**CHAPITRE 12 : LA DÉMATÉRIALISATION DU CHÈQUE ..... 379**

<b>Traitement classique du chèque papier.....</b>	<b>379</b>
Renouvellement du chéquier.....	379
Traitement des chèques papier .....	380
<b>Traitement dématérialisé du chèque papier .....</b>	<b>381</b>
Les images chèques et les chèques tronqués .....	381
Les chèques images.....	382

<b>NetCheque</b> .....	383
Inscription .....	384
Paiement et compensation bancaire.....	385
<b>Bank Internet Payment System (BIPS)</b> .....	386
Types de transactions .....	387
Architecture.....	388
<b>Echeck</b> .....	389
Paiement et compensation.....	390
Représentation du chèque virtuel .....	392
<b>Évaluation</b> .....	395

## **CHAPITRE 13 : LA SÉCURISATION DES CARTES À PUCE** ..... 397

<b>Vue d'ensemble</b> .....	397
Catégories et applications des cartes à puce.....	398
Adaptation des cartes à puce aux ordinateurs.....	399
<b>Description des cartes à puce à contacts</b> .....	400
<b>Sécurisation des cartes à puce</b> .....	402
Sécurisation physique de la carte pendant l'utilisation.....	404
Sécurisation logique de la carte pendant l'utilisation .....	405
Exemples de sécurisation en cours de l'utilisation .....	407
Limites de la sécurisation.....	410
<b>Cartes à puce polyvalentes</b> .....	411
Le système de fichier ISO-7816-4.....	412
La carte d'identité électronique suédoise .....	413
Gestion des applications dans une carte polyvalente.....	414
<b>Normes des cartes à puce</b> .....	417
Normes des cartes à contacts.....	417
Normes des cartes sans contacts.....	418
EMV .....	418

## **CHAPITRE 14 : PLATES-FORMES ET MODÈLES DE CONVERGENCE** ..... 421

<b>SEMPER</b> .....	421
Architecture de SEMPER .....	422
Terminologie de SEMPER.....	424
Le gestionnaire de paiement.....	425
<b>CAFE</b> .....	426
<b>JEPI</b> .....	427
<b>Cartes privatives et cartes bancaires</b> .....	429
<b>Évaluation</b> .....	430

<b>CHAPITRE 15 : PERSPECTIVES</b> .....	433
<b>Infrastructure du commerce électronique</b> .....	433
<b>Quels moyens de paiement ?</b> .....	435
<b>Normalisation</b> .....	437
<b>Éléments de réflexion</b> .....	438
<b>SIGLES</b> .....	441
<b>POUR EN SAVOIR PLUS</b> .....	453
<b>BIBLIOGRAPHIE</b> .....	459
<b>INDEX</b> .....	481