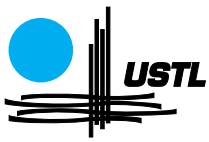

Laboratoire d'Informatique
Fondamentale de Lille

# Thèse de Doctorat

Présentée à
**L'Université des Sciences et Technologies de Lille**

Pour l'obtention du titre de
**Docteur en Informatique**
par

## Sylvain Lecomte

# COST-STIC
# Cartes Orientées Services Transactionnels et Systèmes Transactionnels Intégrant des Cartes

Soutenue le Jeudi 26 novembre 1998 devant le jury :

| | |
|---|---|
| Président : | Jean-Marc Geib, Prof. LIFL |
| Rapporteurs : | Jean Ferrié, Prof. ISIM |
| | Michel Riveill, ENSIMAG |
| Examinateurs : | Vincent Cordonnier, Prof. LIFL |
| | Didier Donsez, MdC LIMAV |
| | Pierre Paradinas, Gemplus |
| | Philippe Pucheral, MdC, Université de Versailles |
| | Simone Sédillot, INRIA Rocquencourt |

UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE
U.F.R. d'I.E.E.A. Bât. M3 – 59655 VILLENEUVE D'ASCQ CEDEX
Tél. (+33) 3 20 43 47 24 – Télécopie (+33) 3 20 43 65 66

# Remerciements



Les travaux présentés dans ce mémoire ont été réalisés au sein de l'équipe de Recherche et Développement sur le Dossier Portable (*RD2P*), du Laboratoire d'Informatique Fondamentale de Lille (*LIFL*). C'est pourquoi, je tiens avant tout à présenter mes remerciements au Professeur Vincent Cordonnier, qui dirige cette équipe, pour ses précieux conseils et la relecture de ce document.

Je tiens aussi à remercier vivement Pierre Paradinas, responsable de l'équipe de recherche avancée de Gemplus, pour son aide, ses encouragements, et sa confiance, tout au long de ces années.

Je remercie aussi le Centre Nationale de la Recherche Scientifique (*CNRS*), et la société Gemplus qui ont bien voulu m'apporter leur appui financier par l'octroi d'une bourse doctorale ingénieur.

J'exprime à présent ma gratitude aux membres du jury:

- A son président, le professeur Jean Marc Geib de l'université de Lille 1,
- Aux rapporteurs, qui ont bien voulu examiner mon travail, le professeur Jean Ferrié de l'université de Montpellier, et le professeur Michel Riveil de l'ENSIMAG,
- Aux examinateurs, le professeur Vincent Cordonnier, de l'université de Lille 1, Didier Donsez de l'université de Valenciennes, Pierre Paradinas de la société Gemplus, Philippe Pucheral de l'université de Versailles, et Simone Sédillot de l'INRIA.

J'ai eu la chance de travailler dans un groupe convivial, énergique et passionné. J'aimerais en remercier David Carlier et Patrick Trane pour les travaux effectués ensemble, ainsi que Didier Donsez et Gilles Grimaud, pour leurs conseils multiples et précieux, ainsi que leur patience et leur rigueur dans la mise au point de ce document.

De la même manière, je tiens à remercier Isabelle Cuignies et Sergiy Nemchenko pour l'aide qu'ils m'ont apportée au cours de leurs stages. Je souhaite aussi chaleureusement féliciter et remercier Lamia Aouni et Jean Jacques Vandewalle, qui ont activement participé à la réalisation du prototype carte.

Il me tient à coeur de présenter ma gratitude aux anciens et actuels membres de l'équipe RD2P, et de l'équipe de recherche de Gemplus, pour leur compétence et leur amitié, et je souhaite bon courage aux nouveaux arrivants.

Ces remerciements ne seraient pas complets, si je n'associais pas aussi à ce travail, mes amis proches, mes parents qui me soutiennent depuis toujours, ainsi que Valérie, qui m'a toujours encouragé, et qui a supporté mes humeurs durant ces 3 années.

# Table des matières



**.1 Introduction** **1**
1.1 Les cartes à microprocesseur . . . . . 1
1.2 Cartes et Systèmes Distribués . . . . . 1
1.3 Orientation du projet . . . . . 2
1.4 Plan de ce mémoire . . . . . 3

**I. Etat de l'Art** **5**

**I.1 Les cartes à microprocesseur: Principes et Evolutions** **7**
1.1 Introduction . . . . . 7
1.2 Caractéristiques Matérielles . . . . . 8
1.2.1 Architecture carte classique . . . . . 8
1.2.2 Les mémoires non volatiles . . . . . 10
1.3 Dialogue Carte / Terminal . . . . . 10
1.3.1 La Connexion . . . . . 11
1.3.2 Le Dialogue . . . . . 12
1.3.3 La Session . . . . . 13
1.4 Architecture Carte: Historique et Futur . . . . . 13
1.4.1 Systèmes Carte existants . . . . . 14
1.4.2 Une autre norme: La carte CQL . . . . . 15
1.4.3 Intégration des cartes dans les systèmes distribués . . . . . 16
1.4.4 Une programmation plus facile... . . . . 17
1.5 Les Applications Carte . . . . . 18
1.5.1 La Sécurisation des accès . . . . . 18
1.5.2 Les Cartes de paiement . . . . . 19
1.5.3 Les Cartes «Dossier Portable» . . . . . 19

1.6 Carte Multi-services . . . . . 20
1.7 Conclusion . . . . . 21

**I.2 Le modèle Transactionnel 23**
2.1 Introduction . . . . . 23
2.2 Les propriétés ACID . . . . . 24
2.2.1 Atomicité . . . . . 24
2.2.2 Cohérence . . . . . 24
2.2.3 Isolation . . . . . 24
2.2.4 Durabilité . . . . . 25
2.2.5 Implantation des propriétés ACID . . . . . 26
2.3 Le contrôle de concurrence . . . . . 26
2.3.1 Le verrouillage à deux phases . . . . . 26
2.3.2 L'estampillage . . . . . 28
2.3.3 Contrôle Optimiste . . . . . 29
2.3.4 Prise en compte de la sémantique . . . . . 29
2.3.5 Choix de la méthode . . . . . 30
2.4 Reprise sur panne . . . . . 30
2.4.1 Influence de la gestion du cache sur la reprise . . . . . 31
2.4.2 Méthodes de Journalisation . . . . . 31
2.4.3 Méthode des Pages Ombres . . . . . 32
2.5 Transactions distribuées . . . . . 33
2.5.1 Implication sur le contrôle de concurrence . . . . . 33
2.5.2 Implication sur la reprise sur panne . . . . . 34
2.5.3 Validation de la Transaction Distribuée . . . . . 34
2.5.3.1 Coordination de la validation . . . . . 34
2.5.3.2 Le protocole de Validation à deux phases . . . . . 35
2.5.3.3 Les protocoles non bloquants . . . . . 36
2.6 Modèles Avancés de Transactions . . . . . 36
2.6.1 Les Transactions Emboîtées . . . . . 36
2.6.2 Les Sagas . . . . . 37
2.6.3 Modèle à flots de tâches . . . . . 37
2.7 Normes et Services Transactionnels existants . . . . . 38
2.7.1 Le protocole OSI TP . . . . . 38
2.7.2 Le modèle DTP de X/OPEN . . . . . 39
2.7.3 OTS de l'OMG . . . . . 40
2.7.4 MTS de Microsoft . . . . . 41
2.7.5 Interopérabilité des Moniteurs Transactionnels . . . . . 42
2.8 Conclusion . . . . . 42

**II. Problématique 45**

**II.1 Nouvelles Applications et Nouveaux Besoins Carte 47**
1.1 Introduction . . . . . 47
1.2 Quelques définitions . . . . . 48
1.2.1 Applications et services . . . . . 48

1.2.2 Contexte d'exécution . . . . . 48
1.3 Applications futures . . . . . 48
1.3.1 Les cartes multi-services . . . . . 49
1.3.1.1 Des exemples d'applications . . . . . 50
1.3.1.2 Coopération Externe . . . . . 51
1.3.1.3 Coopération Interne . . . . . 51
1.3.1.4 Problèmes posés . . . . . 52
1.3.2 Les Applications «longues» . . . . . 53
1.3.2.1 Des exemples d'applications longues . . . . . 53
1.3.2.2 Problèmes posés . . . . . 54
1.3.3 Les applications multi-cartes . . . . . 55
1.4 Cartes et Applications Distribuées . . . . . 55
1.4.1 Sécurité et systèmes distribués . . . . . 56
1.4.2 Intégration des cartes dans les systèmes distribués . . . . . 58
1.4.3 Sécurisation d'applications distribuées par une carte . . . . . 58
1.4.4 D'une Carte Serveur à une Carte Cliente . . . . . 59
1.4.5 Conclusion . . . . . 61
1.5 Modèles de panne et carte . . . . . 61
1.5.1 L'arrachement de la carte . . . . . 62
1.5.2 Panne d'environnement d'exécution . . . . . 63
1.5.3 Perte, destruction . . . . . 64
1.5.4 L'erreur d'exécution . . . . . 64
1.6 Conclusion . . . . . 64

**II.2 Modèle d'Exécution Carte et Besoin Transactionnel 67**
2.1 Introduction . . . . . 67
2.2 Remarques préliminaires sur propriétés ACID et Cartes . . . . . 68
2.3 Besoins d'exécution Atomique des instructions . . . . . 69
2.3.1 Atomicité intra-APDU . . . . . 69
2.3.2 Atomicité APDU . . . . . 70
2.3.3 Atomicité Intra-Session . . . . . 71
2.3.4 Conclusion . . . . . 72
2.4 Nouvelles applications et modèle d'exécution carte . . . . . 72
2.4.1 Transaction Inter-Session et Intra-Connexion . . . . . 73
2.4.2 Transaction Multi-Connexions . . . . . 75
2.4.3 Conclusion . . . . . 76
2.5 Le cas des transactions emboîtées dans la carte . . . . . 77
2.6 La carte et les transactions distribuées . . . . . 78
2.6.1 Intégration dans les systèmes existants . . . . . 78
2.7 La carte cliente de transaction . . . . . 80
2.8 Synthèse . . . . . 80

**III. Solutions Proposées et Implantation 83**

**III.1 Un Gestionnaire de Ressources Transactionnel Carte 85**
1.1 Introduction . . . . . 85

1.2 Choix du Système d'Exploitation de base . . . . . 86
1.2.1 Vers une mémoire virtuelle pour carte . . . . . 86
1.2.2 Permettre le partage d'objets dans la carte . . . . . 87
1.3 Implantation des pages ombres dans une carte . . . . . 88
1.3.1 Principes . . . . . 88
1.3.2 Implantation et type de mémoire . . . . . 88
1.3.2.1 Implantation avec de la Flash . . . . . 88
1.3.2.2 Implantation avec de l'EEPROM . . . . . 90
1.3.3 Synthèse sur les pages ombres . . . . . 91
1.4 Implantation d'une reprise sur panne à base de journaux . . . . . 92
1.4.1 Rappels sur les Principes . . . . . 92
1.4.2 Coûts et optimisations . . . . . 92
1.4.3 Synthèse sur la journalisation . . . . . 93
1.5 Choix du mécanisme de reprise sur panne . . . . . 94
1.5.1 Comparaison des deux mécanismes . . . . . 94
1.5.2 Cartes Actuelles . . . . . 95
1.5.3 Cartes Multi-services . . . . . 95
1.6 Mécanisme de contrôle de concurrence pour carte . . . . . 96
1.6.1 Principes . . . . . 96
1.6.1.1 Le verrouillage à deux phases . . . . . 96
1.6.1.2 La technique d'estampillage . . . . . 99
1.6.2 Choix pour la carte à microprocesseur . . . . . 100
1.7 Mise en Pratique : JavaCard et Transaction . . . . . 101
1.7.1 Architecture d'un Système Transactionnel pour JavaCard . . . 101
1.7.2 Applications . . . . . 102
1.8 Limites du modèle transactionnel strict . . . . . 102
1.8.1 Le cas de l'application GSM-PME-CB . . . . . 102
1.8.2 Problématique . . . . . 103
1.8.3 Prise en compte de la commutativité des opérations . . . . . 103
1.9 Débordement des données à l'extérieur de la carte . . . . . 105
1.10 Conclusion . . . . . 105

**III.2 La carte transactionnelle dans un contexte distribué 107**
2.1 Introduction . . . . . 107
2.2 La carte à microprocesseur serveur transactionnel . . . . . 108
2.2.1 Choix de l'environnement . . . . . 108
2.2.2 Définition de l'architecture . . . . . 108
2.2.3 Choix de l'algorithme de validation distribuée . . . . . 110
2.3 Caractéristiques de l'OTS Carte et du COA . . . . . 111
2.3.1 Une évolution du COA... . . . . 111
2.3.2 Protocoles de Communication . . . . . 112
2.3.3 L'intérêt d'un OTS dédié aux cartes . . . . . 114
2.4 Tolérance aux pannes de cette Architecture . . . . . 115
2.4.1 Transaction distribuée et panne carte . . . . . 115
2.4.2 D'un objet d'adaptation à une véritable représentation externe 116
2.4.3 Tolérance aux pannes du site accepteur de représentation externe 118

2.4.4 Architecture globale des machines de connexion carte . . . . . 118
2.5 Un rôle plus important pour la carte ... . . . . 119
2.5.1 Le Coordinateur dans la carte . . . . . 119
2.5.2 La carte Cliente de Transactions . . . . . 120
2.6 Conclusion . . . . . 121

**III.3 Une Implantation de nos solutions : GemXpresso et Transaction 123**
3.1 Introduction . . . . . 123
3.2 Point de Départ : La GemXpresso . . . . . 124
3.3 Problèmes spécifiques aux composants utilisés . . . . . 124
3.4 Réalisation d'un mécanisme de Reprise sur Panne . . . . . 125
3.4.1 Mécanisme de reprise après panne implanté . . . . . 125
3.4.2 Limites de cette solution . . . . . 127
3.5 Intégration dans une Application Distribuée . . . . . 127
3.5.1 Description du composant d'adaptation . . . . . 127
3.5.2 Fonctionnement du COA . . . . . 128
3.6 Le service transactionnel . . . . . 129
3.6.1 Problèmes rencontrés . . . . . 129
3.6.2 Description de l'OTS réalisé . . . . . 129
3.7 L'application : Transfert d'un compte Bancaire sur un PME . . . . . 131
3.7.1 Architecture Globale . . . . . 131
3.7.2 Le Client . . . . . 131
3.7.3 Le Serveur Banque . . . . . 132
3.7.4 Le serveur Carte . . . . . 133
3.7.5 Conclusion et Résultats . . . . . 134
3.8 Portabilité de la maquette . . . . . 135

**IV. Conclusion et Perspectives 137**

**IV.1 Conclusion 139**
1.1 Une utilisation plus évoluée des cartes à microprocesseur . . . . . 139
1.2 COST : un gestionnaire de ressources transactionnel pour la carte . . 140
1.2.1 La reprise sur panne . . . . . 140
1.2.2 Le contrôle de concurrence . . . . . 141
1.3 La carte dans les Transactions Distribuées . . . . . 142
1.3.1 Résultats . . . . . 142
1.3.2 Liens avec les travaux sur l'informatique mobile . . . . . 143

**IV.2 Perspectives 145**
2.1 Evolution des systèmes d'exploitation carte . . . . . 145
2.2 Un monde carte en pleine évolution . . . . . 146
2.3 L'arrivée de très petits composants dans le monde distribué . . . . . 146

**V. Annexes** **147**

**V.1 Interfaces OTS de l'OMG** **149**

**V.2 Acronymes utilisés** **155**

**V.3 Bibliographie** **159**