Université de Montréal

SecAdvise - un aviseur de mécanismes de sécurité: implantation, validation et expérimentation du modèle proposé

par

Marian Dagher

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en informatique

Décembre 2003

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

SecAdvise - un aviseur de mécanismes de sécurité : implantation, validation et expérimentation du modèle proposé

présenté par :

Marian Dagher

a été évalué par un jury composé des personnes suivantes :

Stefan Wolf,	Président-rapporteur
Peter Kropf,	Directeur de recherche
Gilbert Babin,	Codirecteur
Houari A. Sahraoui,	Membre du jury

Mémoire accepté le : 12 février 2004

Sommaire

Un modèle conceptuel d'un aviseur de mécanismes de sécurité a été développé au département d'informatique et de recherche opérationnelle de l'Université de Montréal. L'architecture préliminaire de l'aviseur SecAdvise, inclut un gestionnaire de risques, intègre différents mécanismes de sécurité et rend possible le choix dynamique des mécanismes appropriés à utiliser entre plusieurs parties effectuant des transactions d'affaires selon le contexte en cours.

SecAdvise vise à contourner les problèmes d'interopérabilité et de compatibilité, à évaluer et réduire les risques de sécurité et à augmenter la confiance des utilisateurs [RS02].

Le travail de ce mémoire effectue l'étude de l'architecture proposée et de son applicabilité. Cela inclut l'investigation de la correspondance entre l'architecture proposée et les modèles actuels du commerce électronique, la conception détaillée du modèle (incluant la modification de la modélisation formelle proposée selon le besoin), l'implantation du modèle en construisant un prototype et en joignant la base de données nécessaire aux standards et aux spécifications du commerce électronique, l'expérimentation du prototype avec des scénarios d'utilisation concrets et, finalement, l'étude de la qualité de service.

Mots clés : commerce électronique, transaction, sécurité, risque, service de sécurité, mécanisme de sécurité, modèle OSI, TPS (*Trust Problem Space*), TU (*Trust Unit*), SecAdvise.

Abstract

A conceptual model of a security mechanisms advisor was developed in the Computer Science and Operational Research department of the University of Montréal. The preliminary architecture of the advisor SecAdvise includes a risk manager integrates different security mechanisms and makes possible the dynamic choice of the appropriate ones to use to secure business transactions among several parties according to the ongoing transactions context.

SecAdvise aims to rectify interoperability and compatibility problems, evaluate and reduce risks and enhance users confidence [RS02].

In this thesis, we study the proposed architecture and its applicability. This includes investigating the correspondence between the proposed architecture and actual Electronic Commerce models, preparing a detailed conception of the model including the modification of the proposed formal modelling as needed, implementing the model by constructing a prototype and by joining the necessary database to Electronic Commerce standards and specifications, experimenting the prototype by concrete utilization scenarios and studying the quality of service.

Keywords **:** E-Commerce, transaction, security, threat, security services, security mechanisms, OSI model, TPS (Trust Problem Space), TU (Trust Unit), SecAdvise.

Table des matières

CHAPITRE 1. INTRODUCTION 1

1.1 CONTEXTE DU TRAVAIL 1
1.2 RÉSULTATS ATTENDUS 1
1.3 PROBLÉMATIQUE ET APPROCHE DE RECHERCHE 2
1.4 STRUCTURE DU MÉMOIRE 4

CHAPITRE 2. ÉTAT DE L'ART 6

2.1 LA COMMUNICATION SÉCURITAIRE 6
2.1.1 L'Internet 6
2.1.2 La conception d'un système sécuritaire 6
2.1.3 La cryptographie 7
2.1.4 L'infrastructure de gestion des clés (IGC) 8
2.2 LES PROTOCOLES 9
2.2.1 Les modèles OSI et TCP/IP 9
2.2.2 Introduction aux protocoles 9
2.2.3 Les protocoles de sécurité sur l'Internet 10
2.2.4 Exemple d'un protocole de sécurité : S/MIME 10
2.3 LE COMMERCE ÉLECTRONIQUE 11
2.3.1 Introduction au commerce électronique 11
2.3.2 L'interopérabilité du commerce électronique 12
2.3.3 Exemples d'interopérabilité dans l'économie digitale 12
2.4 LES STANDARDS ET LES SPÉCIFICATIONS 13
2.4.1 Les standards 13
2.4.2 Les spécifications 13
2.4.3 Les standards actuels et l'interopérabilité 14
2.5 LES MODÈLES EXISTANTS DU COMMERCE ÉLECTRONIQUE 14
2.5.1 Introduction aux modèles du commerce électronique 14
2.5.2 Comparaison de modèles du commerce électronique 15
2.6 L'AVISEUR DE MÉCANISMES DE SÉCURITÉ SECADVISE 17
2.6.1 Le modèle de confiance de Robles 17
2.6.2 L'approche SecAdvise 19
2.6.3 La modélisation formelle de SecAdvise 21
2.6.4 Mise en contexte de SecAdvise (face aux modèles existants) 22

CHAPITRE 3. MÉTHODOLOGIE ET CONCEPTION 23

3.1 VUE GÉNÉRALE DE SECADVISE 23
3.2 LE MODÈLE DE SÉCURITÉ DE SECADVISE 24
3.2.1 Justification et choix 24
3.2.2 Le modèle de sécurité CEN/TC 224 –ISO/TC 68/SC 6 25
3.2.3 Le protocole de communication 26
3.3 LA CONCEPTION DE SECADVISE 29
3.3.1 Introduction 29
3.3.2 Le diagramme de cas d'utilisation 30
3.3.3 Le diagramme de paquetage (package) 32
3.3.4 Les diagrammes de classe 32
3.3.5 Le diagramme d'activité 35
3.3.6 Le diagramme de séquence 39
3.4 LE MODÈLE DE LA BASE DE DONNÉES 40
3.4.1 Le niveau conceptuel 40
3.4.2 Le niveau externe 41

3.5 REVUE DE LA MODÉLISATION FORMELLE 44

CHAPITRE 4. RÉALISATION ET IMPLANTATION 49

4.1 LES INTERFACES GRAPHIQUES DE L'USAGER 50
4.2 CONCEVOIR LE CALCUL DE L'ENSEMBLE DES SOLUTIONS LOCALES 56
4.3 L'IMPLANTATION DE LA BASE DE DONNÉES 59
4.3.1 Le gestionnaire de la base de données 59
4.3.2 Les affichages de données 60
4.3.3 La matrice de calcul des solutions locales 61
4.4 CONCEVOIR L'ASSOCIATION MUTUELLE 63
4.4.1 Concevoir l'association mutuelle directe 63
4.4.2 Concevoir l'association mutuelle indirecte 64
4.5 LA COMMUNICATION ENTRE LES ENTITÉS 66

CHAPITRE 5. L'EXPÉRIMENTATION DU MODÈLE 68

5.1 LES SCÉNARIOS DE TEST 68
5.2 LES EXPÉRIMENTATIONS 69
5.2.1 Les transactions du commerce électronique 69
5.2.2 Test et analyse d'une activité de commande 71
5.2.3 Test et analyse d'une activité de livraison 74
5.2.4 Test et analyse d'une activité de paiement 77
5.3 CONCLUSION DES EXPÉRIMENTATIONS 81

CHAPITRE 6. CONCLUSION 83

6.1 ANALYSE DES RÉSULTATS 83
6.2 ATTEINTE DES OBJECTIFS ET CONCLUSION 85
6.3 TRAVAUX FUTURS 86

BIBLIOGRAPHIE 88

ANNEXE A. SERVICES ET SOLUTIONS DE SÉCURITÉ 91

A.1 SERVICES ET MÉCANISMES DE SÉCURITÉ 91
A.2 RELATION ENTRE LES MÉCANISMES ÉLÉMENTAIRES ÉT COMBINÉS 95
A.3 LES SERVICES DE SÉCURITÉ OFFERTS PAR LES MÉCANISMES DE SÉCURITÉ 96
A.4 LES INTERACTIONS ENTRE LES SERVICES DE SÉCURITÉ 97
A.5 RÉSUMÉ DE SOLUTIONS DE SÉCURITÉ 98
A.5.1 Standard - ISO/IEC 7816 98
A.5.2 Standard - ISO/IEC 8731 99
A.5.3 Standard – ISO/IEC 9594 99
A.5.4 Standard - ISO/IEC 9796 99
A.5.5 Standard – ISO/IEC 9797 100
A.5.6 Standard – ISO/IEC 9798 101
A.5.7 Standard – ISO 10126 101
A.5.8 Standard – ISO 10202 102
A.5.9 Standard – ISO/IEC 14888 102
A.5.10 Standard – ECBS TCD110 103
A.5.11 Standard – ANSI X3.92 103
A.5.12 Standard – ANSI X3.106 104
A.5.13 Spécification – C-SET 104
A.5.14 Spécification – e-COMM 104
A.5.15 Spécification – EMV 105
A.5.16 Spécification – GDSA 105
A.5.17 Spécification – HBCI 106
A.5.18 Spécification – IC-SET 106
A.5.19 Spécification – IPSec 107
A.5.20 Spécification – PGP 107

A.5.21 Spécification – PKCS *108*
A.5.22 Spécification – S/MIME *108*
A.5.23 Spécification - SET *109*
A.5.24 Spécification – TLS & SSL *109*

ANNEXE B. LE PROTOCOLE DE COMMUNICATION **111**

Liste des tableaux

TABLEAU 2.1 LES MODÈLES LES PLUS RÉPANDUS DU COMMERCE ÉLECTRONIQUE, SYNTHÉTISÉS DE [CEN01] 17
TABLEAU 3.1 UNE LISTE DES MESSAGES QUE LES PARTICIPANTS S'ÉCHANGENT 27
TABLEAU 3.2 UN EXEMPLE DES VALEURS POSSIBLES POUR UNE TRANSACTION 41
TABLEAU 3.3 LA MODÉLISATION FORMELLE DE SECADVISE, ADAPTÉE DE [RS02] ET [RS02A] 45
TABLEAU 3.4 REVUE DE LA MODÉLISATION FORMELLE DE SECADVISE 48
TABLEAU 4.1 LES GESTIONS DES RISQUES ET LES MODÈLES D'INTERACTION 57
TABLEAU 4.2 MATRICE DE CALCUL DE L'ENSEMBLE DES SOLUTIONS LOCALES 57
TABLEAU 5.1 LES SERVICES DE SÉCURITÉ DES ACTIVITÉS DU COMMERCE ÉLECTRONIQUE, ADAPTÉ DE [CEN99] 70
TABLEAU 5.2 LE TEST DE SECADVISE DANS UNE ACTIVITÉ DE COMMANDE 72
TABLEAU 5.3 LE TEST DE SECADVISE DANS UNE ACTIVITÉ DE LIVRAISON 75
TABLEAU 5.4 LE TEST DE L'ACTIVITÉ DE LIVRAISON AVEC DES GESTIONS DIFFÉRENTES DES RISQUES 76
TABLEAU 5.5 LE TEST DE SECADVISE DANS UNE ACTIVITÉ D'AUTORISATION 78
TABLEAU 5.6 LE DEUXIÈME TEST DE SECADVISE DANS UNE ACTIVITÉ D'AUTORISATION 80
TABLEAU A.1 LES SERVICES ET LES MÉCANISMES DE SÉCURITÉ, SYNTHÉTISÉ DE [CEN99] 94
TABLEAU A.2 LES MÉCANISMES ÉLÉMENTAIRES QUI IMPLANTENT DES MÉCANISMES COMBINÉS DE SÉCURITÉ, TRADUIT DE [CEN99] 95
TABLEAU A.3 LES SERVICES DE SÉCURITÉ FOURNIS PAR LES MÉCANISMES COMBINÉS DE SÉCURITÉ, SYNTHÉTISÉ DE [CEN99] 96
TABLEAU A.4 LES INTERACTIONS ENTRE LES DIFFÉRENTS SERVICES DE SÉCURITÉ, SYNTHÉTISÉ DE [CEN99] 97
TABLEAU B.1 UNE LISTE DÉTAILLÉE DES MESSAGES DU PROTOCOLE DE COMMUNICATION ET DE LEUR SIGNIFICATION 112

Liste des figures

FIGURE 1.1 UNE TRANSACTION SÉCURITAIRE TYPIQUE SANS ET AVEC L'UTILISATION DE SECADVISE....3
FIGURE 2.1 LES ÉLÉMENTS ET LES ÉTAPES DE LA CONCEPTION SÉCURITAIRE....6
FIGURE 2.2 LES ÉTAPES DE L'ENVOI D'UN MESSAGE EN UTILISANT S/MIME, ADAPTÉ DE [SC02]....11
FIGURE 2.3 LE MODÈLE DE COMPARAISON DU GROUPE CEN/ISSS, TRADUIT DE [CEN01]....15
FIGURE 2.4 LE MODÈLE DE CONFIANCE DE ROBLES, ADAPTÉ DE [SR01]....18
FIGURE 2.5 UN MODÈLE ENTITÉ-RELATION QUI MONTRE LES RELATIONS ENTRE LES NOTATIONS DU MODÈLE DE ROBLES....19
FIGURE 2.6 LA GESTION DE RISQUE DANS SECADVISE....20
FIGURE 2.7 APPLICATION DU MODÈLE DE ROBLES À SECADVISE....21
FIGURE 3.1 UNE VUE GÉNÉRALE DE SECADVISE - LE CÔTÉ DE L'INITIATEUR....24
FIGURE 3.2 LE MODÈLE DE SÉCURITÉ CEN/TC 224 –ISO/TC 68/SC 6, TRADUIT DE [CEN99]....25
FIGURE 3.3 UN MODÈLE ENTITÉ–RELATION QUI MONTRE LES RELATIONS ENTRE LES COMPOSANTES DU MODÈLE DE SÉCURITÉ....26
FIGURE 3.4 TENTATIVE D'ASSOCIATION MUTUELLE ENTRE TROIS PARTICIPANTS....27
FIGURE 3.5 QUELQUES SCÉNARIOS DU PROTOCOLE DE COMMUNICATION....28
FIGURE 3.6 LE DÉROULEMENT DU PROCESSUS DE SECADVISE....29
FIGURE 3.7 LE DIAGRAMME DE CAS D'UTILISATION DU SYSTÈME....31
FIGURE 3.8 LE DIAGRAMME DE PAQUETAGE DU SYSTÈME....32
FIGURE 3.9 LE DIAGRAMME DE CLASSE DU PAQUETAGE DE LA COMMUNICATION....33
FIGURE 3.10 LE DIAGRAMME DE CLASSE DU PAQUETAGE DES INTERFACES GRAPHIQUES....34
FIGURE 3.11 LE DIAGRAMME DE CLASSE DU PAQUETAGE DE LA BASE DE DONNÉES....35
FIGURE 3.12 LE DIAGRAMME D'ACTIVITÉ INITIAL D'UN USAGER....36
FIGURE 3.13 LE DIAGRAMME D'ACTIVITÉ D'UN INITIATEUR....37
FIGURE 3.14 LE DIAGRAMME D'ACTIVITÉ D'UN PARTICIPANT....38
FIGURE 3.15 LE DIAGRAMME DE SÉQUENCE D'UNE ASSOCIATION MUTUELLE RÉUSSIE....39
FIGURE 3.16 UN MODÈLE ENTITÉ-RELATION DE LA BASE DE DONNÉES DE LA PLATE-FORME DE SÉCURITÉ....42
FIGURE 3.17 UN MODÈLE ENTITÉ-RELATION DE LA BASE DE DONNÉES DES PROFILS DES TRANSACTIONS....43
FIGURE 4.1 LE RÔLE DE SECADVISE DANS LA SÉCURISATION D'UNE TRANSACTION....49
FIGURE 4.2 LA FENÊTRE INITIALE DE SECADVISE....50
FIGURE 4.3 LA FENÊTRE D'INITIATION D'UNE TRANSACTION....51

FIGURE 4.4 LA FENÊTRE D'ANALYSE DU CONTEXTE D'UNE TRANSACTION 52
FIGURE 4.5 LA FENÊTRE DE CALCUL DE L'ENSEMBLE DES SOLUTIONS LOCALES 52
FIGURE 4.6 LA FENÊTRE DE L'ASSOCIATION MUTUELLE – PARTICIPANT 53
FIGURE 4.7 LA FENÊTRE DE L'ASSOCIATION MUTUELLE – INITIATEUR 54
FIGURE 4.8 LA FENÊTRE DE L'ADMINISTRATEUR 55
FIGURE 4.9 LA FENÊTRE DE L'AIDE A L'USAGER 55
FIGURE 4.10 LA FENÊTRE DE LA BASE DE DONNÉES 56
FIGURE 4.11 LA CLASSE DU GESTIONNAIRE DE LA BASE DE DONNÉES 60
FIGURE 4.12 APPEL D'UNE MÉTHODE DU GESTIONNAIRE DE LA BASE DE DONNÉES 60
FIGURE 4.13 UNE MÉTHODE DE LA CLASSE DU GESTIONNAIRE DE LA BASE DE DONNÉES 61
FIGURE 4.14 LA REQUÊTE QUI CHERCHE LES MODÈLES D'INTERACTION DE SÉCURITÉ 62
FIGURE 4.15 LES REQUÊTES QUI CHERCHENT LES SOLUTIONS OPTIMALES 63
FIGURE 4.16 ASSOCIATION MUTUELLE DIRECTE 63
FIGURE 4.17 ASSOCIATION MUTUELLE PARTIELLE - INITIATEUR 64
FIGURE 4.18 ASSOCIATION MUTUELLE PARTIELLE – PARTICIPANT 65
FIGURE 5.1 ÉTAPES ET RÔLES DES ENTITÉS DANS DES TRANSACTIONS DU COMMERCE ÉLECTRONIQUE, TRADUIT DE [CEN99] 69
FIGURE 5.2 SOLUTIONS COMMUNES DANS DES TRANSACTIONS DE COMMERCE ÉLECTRONIQUE, TRADUIT DE [CEN99] 71
FIGURE 5.3 PLACEMENT D'ACTIVITÉ DE PASSATION DE COMMANDE DANS UN SCÉNARIO DE COMMANDE, TRADUIT DE [CEN99] 71
FIGURE 5.4 PLACEMENT D'ACTIVITÉ DE LIVRAISON DANS UN SCÉNARIO TYPIQUE DE COMMANDE, TRADUIT DE [CEN99] 74
FIGURE 5.5 LES ACTIVITÉS D'UN SCÉNARIO TYPIQUE DE PAIEMENT, TRADUIT DE [CEN99] 77

À mes parents

Remerciements

Je remercie mon directeur de recherche monsieur Peter Kropf, professeur à l'Université de Montréal, de me donner l'opportunité de faire ce travail et de suivre de près les étapes de ma recherche. J'ai apprécié son expérience, son souci de la qualité, sa générosité et son attention.

Je remercie mon codirecteur de recherche monsieur Gilbert Babin, professeur aux HEC à Montréal. J'ai apprécié son expérience, ses conseils, ses idées enrichissantes et sa compréhension.

Je remercie chacun des membres du jury d'avoir accepté d'être le juge de mon projet de maîtrise.

Mes remerciements vont aussi à ma famille et à mes amis qui m'ont offert leur support. Je remercie également mes enseignants pour la qualité de leur travail et leur dévouement.

Chapitre 1. Introduction

1.1 Contexte du travail

L'Internet est un réseau mondial de réseaux ouverts de communication électronique dont la création date de 1969. En 1991, après avoir été une infrastructure qui connectait plutôt les institutions gouvernementales et universitaires, l'Internet a commencé à servir des entreprises commerciales [SC02]. Avec l'avènement du commerce électronique, l'économie bénéficie d'un nouveau médium extrêmement puissant et efficace. En effet, l'Internet a changé fondamentalement, et continue encore à le faire, la façon dont les gens communiquent entre eux. Pour bien comprendre les dimensions de l'Internet, on doit le considérer comme un amalgame de trois composantes : l'infrastructure, le contenu et les usagers.

La taille massive de l'infrastructure de l'Internet, avec ses 300 millions d'utilisateurs et sa quantité immense de données éparpillées partout dans le monde, ainsi que le fait que les fonctions de l'administration de ce réseau ouvert soient parcellaires et décentralisées rend très compliquée la tâche d'assurer la confidentialité et l'intégrité des informations qui y circulent ou qui sont stockées sur les équipements qui y sont raccordés [JC02]. Cette assurance de la confidentialité et l'intégrité des informations est très importante pour l'avancement du domaine.

Différents moyens pour assurer la sécurité des échanges sur l'Internet ont été proposés partout dans le monde. Ces différentes technologies de sécurité sont, dans une certaine limite, normalisées et assurent une interopérabilité minimale, mais plus de travail est encore nécessaire en vue d'atteindre une vrai interopérabilité [VH00]. L'aviseur de mécanismes de sécurité SecAdvise tente de résoudre ce problème.

1.2 Résultats attendus

L'architecture de SecAdvise, qui a été proposée dans [RS02], intègre un gestionnaire de risques de sécurité et présente un système capable de choisir de manière dynamique et

optimale les solutions de sécurité à utiliser entre les parties souhaitant exécuter des transactions électroniques entre eux.

Dans ce mémoire, nous effectuons une étude détaillée de l'architecture proposée et de son applicabilité. Cela inclut une conception détaillée du modèle avant d'arriver à programmer et à expérimenter un prototype du système.

Par les expérimentations du prototype et les analyses qui suivront les tests, nous voulons démontrer qu'en proposant les solutions de sécurité appropriées aux types de transactions effectuées, SecAdvise réduira les risques de sécurité et augmentera donc la confiance des utilisateurs.

On veut aussi démontrer que grâce à leur capacité de négociation en ligne, les entités de SecAdvise pourront échanger leurs solutions locales de sécurité et arriveront ainsi à décider s'il existe des solutions communes à tous les partis impliqués qui pourront les adopter et les utiliser pour sécuriser la transaction en cours. SecAdvise va ainsi augmenter le degré d'interopérabilité entre les systèmes des différents partis et contourner le problème de compatibilité.

1.3 Problématique et approche de recherche

L'aviseur SecAdvise inclut un gestionnaire de risque qui couvre les domaines d'applications suivants : sécurité individuelle, sécurité collective et sécurité des échanges. SecAdvise va analyser les besoins de sécurité propres aux utilisateurs et proposer des solutions de types différents selon le domaine d'application choisi. Par exemple, en ce qui concerne le domaine d'application des échanges électroniques, les solutions peuvent être des mécanismes de sécurité, des protocoles, des infrastructures ou une combinaison de ce qui précède.

La figure 1.1 montre deux exemples de transaction sécurisée. Le premier dessin montre un cas traditionnel sans l'utilisation de la plate-forme de SecAdvise. Dans ce cas, c'est à l'application de trouver et d'appliquer les solutions de sécurité appropriées au contexte

de la transaction. Le dessin en bas montre une transaction sécurisée avec la plate-forme SecAdvise qui se place entre l'application et les différents systèmes de sécurité. SecAdvise assure plus de flexibilité dans le choix de solutions. En proposant à chaque utilisateur des solutions appropriées aux problèmes locaux de sécurité et en négociant ces solutions plus tard avec les autres entités, SecAdvise libérera l'application haut niveau de cette tâche et atteindra ses objectifs.

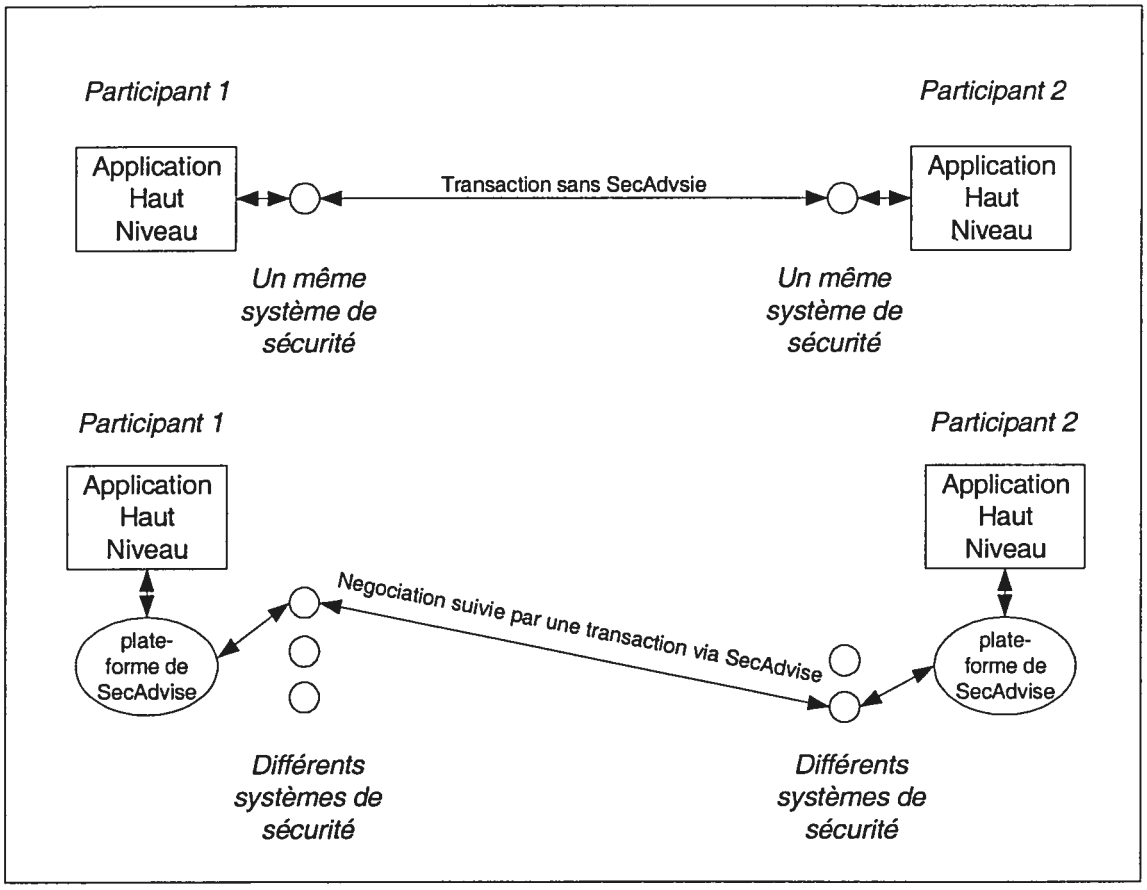

Figure 1.1 Une transaction sécuritaire typique sans et avec l'utilisation de SecAdvise

Plusieurs organisations internationales de normalisation cherchent à trouver des moyens pour contourner les problèmes actuels de l'incompatibilité des différents systèmes électroniques en général, y compris l'interopérabilité des différents systèmes de sécurité informatiques. Ces organisations publient régulièrement des standards et des spécifications de sécurité en espérant qu'on les respecte. En ce faisant, les utilisateurs vont pouvoir faire leurs échanges de façon interopérable. Par exemple, l'organisation ISO (*International Standardisation Organisation*) a déjà standardisé les services de sécurité en les regroupant en cinq catégories principales : l'authentification, la

confidentialité des données, l'intégrité des données, le contrôle d'accès et la non-répudiation. Quelques standards et spécifications émis par ISO et par d'autres organisations présentent des façons d'exécuter ces services de sécurité qu'on appelle des modèles d'interaction.

Dans le but de démontrer l'applicabilité du modèle, nous allons instancier la base de données du prototype par les standards et les spécifications de sécurité les plus importants, les services de sécurité qu'ils offrent et les risques que ces services de sécurité couvrent. Cette base de données assurera la correspondance entre les solutions de sécurité et les transactions en cours, selon les besoins de sécurité des utilisateurs.

La conception, qui précédera la programmation et le test d'un prototype, prendra en considération la modélisation formelle proposée du modèle SecAdvise et ce, sans exclure la possibilité de la modifier si cela s'avère utile. Par exemple, on a remarqué que la modélisation actuelle n'inclut pas la possibilité de négocier des critères qui pourraient optimiser les choix.

1.4 Structure du mémoire

Le chapitre 2 commence par une introduction aux réseaux de communication électronique et leurs concepts de sécurité avant d'aborder les sujets du commerce électronique et de l'importance de l'interopérabilité des différents systèmes pour son avancement. Nous comparons, dans le même chapitre, quelques architectures connues de commerce électronique et nous donnons des exemples de standards et de spécifications dans le domaine de la sécurité du commerce électronique. Nous concluons ce chapitre par une introduction rapide à SecAdvise comme il a été proposé dans [RS02] en le comparant aux modèles existants du commerce électronique.

Dans le chapitre 3, nous nous basons sur un modèle standard de sécurité tirée de la référence [CEN99] pour concevoir un modèle haut niveau de SecAdvise en utilisant le langage de modélisation UML (*Unified Modeling Language*). Dans le même chapitre,

nous concevons le schéma de la base de données et nous montrons la correspondance entre la conception et la modélisation formelle de SecAdvise.

Nous détaillons dans le chapitre 4 notre implantation d'un prototype en utilisant le langage Java pour la programmation et la technologie Java RMI (*Remote Methods Invocation*) pour assurer la communication entre les entités. Nous utilisons le langage SQL (*Structured Query Language*) pour interroger la base de données.

Dans le chapitre 5, nous donnons une description de quelques scénarios concrets d'utilisation et nous effectuons quelques tests sur le prototype. Cela est suivi d'une analyse et d'une évaluation des résultats des tests.

Nous commençons le chapitre final en analysant les résultats du travail en général et en les comparant aux objectifs attendus. Enfin, nous tirons une conclusion globale du mémoire et proposons des possibilités de futurs travaux.

Nous avons joint au mémoire plusieurs annexes que nous avons jugées pertinentes. Par exemple, des résumés des standards et des spécifications.

Chapitre 2. État de l'art

2.1 La communication sécuritaire

2.1.1 L'Internet

Les échanges de données sur le réseau Internet se font par des fichiers informatiques; le réseau Internet ne garantit pas l'authenticité, la validité ni l'intégrité des informations qu'il transmet aux usagers. En plus, les logiciels et les utilitaires sont aussi des fichiers informatiques et les informations des utilisateurs connectés au réseau Internet sont accessibles à tous [JC02].

L'Internet est un réseau qui convient pour transférer les données, mais l'insécurité de son infrastructure et le fait qu'il soit public doivent être pris en considération lors de la conception de ses logiciels et de ses matériaux. Aussi, les données qui circulent doivent être manipulées par des moyens appropriés [VH00].

2.1.2 La conception d'un système sécuritaire

La notion de sécurité informatique couvre les risques d'origine matérielle et d'origine humaine, intentionnelle ou accidentelle [JC02]. La figure 2.1 montre les éléments d'une conception sécuritaire. Une analyse des risques (gestion des risques) doit être réalisée durant la phase de planification, cette analyse évalue la relation entre le niveau d'importance d'une menace (le coût de réparation), la probabilité de l'occurrence de cette menace et le coût de l'implantation des mécanismes de protection appropriés.

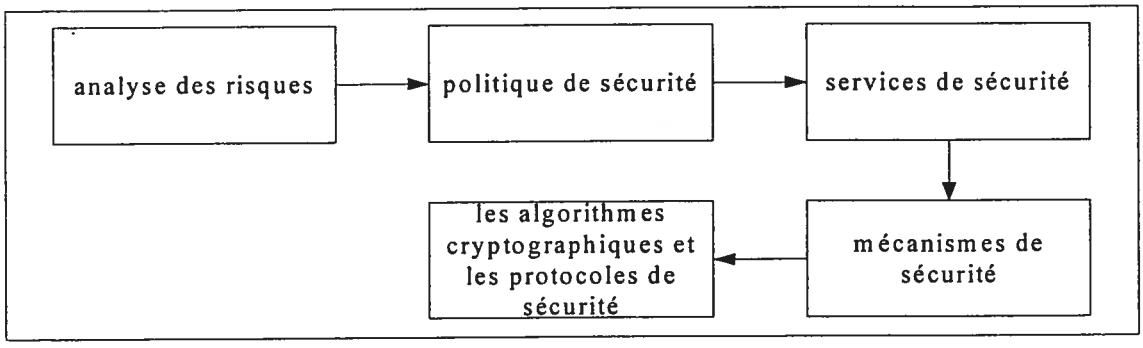

Figure 2.1 Les éléments et les étapes de la conception sécuritaire

L'analyse des risques mène à la définition d'une politique de sécurité qui spécifie clairement les actifs à protéger et qui présente un compromis raisonnable entre les risques et les ressources disponibles. Les fonctions qui mettent la politique de sécurité en vigueur s'appellent les services de sécurité, par exemple le contrôle d'accès. Les mécanismes de sécurité sont des moyens pour implanter les services de sécurité, par exemple la signature digitale. Les algorithmes cryptographiques et les protocoles de sécurité sont des moyens pour réaliser les mécanismes de sécurité. La gestion de conformité (*compliance management*) analyse si les fonctionnalités de sécurité mises en place offrent la protection attendue [VH00].

La disponibilité et la fiabilité sont deux points importants dans la conception des systèmes sécuritaires. La disponibilité exige une protection contre les attaques et une détection rapide de leurs occurrences avec des procédures de reprise. La fiabilité exige des transactions atomiques, des services de mise en réseau fiables, des logiciels et des matériaux fiables (par exemple, en ajoutant la redondance statique ou dynamique) et des mécanismes de tolérance aux erreurs éventuelles (par exemple, le stockage stable). Il est impossible de prouver formellement qu'un système arbitraire est sécuritaire, mais il est possible de construire des systèmes sécuritaires corrects et vérifiables en introduisant la vérification dans la spécification, la conception et l'implantation des systèmes [VH00].

2.1.3 La cryptographie

Propager les informations par des moyens de télécommunication accroît considérablement leur vulnérabilité. Le chiffrement de données, qui est le processus pour masquer les données afin de les garder secrètes, est une des mesures de protection souvent employée sur l'Internet. La cryptographie est la science de protéger la confidentialité et l'intégrité de données [SM01]. Elle offre des méthodes mathématiques pour établir la sécurité des systèmes de communication et elle inclut l'étude des systèmes de chiffrement et de déchiffrement des messages. L'utilisation d'un système de chiffrement de messages est complexe et demande généralement des systèmes de clés cryptographiques aux procédures compliquées que les usagers doivent respecter [JC02].

En général, on utilise un algorithme de chiffrement (*cipher*) pour masquer la signification des données originales (code en langage clair) et produire une version chiffrée (texte chiffré). Deux systèmes de clés de chiffrement existent : les systèmes à clés symétriques (privés), où la même clé est utilisée pour chiffrer et pour déchiffrer les messages, et les systèmes à clés asymétriques (publiques), où une clé publique est utilisée pour chiffrer le message et une autre clé privée que seul le receveur connaît est utilisée pour déchiffrer le message.

2.1.4 L'infrastructure de gestion des clés (IGC)

Un certificat de clé publique (*Public Key Certificat; PKC*) est une structure de données qui, entre autres, associe une valeur d'une clé publique et un objet. Cette association est assurée par une autorité de certification (*Certification Authority; CA*) qui vérifie les identités et signe les certificats. Actuellement, Il y a plusieurs types de certificats standards utilisés, comme le certificat ISO/IEC 9594-8 (équivalent au certificat X.509v3), le certificat ISO/IEC 9594-8, etc. Ces certificats se distinguent selon leur usage, la syntaxe du codage de leurs informations, leur contenu et leur taille.

Les utilisateurs des systèmes à clé publique comptent sur les certificats de clé publique pour s'assurer que l'entité avec laquelle ils communiquent possède vraiment l'identité dont elle se réclame et, par le fait même, possède la clé privée associée avec la clé publique en question [CEN01].

L'infrastructure à clé publique (*Public Key Infrastructure; PKI*) est l'ensemble des matériaux, des logiciels, des personnes, des politiques et des procédures nécessaires pour créer, gérer, stocker, distribuer et révoquer les certificats de clé publique basés sur la cryptographie à clé publique. Le but de l'infrastructure à clé publique est de fournir une gestion efficace et éprouvée des clés et des certificats des clés publiques.

Le groupe PKIX (group de travail d'*Internet Engineering Task Force; IETF*) produit des recommandations (*Requests for Comment; RFC*) et des épreuves (*Internet drafts*)

concernant la gestion, la distribution et l'usage des clés pour les fonctions cryptographiques à clé publique [CEN01].

2.2 Les protocoles

2.2.1 Les modèles OSI et TCP/IP

C'est important que les produits informatiques faits par les différentes compagnies soient interopérables. Le modèle de référence OSI (*Open System Interconnection*) est un standard élaboré par ISO (*International Standardization Organization*) qui vise à faciliter l'interopérabilité des composantes informatiques produites par différents producteurs. Le modèle OSI sépare le processus de communication entre les ordinateurs en sept couches distinctes qui sont basées sur la séquence naturelle des évènements de la communication. Le but du modèle OSI est de réduire le problème complexe de communication sur les réseaux en petits morceaux plus facilement gérables.

Le modèle TCP/IP (*Transmission Control Protocol / Internet Protocol*) est un modèle similaire à OSI sauf qu'il a seulement quatre couches. Le modèle OSI fait concurrence à TCP/IP comme façon d'interconnecter différentes marques d'ordinateurs et de réseaux à travers un réseau global commun. Cependant, le modèle TCP/IP est plus répandu et forme la base de l'Internet [SC02].

2.2.2 Introduction aux protocoles

Les couches des modèles OSI et TCP/IP sont définies par deux concepts : les services de communication et les protocoles de communication. Un service de communication offre aux couches supérieures un ensemble de services tel que le transfert de données, le routage, la gestion des sessions, etc. Un protocole de communication est un ensemble bien défini de règles et de formats sémantiques et syntaxiques. Cet ensemble détermine le comportement d'une entité durant l'exécution des fonctions offrant les services de communication et interchangeant l'information avec les autres entités participantes [CEN99].

Il existe différentes technologies de composantes de système qui ont des propriétés et des fonctionnalités spécifiques. L'utilisation des différents protocoles de communication assure une interopérabilité technique entre ces différentes technologies.

TCP/IP est une suite de protocoles et d'applications qui supportent la grande majorité des réseaux dans le monde. Toutes les données qui traversent Internet suivent les règles de la technologie de réseau TCP/IP. TCP et IP sont les protocoles les plus importants d'Internet, ils établissent une méthode pour diffuser les données à travers l'Internet et pour vérifier l'intégrité de la transmission des données [SC02].

2.2.3 Les protocoles de sécurité sur l'Internet

Les protocoles de sécurité se placent dans les différentes couches de modèle TCP/IP et utilisent les algorithmes cryptographiques pour assurer la sécurité des communications. Les protocoles de sécurité supportent les services de sécurité en communiquant les informations reliées à la sécurité et en fournissant une sécurité « *bout à bout* » entre les partis impliqués [CEN99]. C'est grâce aux protocoles de sécurité que l'exécution des transactions d'affaires sécuritaires est possible sur l'Internet. Les protocoles de sécurité les plus importants sont : IPSec (*Internet Protocol Security Protocol*), PPTP (*Point-to-Point Tunnelling Protocol*), SET (*Secure Electronic Transmission*), S/MIME (*Secure Multipurpose Internet Message Extensions*), SSH (*Secure Shell Protocol*) et SSL (*Secure Socket Layer*) [SC02]. L'annexe A contient une courte description de quelques-uns de ces protocoles.

2.2.4 Exemple d'un protocole de sécurité : S/MIME

MIME (*Multipurpose Internet Mail Extensions*) est un ensemble de spécifications qui permettent aux utilisateurs d'échanger des messages de courrier électronique incluant des textes à caractères différents et des fichiers de formats différents. S/MIME (*Secure MIME*) ajoute un ensemble de spécifications qui permet de signer et de chiffrer les messages. La figure 2.2 montre les étapes de l'envoi d'un message en utilisant S/MIME [SC02] .

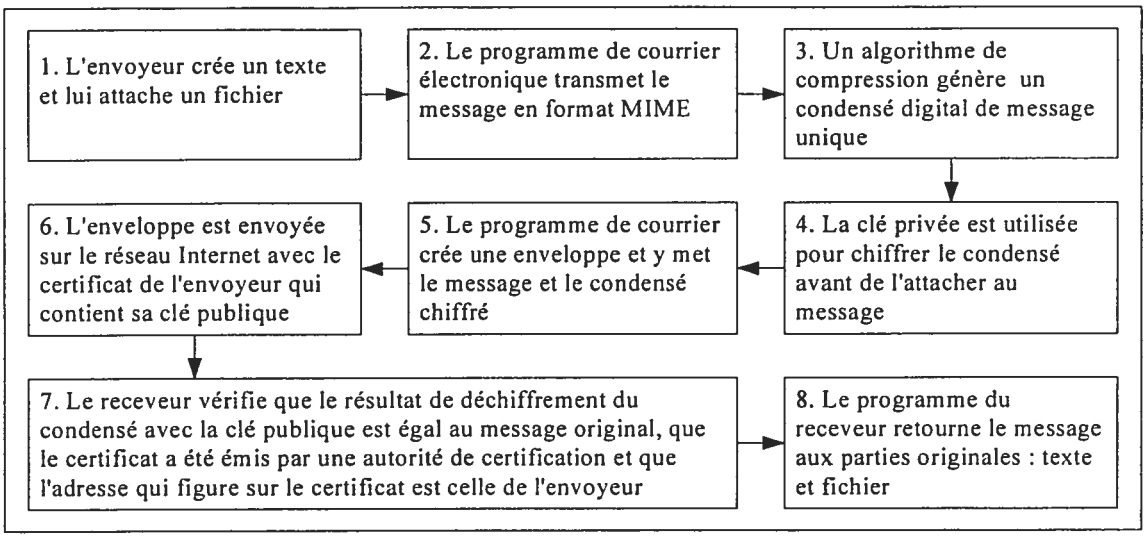

Figure 2.2 Les étapes de l'envoi d'un message en utilisant S/MIME, adapté de [SC02]

2.3 Le commerce électronique

2.3.1 Introduction au commerce électronique

L'organisation CEFACT (*United Nations Centre for Trade Facilitation and Electronic Business*) définit le commerce électronique comme suit : « Le commerce électronique consiste à entreprendre les affaires de manière électronique. Cela inclut le partage des informations structurées ou non structurées d'affaires par des moyens électroniques (comme le courrier électronique ou la messagerie, les technologies du *World Wide Web*, les systèmes de tribunes électroniques, *smart cards*, le transfert électronique de fonds et l'échange électronique de données) entre les fournisseurs, les clients, les établissements gouvernementaux et autres partenaires afin d'entreprendre et d'exécuter des transactions d'affaires et des activités de clientèle et administratives » [CEN01].

Le but du commerce électronique est de fournir un environnement d'affaires plus favorable. Le déploiement rapide de l'Internet, les coûts réduits et l'efficacité croissante d'autres réseaux globaux de communication d'affaires et de traitement de transactions rendent le commerce électronique de plus en plus répandu.

Le développement et l'adaptation des technologies de l'information, des technologies de télécommunication et des pratiques saines d'affaires sont importants pour

l'avancement du commerce électronique puisque cela augmente la confiance entre les partenaires et encourage l'industrie à exploiter davantage les opportunités existantes [CEN01].

2.3.2 L'interopérabilité du commerce électronique

Les avantages des standards et de l'interopérabilité dans l'économie traditionnelle étaient la réduction des coûts et des prix et l'augmentation de la compétition et des bénéfices des clients. Le rôle de l'interopérabilité sera encore plus important dans l'économie digitale basée sur les infrastructures des réseaux interopérables comme l'Internet [ABW99].

Alors que l'interopérabilité dans le monde physique est une question de standards et de compatibilités technologiques, la nature dynamique des interactions et des échanges du monde digital, souvent en temps réel, rend ce besoin d'interopérabilité encore plus présent. L'environnement global de l'Internet restera un monde théorique si les utilisateurs sont incapables de communiquer et d'effectuer des transactions d'affaires en raison de barrières technologiques et commerciales [ABW99].

2.3.3 Exemples d'interopérabilité dans l'économie digitale

Être une entreprise fonctionnant sur Internet implique parfois que tout le processus d'affaires de l'entreprise est intégré et connecté avec le reste de l'économie en ligne. Un détaillant électronique comme *Amazon.com* utilise des logiciels pour opérer son magasin *Web* mais utilise aussi de manière permanente des services auxiliaires de l'Internet comme les moteurs de recherche, les systèmes de paiements en ligne, les services d'enchère électronique et les supports de distribution en temps réel. Atteindre l'interopérabilité sur ce niveau de processus d'affaires est plus difficile que de l'atteindre sur le niveau de l'infrastructure technologique [ABW99].

Les applications de l'économie digitale dans le futur seront des applications qui permettront de trouver, d'assembler, et de personnaliser les produits et les services aux clients de manière individuelle et en temps réel. Ce genre de service est très difficile à gérer dans le monde physique traditionnel des affaires. Le besoin de l'interopérabilité

des technologies est évident si l'on veut faciliter les transactions des services et des produits qui impliquent différentes entreprises et consommateurs dans plusieurs marchés. Par exemple, une combinaison de billets d'avion, de chambres d'hôtel, de voitures louées, de billets de théâtre, peut être vendue en forfait personnalisé [ABW99].

2.4 Les standards et les spécifications

2.4.1 Les standards

Un standard, selon la définition de ISO, est un document, établi par un consensus et approuvé par un établissement reconnu, qui fournit, pour un usage commun et répété, des règles, des directives ou des caractéristiques pour les activités ou pour leurs résultats, dans le but d'atteindre un degré optimal d'ordre dans un contexte donné. Les standards doivent être basés sur les résultats consolidés de la science, de la technologie et de l'expérience, et doivent viser la promotion des avantages optimums pour la communauté.

2.4.2 Les spécifications

Une spécification technique, selon la définition de ISO, est un document qui prescrit les exigences techniques à remplir par un produit, un processus ou un service. Une spécification technique doit indiquer, lorsque approprié, les procédures par lesquelles il est possible de déterminer si les exigences ont été remplies ou pas. Une spécification technique peut être un standard, une partie d'un standard ou indépendante d'un standard.

Une différence entre les standards et les spécifications est que les standards sont validés par des établissements reconnus de standardisation nationaux, régionaux ou internationaux, et sont soumis à des règles clairement définies de vote. Les standards et les spécifications sont importants parce qu'ils facilitent l'interopérabilité et la coexistence entre les composantes techniques utilisées dans le monde de l'économie digitale et donc, encourage le développement de ce nouveau marché [CEN99].

2.4.3 Les standards actuels et l'interopérabilité

Pour faciliter le commerce électronique, de nombreux standards ont été créés et cela a causé une surabondance de standards. Cependant, ce trop-plein de standards nuit à l'interopérabilité qu'il tente de promouvoir.

Les différents partis impliqués dans la création des standards du commerce électronique comme les secteurs industriels, les organisations de standardisation et les consortiums semblent avoir créé des standards qui facilitent les transactions du commerce électronique pour leurs membres. Donc, les entités voulant entreprendre des transactions se retrouvent souvent avec des systèmes de commerce électronique basés sur différents standards de protocoles, de types de documents et de modèles de transactions [CEN01].

D'un autre côté, la solution qui consiste à définir un seul ensemble de documents, un seul protocole et un seul modèle de transaction n'est pas une solution pratique. Les différents secteurs de l'industrie ont souvent des raisons légitimes pour qu'existe une différence de format entre les différents documents qu'ils s'échangent et entre les modèles de transaction qu'ils utilisent en faisant une transaction de commerce électronique. De plus, les politiques en vigueur entre les différents établissements de standardisation ne permettent pas qu'un seul établissement s'approprie un standard regroupant tous les aspects d'un domaine aussi important que le commerce électronique [CEN01].

2.5 Les modèles existants du commerce électronique

2.5.1 Introduction aux modèles du commerce électronique

L'application correcte des règles et des standards communs du commerce électronique facilite les échanges entre les participants. Selon [CEN01], les modèles du commerce électronique qu'on appelle aussi architectures ou cadres (*frameworks*), sont une façon de représenter ces règles et ces standards. Ces modèles sont proposés par les établissements de standardisation, les consortiums d'industrie et les organisations privées.

Le rôle des modèles du commerce électronique est de faciliter l'interopérabilité et d'utiliser des mécanismes de sécurité, des protocoles de communication et des formats de messages communs. Il y a actuellement plusieurs systèmes du commerce électronique en opération qui n'implantent aucun modèle formellement documenté. Ces modèles « *de facto* » ont des conséquences négatives sur l'interopérabilité et sur l'avancement du commerce électronique en général [CEN01].

2.5.2 Comparaison de modèles du commerce électronique

Le groupe CEN/ISSS (*Comité Européen de Standardisation/Information Society Standardization System*) a suggéré dans [CEN01] un modèle de comparaison des modèles du commerce électronique. Le but du modèle de comparaison est de positionner les modèles de commerce électronique selon les blocs d'intérêt davantage couverts.

Les composantes de ce modèle, que nous remarquons sur la figure 2.3, sont des blocs d'intérêt qui touchent et affectent le domaine du commerce électronique. Nous notons que l'emplacement des blocs en couches horizontales n'a pas de signification temporelle et que les couches verticales sont des intérêts généraux qui affectent tous les autres blocs.

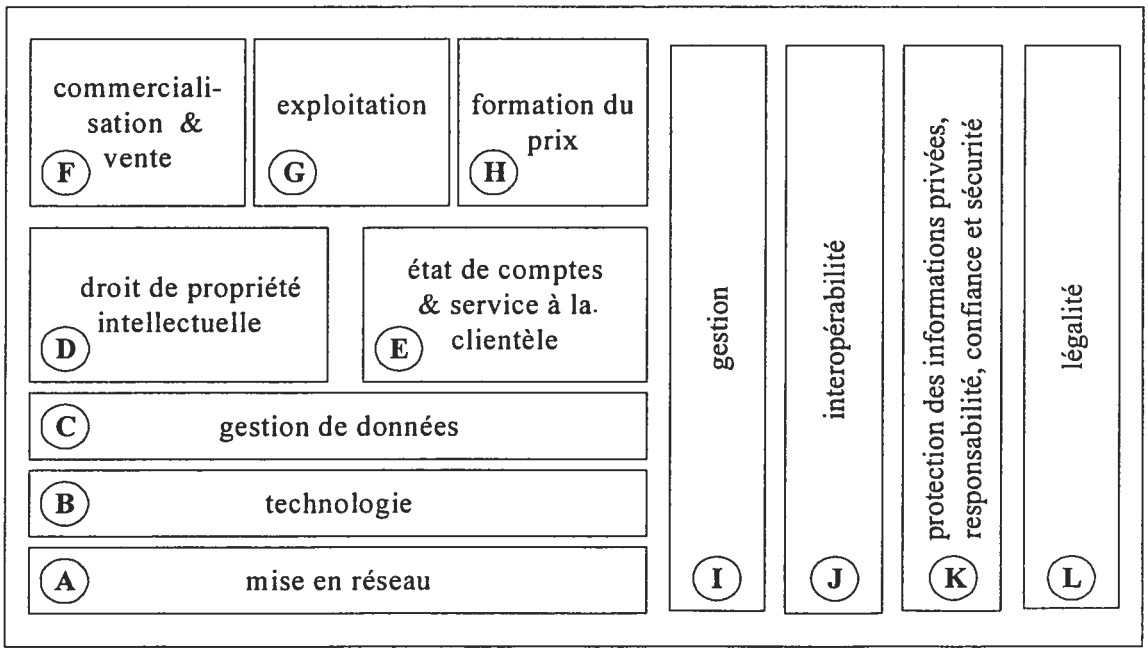

Figure 2.3 Le modèle de comparaison du groupe CEN/ISSS, traduit de [CEN01]

Le groupe CEN/ISSS identifie aussi dans la même référence [CEN01] une liste des modèles du commerce électronique placés selon les blocs d'intérêt du modèle précédent de comparaison. Le tableau 2.1 résume la liste des modèles et leurs relations aux blocs d'intérêts. Les critères que le groupe CEN/ISSS a utilisé pour inclure un modèle dans cette liste étaient la disponibilité publique des spécifications et l'existence des implantations de ces spécifications sur le marché. Nous allons choisir un modèle de ce tableau pour l'implantation de SecAdvise. La liste aide à classer et à comprendre le but des systèmes du commerce électronique, mais elle n'est pas exhaustive.

	Numéros de blocs selon la figure 2.5.2.1											
	A	B	C	D	E	F	G	H	I	J	K	L
Modèles Générales												
The Biztalk framework		√										
CEN/ISSS Building Blocks							√	√		√		√
EbXML Technical Architecture		√					√			√		
The Commerce Net eCo Framework			√				√			√		
IMPRIMATUR Business Model				√								√
Industrial Data Framework (STEP)			√		√	√	√					
Java EC Framework					√		√			√	√	
OMG E-Commerce Domain Specifications							√			√	√	
Open – edi Reference Model (ISO 14662)							√			√		
SPIRIT	√	√										
Modèles d'exploitation												
Ad Hoc Functional and Process Models							√			√		
IOTP– Internet Open Trading Protocol IETF							√	.		√		
Open Applications Group XML Framework							√			√		
OBI (The Open Buying on the Internet)							√			√		
RosettaNet	√	√	√	√	√	√	√	√	√	√	√	√
SEMPER			√				√				√	√
Modèles de paiement												
Electronic Payment Technologies					√		√	√				

SET-Secure Electronic Transaction							√					
Trading & Payment model in TC 224 Report							√				√	
Modèles de sécurité												
PKIX											√	
Security model in TC 224 Report											√	
Modèles sans fil												
MeT		√									√	

Tableau 2.1 Les modèles les plus répandus du commerce électronique, synthétisés de [CEN01]

2.6 L'aviseur de mécanismes de sécurité SecAdvise

2.6.1 Le modèle de confiance de Robles

Selon Robles dans [SR01], il y a encore un manque de sécurité dans l'économie digitale où des interactions électroniques complexes et distribuées d'affaires se passent entre plusieurs participants et à travers plusieurs domaines d'affaires. Ce problème de sécurité est une partie d'un plus grand problème, celui de la confiance entre les participants.

Développer la confiance demande une méthodologie qui détermine les types de confiance exigés et qui détermine comment transférer cette confiance de façon efficace à l'implantation de l'application. Le modèle proposé définit un espace de problème de confiance et relie cet espace à des mécanismes de sécurité de manière à protéger les systèmes et à augmenter la confiance qu'on porte à leur égard.

Un espace de problème de confiance (*Trust Problem Space; TPS*) est l'ensemble de toutes les situations possibles d'un système dans un contexte donné où les utilisateurs ont des problèmes de confiance envers les autres utilisateurs ou envers l'environnement d'exécution. L'espace de problème de confiance inclut les attaques, les tromperies, les mauvais usages, etc. L'objectif est d'identifier les évènements indésirables qui risquent d'arriver, leur probabilité et la sévérité des conséquences de ces occurrences indésirables.

Une unité de confiance (*Trust Unit; TU*) est une unité logique qui représente une solution partielle ou complète ou une contre-mesure pour n'importe quel sous-espace de problème de confiance (*Trust Problem Sub Space; TPSS*). Une unité de confiance peut impliquer un protocole cryptographique, un mécanisme de contrôle ou une infrastructure. Une unité de confiance peut dépendre d'autres unités de confiance (être une partie d'une plus grande structure). La taille de l'unité de confiance dépend du niveau de détail du modèle de confiance.

Une solution de confiance (*Trust Solution; TS*) couvre l'espace de problème de confiance (TPS) et remplit les exigences de confiance. Une solution de confiance (TS) est un ensemble d'unités de confiance (TU) qui couvre totalement les sous-espaces de problème de confiance (TPSS). Plusieurs solutions de confiance peuvent couvrir le même problème de confiance, mais il est possible de déterminer la complexité de chaque solution et de choisir une solution optimale parmi elles. Les figures 2.4 et 2.5 montrent respectivement les notations utilisées dans le modèle de Robles et les relations entre elles.

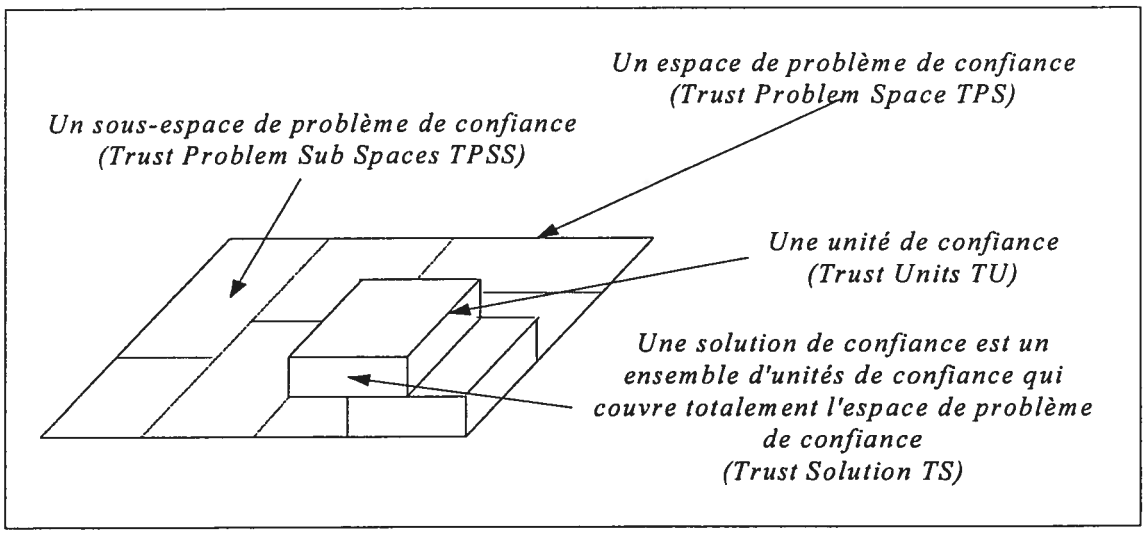

Figure 2.4 Le modèle de confiance de Robles, adapté de [SR01]

La méthodologie du modèle (*The Trust Model*) :

1. Définir l'espace du problème de confiance (TPS), les exigences et les vulnérabilités de confiance. Cet espace inclut les différents types d'attaque et de

vulnérabilité associés à la tricherie et au mauvais usage des ressources des systèmes.

2. Définir les unités de confiance (TU) qui représentent des solutions partielles pour des sous-espaces du problème de confiance (TPSS). Ceci inclut les protocoles cryptographiques, les mécanismes de controle et les infrastructures.
3. Choisir et combiner quelques unités de confiance (TU) pour composer une solution de confiance (TS) qui couvre entièrement l'espace du problème pour le système. Chacune des (TS) est une combinaison de plusieurs (TU), les (TU) peuvent, dans certains cas, dépendre les uns des autres. La cardinalité de chaque (TS) dépend de la granularité des (TU) utilisées. Le nombre total de (TS) dépend de la qualité et de la quantité des (TU) fournis au système.
4. Au cas où plusieurs solutions existeraient, une solution optimale devrait être choisie.

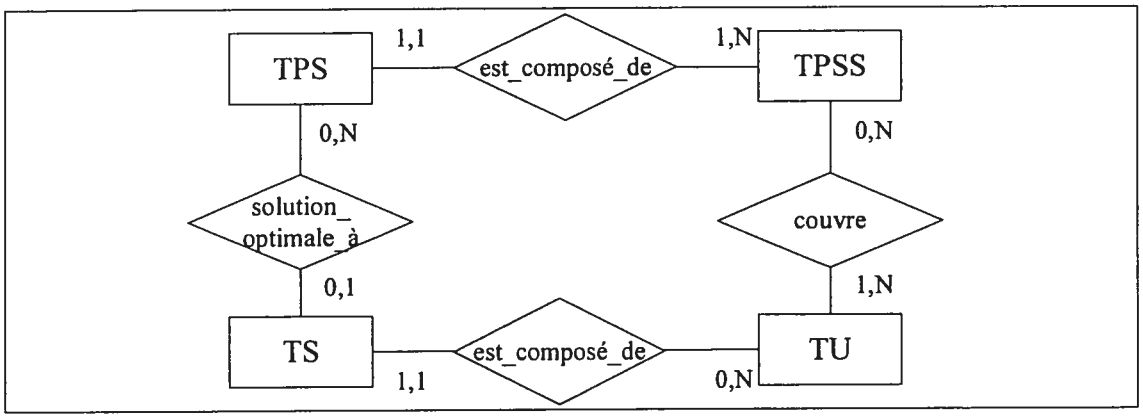

Figure 2.5 Un modèle entité-relation qui montre les relations entre les notations du modèle de Robles

2.6.2 L'approche SecAdvise

L'architecture préliminaire du système SecAdvise qui a été proposée dans [RS02] ne se limite pas à un domaine d'application spécifique. Le rôle des entités SecAdvise durant une transaction électronique est d'assurer un passage optimal entre l'étape de la définition des risques de sécurité et l'étape du choix des solutions à utiliser par les deux participants pour sécuriser la transaction en cours [RS02].

Les entités SecAdvise proposent aux utilisateurs des solutions qui ont pour but d'assurer les services de sécurité que les transactions nécessitent selon leur contexte, donc en

principe ces solutions ne doivent pas appartenir à une catégorie spécifique. Les solutions peuvent être des algorithmes cryptographiques, des protocoles de sécurité, des infrastructures de clés, etc. Cela peut être même une combinaison de ce qui précède selon le besoin et/ou le choix des utilisateurs [RS02].

SecAdvise est un gestionnaire de risques qui vise à augmenter la confiance des utilisateurs et faciliter l'interopérabilité des systèmes du commerce électronique. L'entité SecAdvise de chacun des deux participants dans une transaction tient compte des risques individuels du participant et du niveau de sécurité désiré et sélectionne localement les mécanismes de sécurité qui permettent d'exécuter la transaction sécurisée. Ensuite, les entités de SecAdvise des deux participants négocient entre elles les choix locaux de mécanismes de sécurité en vue de trouver une solution mutuelle de sécurité qui satisfait les deux partis et permet d'effectuer la transaction [RS02].

Une menace exploite la vulnérabilité d'un actif et un risque en résulte. La réduction des risques peut s'effectuer de plusieurs façons : réduire la vulnérabilité, utiliser un mécanisme qui élimine une vulnérabilité ou qui repousse une menace, etc. [RS02]. Nous définissons une gestion de risque dans SecAdvise comme étant une mesure (protection, prévention, détection, etc.) qui vise à protéger les actifs d'un participant (information, etc.) en réduisant ou en éliminant la vulnérabilité de ces actifs ou encore, en repoussant les menaces s'attaquant aux aspects vulnérables de ces actifs. Nous montrons un exemple d'une gestion de risque dans la figure 2.6.

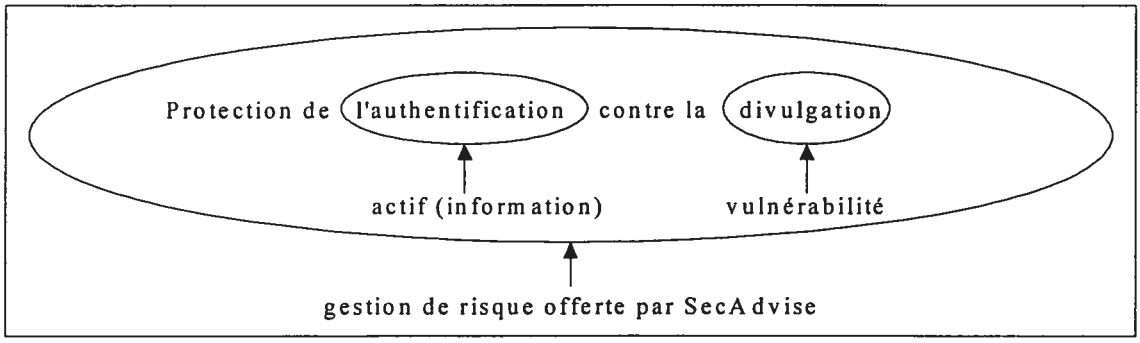

Figure 2.6 La gestion de risque dans SecAdvise

Notre définition de la gestion des risques nous permet d'appliquer le modèle de Robles dans SecAdvise de la même façon que dans la figure 2.7 : le système de l'usager est sujet à un ensemble de risques de sécurité qui requièrent certaines gestions des risques. Chacune de ces gestions des risques peut être réalisée par un modèle d'interaction de sécurité qui est un moyen d'exécuter un service de sécurité. Les modèles d'interaction de sécurité sont décrits par des standards et des spécifications. Un ensemble de ces standards et spécifications sera la solution au problème de sécurité.

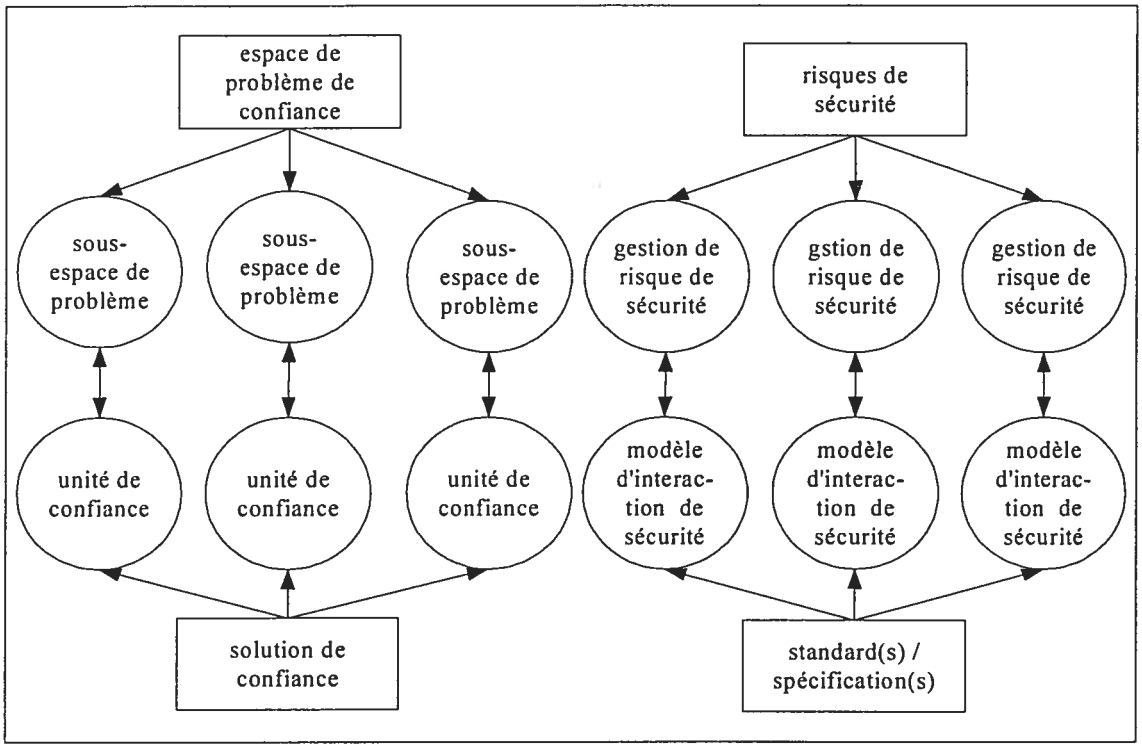

Figure 2.7 Application du modèle de Robles à SecAdvise

Dans notre conception du système, détaillée ultérieurement, nous nous assurons que les mécanismes de sécurité suggérés par SecAdvise sont appropriés aux gestions des risques exigées. Nous donnons aussi à l'usager la possibilité de choisir un pourcentage de la couverture des risques selon son estimation de la probabilité d'une menace et d'une perte potentielle.

2.6.3 La modélisation formelle de SecAdvise

Le chapitre 3 montre la modélisation formelle du modèle comme elle a été proposée dans [RS02] et [RS02a]. En principe, la sélection des unités de confiance (TU) doit être

conforme aux formules mentionnées pour que l'architecture soit fonctionnellement applicable. Cette modélisation formelle est préliminaire et peut être l'objet de modifications ultérieures.

2.6.4 Mise en contexte de SecAdvise (face aux modèles existants)

Nous constatons que SecAdvise est une architecture générale. Parmi les 12 blocs d'intérêts du commerce électronique de la figure 2.3, on remarque que les principes de SecAdvise s'adressent surtout aux questions du bloc K (protection des informations privées, responsabilité, confiance et sécurité) et du bloc J (interopérabilité). Ces blocs sont des blocs d'intérêt général et affectent donc tous les autres blocs.

Néanmoins, l'approche SecAdvise se distingue des autres modèles existants puisqu'elle combine tous ces points:

- SecAdvise repose sur le modèle méthodologique de confiance de Robles. Cela implique qu'au-delà des concepts traditionnels de la sécurité, SecAdvise couvre les aspects sociaux de la confiance. Les solutions de sécurité suggérées par SecAdvise évaluent les besoins de sécurité dans une optique plus large.
- SecAdvise ne dépend pas d'une architecture spécifique, Il peut donc être jumelé à d'autres modèles pour les aider à trouver les solutions de sécurité convenables et ce, sans qu'il intervienne dans leur fonctionnement.
- SecAdvise a une nature dynamique, il a la possibilité de négocier, automatiquement et de façon indépendante, les paramètres de sécurité à utiliser entre des partis voulant entreprendre des transactions d'affaires sécurisées à travers différents domaines.

Chapitre 3. Méthodologie et conception

3.1 Vue générale de SecAdvise

Nous considérons que le système a trois utilisateurs potentiels : l'initiateur de la transaction, le participant choisi par l'initiateur et l'administrateur du système. C'est l'initiateur qui définira le contexte de la transaction avant de l'envoyer au participant. Chaque propriétaire d'un système SecAdvise a les coordonnés des autres propriétaires inscrits dans sa base de données, mais les participants peuvent avoir différentes applications et divers systèmes de support. Nous considérons aussi que les participants se font confiance mutuellement.

Selon [RS02], SecAdvise vise à assurer un niveau de sécurité optimal dans une transaction électronique tout en restant flexible. Alors, nous supposons dans ce travail que la structure de SecAdvise ne se limite pas aux applications du commerce électronique, d'autres applications peuvent être intégrées comme les applications de vote électronique ou de vente aux enchères.

Nous montrons dans la figure 3.1 une vue générale de notre vision de SecAdvise. Comme le dévoile la figure 3.1, l'usager (l'initiateur ou le participant) commencera la transaction en utilisant une application haut niveau qui donnera ensuite la relève au système SecAdvise. L'utilisateur fournira alors au système un ensemble de risques locaux de sécurité et des critères de choix de solution. Par la suite, le système calculera un ensemble de solutions locales optimales à utiliser selon le contexte de la transaction en cours; ces solutions peuvent être des mécanismes de sécurité, des protocoles, des infrastructures ou une combinaison des trois.

La prochaine étape sera l'association mutuelle où le système de l'initiateur recevra graduellement des éléments de l'ensemble de solutions locales de l'autre participant et tentera de trouver une solution commune satisfaisante aux deux partis. Si une solution mutuelle existe, alors la transaction sera prête à commencer et sera sécurisée grâce à la

solution trouvée. En cas contraire, la transaction sera abandonnée. On note que les ensembles de solutions locales des deux partis peuvent être égaux même si leurs risques de sécurité ne le sont pas. On note aussi que, pour des raisons de sécurité, le participant évitera d'envoyer l'ensemble complet de ses solutions locales à l'initiateur dès le début de la négociation. Au lieu de cela, le participant commencera par envoyer sa meilleure solution locale et attendra la réaction de l'initiateur avant d'envoyer d'autres solutions alternatives.

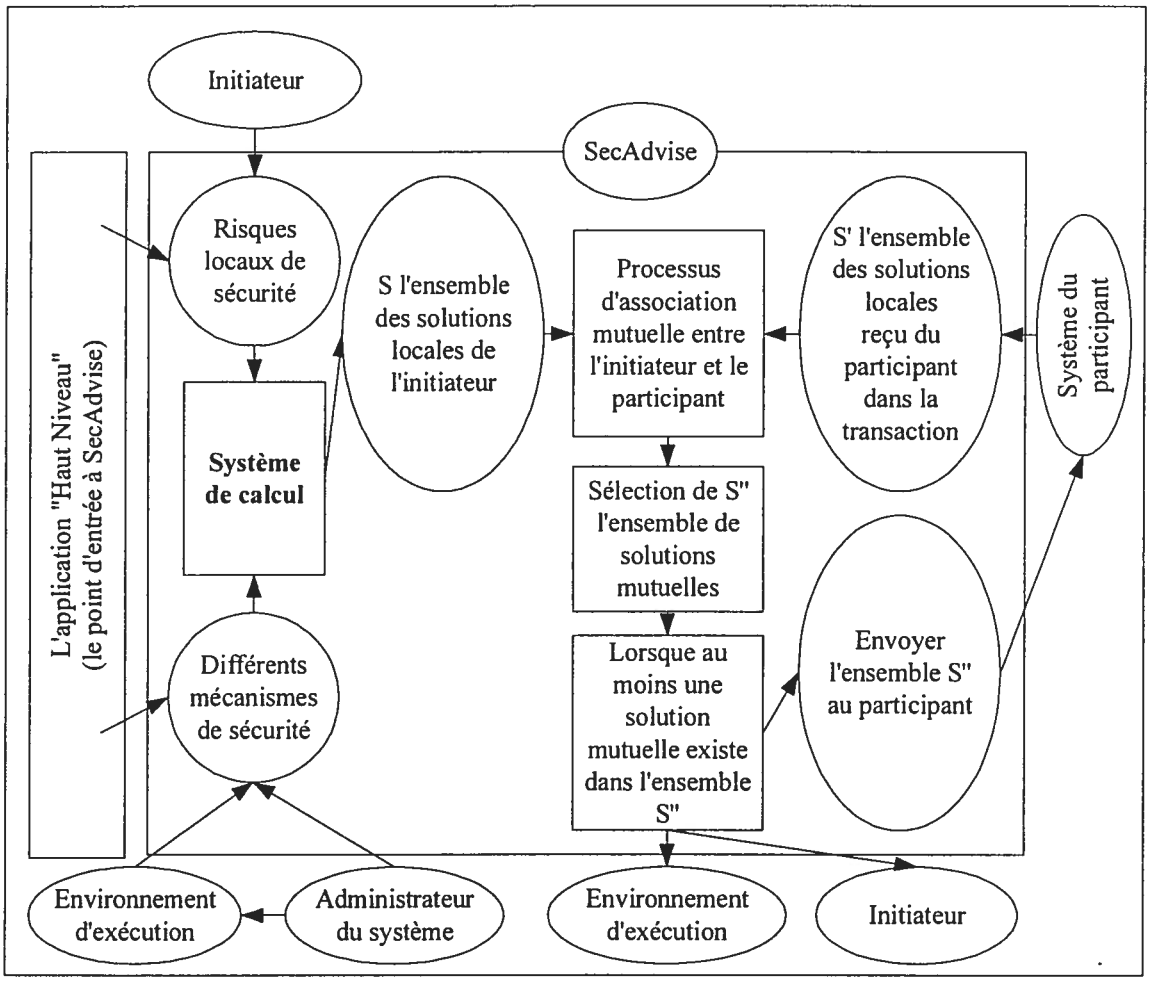

Figure 3.1 Une vue générale de SecAdvise - le côté de l'initiateur

3.2 Le modèle de sécurité de SecAdvise

3.2.1 Justification et choix

Parce qu'une partie importante de l'architecture de SecAdvise concerne les questions de sécurité, nous avons décidé d'y intégrer un modèle standard de sécurité. Nous avons

choisi le modèle de sécurité CEN/TC 224 –ISO/TC 68/SC 6 du comité européen de standardisation. Il s'agit d'un modèle sur lequel peut se baser l'implantation des systèmes de sécurité de commerce électronique [CEN99].

Le modèle CEN/TC 224 –ISO/TC 68/SC 6 a l'avantage d'être, en grande partie, axé sur le traitement des demandes de sécurité et des moyens de les atteindre indépendamment des types et des étapes des transactions effectuées. Un autre avantage de ce modèle est que la méthodologie qu'il définit peut être utilisée pour la description de tous les aspects de sécurité applicables au commerce électronique.

En tenant compte des demandes de standardisation et de spécification du commerce électronique, ce modèle permet le développement d'applications valides du point de vue technique et l'amélioration des conditions de leur interopérabilité et coexistence [CEN99].

3.2.2 Le modèle de sécurité CEN/TC 224 –ISO/TC 68/SC 6

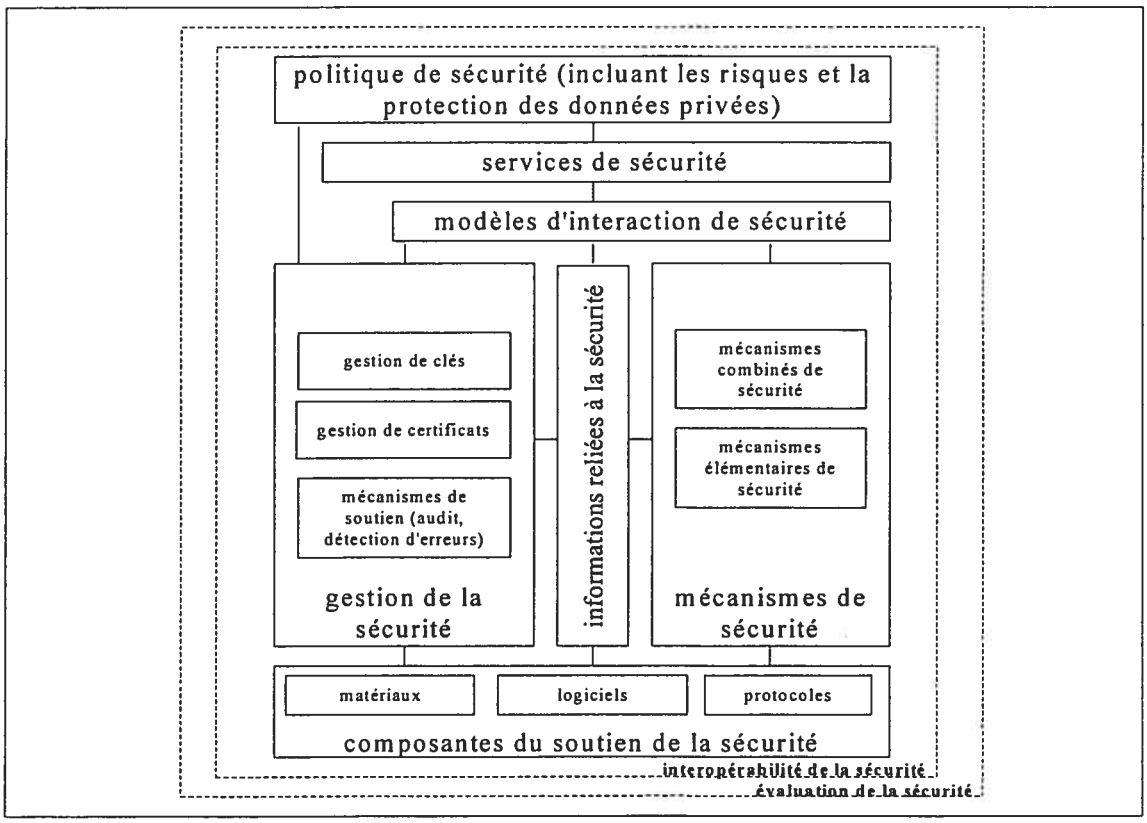

Figure 3.2 Le modèle de sécurité CEN/TC 224 –ISO/TC 68/SC 6, traduit de [CEN99]

La figure 3.2 montre le modèle de sécurité CEN/TC 224 –ISO/TC 68/SC 6. Nous montrons dans la figure 3.3, synthétisée à partir de [CEN99], les relations entre les différentes composantes de ce modèle de sécurité. Le schéma de la base de données de SecAdvise ainsi que le calcul de l'ensemble des solutions locales de sécurité seront basés sur ce modèle. La référence [CEN99] décrit ce modèle de sécurité en détail.

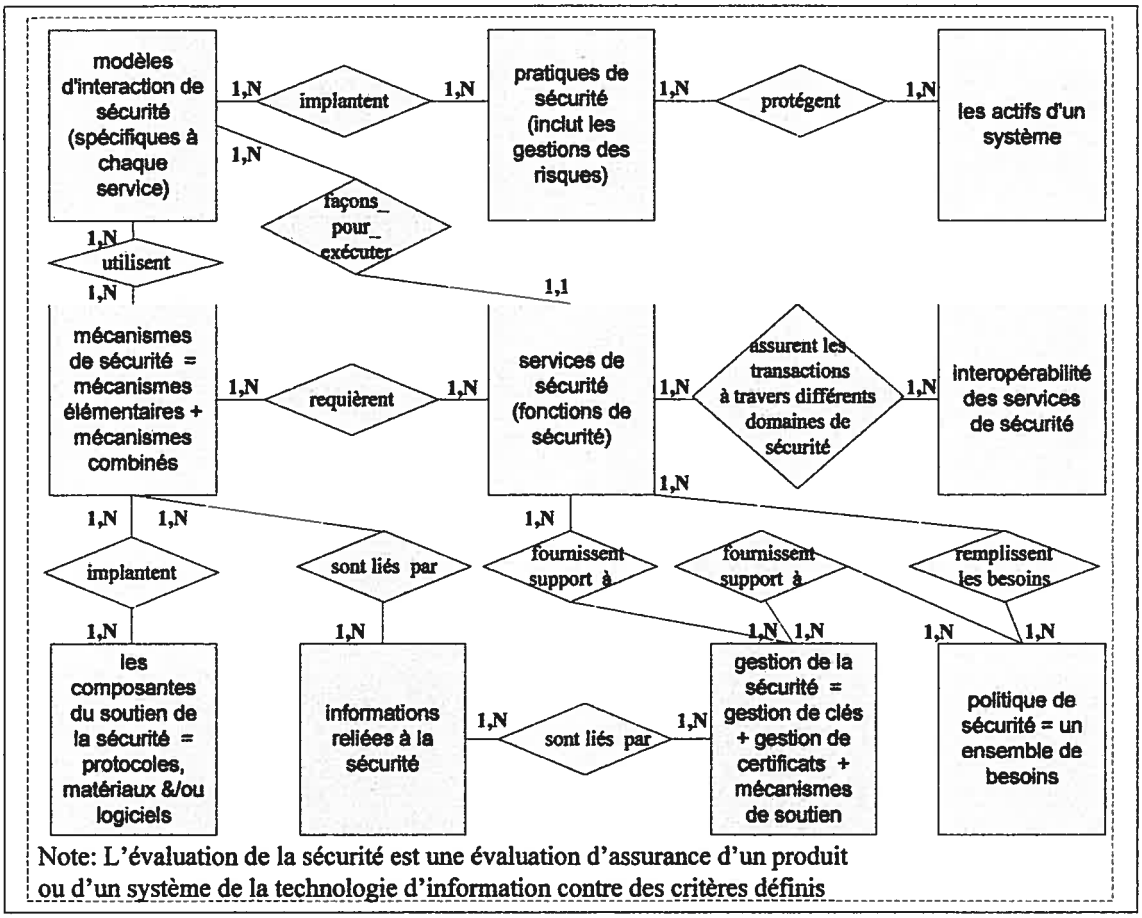

Figure 3.3 Un modèle entité–relation qui montre les relations entre les composantes du modèle de sécurité

3.2.3 Le protocole de communication

Dans cette section nous concevons le protocole de communication de SecAdvise. Pour chaque tentative d'association mutuelle, il y aura deux partis dont l'un sera l'initiateur et l'autre sera le participant choisi par le premier. Dans une communication à entreprendre entre deux partis, une entité de SecAdvise sera soit l'initiateur, soit le participant, mais pas les deux. Toute communication multilatérale comprend plusieurs communications bilatérales. Alors, si la transaction implique plus de deux participants, différents fils d'exécution *(threads)* du programme tenteront de trouver l'association mutuelle entre

chaque paire. La figure 3.4 montre un exemple d'association mutuelle entre trois participants.

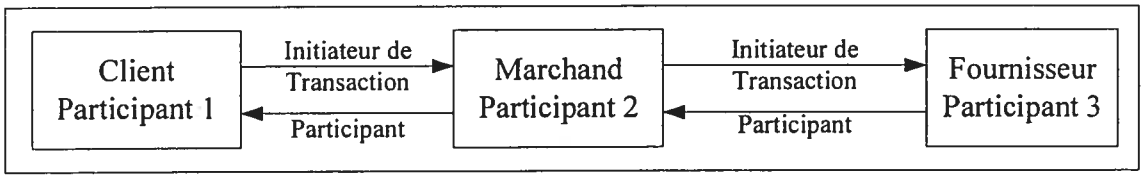

Figure 3.4 Tentative d'association mutuelle entre trois participants

Nous avons décidé de constituer le protocole de communication de SecAdvise à partir d'une suite de messages échangés entre l'initiateur et le participant, l'ensemble des messages est défini et après chaque message un autre message accuse la réception. Nous supposons que chaque message, sans accusation de réception reçue dans l'espace d'un certain délai, sera renvoyé jusqu'à trois fois. Si l'accusé de réception n'est toujours pas reçu, la communication sera abandonnée. Pour que les messages soient clairement interprétés, ils ont un nom fixe et transmettent avec eux le nom et l'adresse d'origine et du destinataire ainsi que le numéro de référence de la transaction en cours. Le tableau 3.1 donne une liste des messages échangés. Cette décomposition du protocole de communication en messages assure la flexibilité des scénarios d'échange entre les participants. Nous montrons dans la figure 3.5 quelques scénarios possibles de communication.

#	Nom du message
1	Proposer une transaction
2	Refuser une communication
3	Refuser une transaction
4	Approuver une transaction
5	Confirmer une transaction
6	Proposer une solution locale
7	Demander une solution alternative
8	No solution alternative
9	Confirmer l'association mutuelle
10	Solution complémentaire à demander
11	Accepter une solution complémentaire
12	Refuser une solution complémentaire
13	Commencer la transaction
14	Abandonner une transaction

Tableau 3.1 Une liste des messages que les participants s'échangent

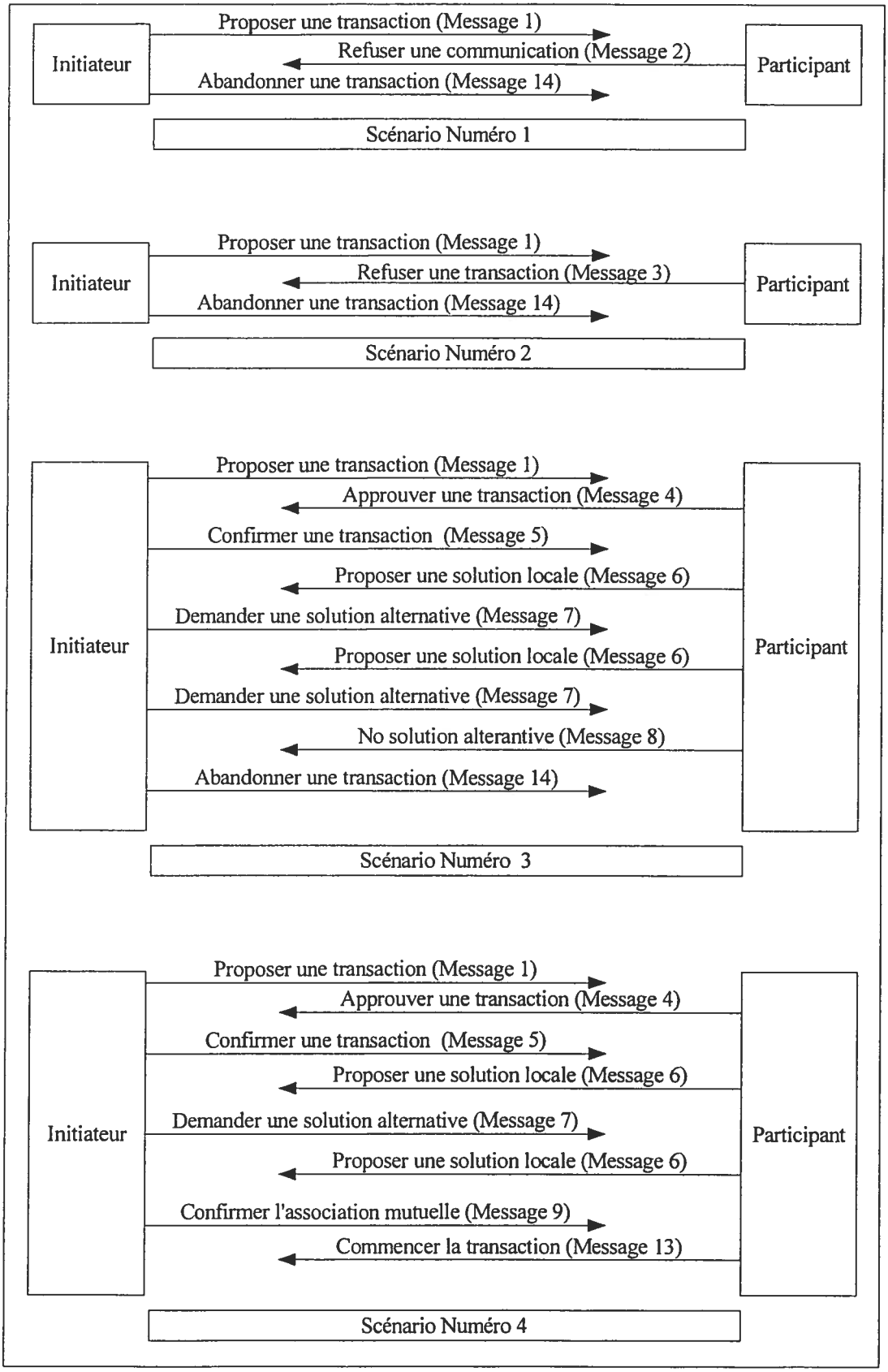

Figure 3.5 Quelques scénarios du protocole de communication

Nous donnons dans le tableau B.1 de l'annexe B une liste détaillée des significations des messages du protocole de communication. Cette liste permet de construire les scénarios désirés selon le déroulement de la communication.

3.3 La conception de SecAdvise

3.3.1 Introduction

Notre prototype de SecAdvise aura plusieurs interfaces graphiques pour illustrer en détail les messages du protocole de communication et les étapes de l'association mutuelle entre deux participants. Chaque usager interagira avec le prototype de près et décidera du flux des messages échangés au fur et à mesure, selon les messages reçus de l'autre participant. Dans le prototype, l'usager aura la possibilité de définir le contexte de la transaction voulue ainsi que les éléments de calcul de l'ensemble des solutions locales. La version définitive du programme sera, en principe, différente de sorte que l'administrateur du système configurera plusieurs profils d'utilisation et les usagers interagiront moins avec le programme. Au moment de la transaction, les usagers des applications haut-niveau choisiront les profils qui conviennent aux transactions voulues et SecAdvise prendra automatiquement la relève et procédera pour trouver une association mutuelle avec l'autre entité à l'autre bout de ligne. La transition entre la version manuelle du prototype et la version automatique du programme est facile à faire lorsque toutes les interactions des usagers sont faites via des boutons aux tâches bien définies. Nous montrons en bref dans la figure 3.6 le déroulement de ce processus.

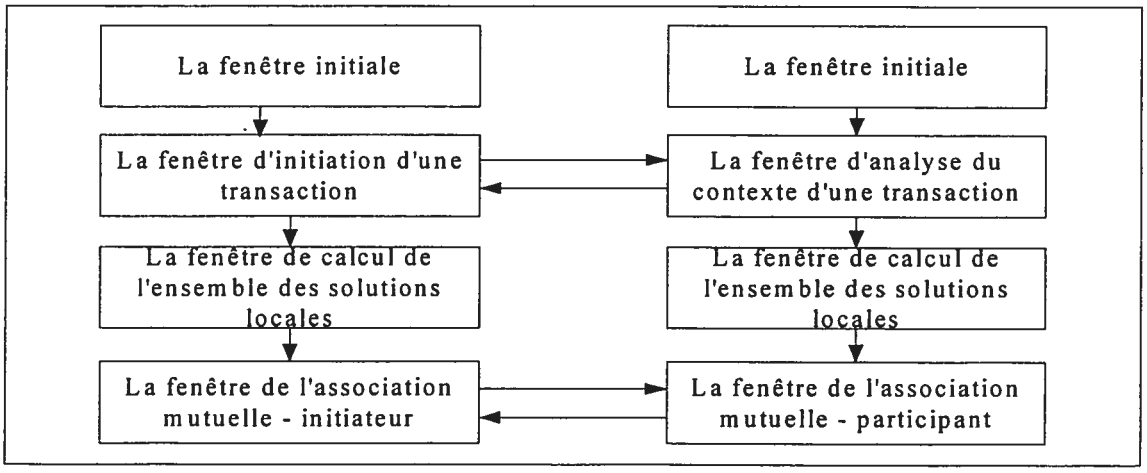

Figure 3.6 Le déroulement du processus de SecAdvise

3.3.2 Le diagramme de cas d'utilisation

Le rôle de ce diagramme est de fournir une explication haut niveau de la relation entre le système et le monde extérieur. Les cas d'utilisation montrés dans ce diagramme sont des moyens pour spécifier les usages requis d'un système en mettant l'accent sur les buts des processus et en identifiant les fonctions clés du système [TAP02]. La figure 3.7 montre les cas d'utilisation que nous prévoyons pour SecAdvise. Comme le montre la figure 3.7, en plus de l'application haut niveau et des devises qui échangent les informations avec le système, il y a trois autres acteurs humains : l'initiateur, le participant et l'administrateur du système.

L'administrateur du système est responsable de la configuration des systèmes et de la mise à jour de la base de données (les cas d'utilisation 1 et 2).

C'est l'application haut niveau qui commence la transaction et, ensuite, qui lance SecAdvise (le cas d'utilisation 3). Après cela, l'initiateur commence son interaction avec le système en définissant le contexte de la transaction (le cas d'utilisation 4), le participant doit approuver le contexte défini par l'initiateur pour que la transaction ait lieu.

L'initiateur et le participant calculent, chacun de son côté, l'ensemble des solutions locales selon leurs besoins de sécurité respectifs (le cas d'utilisation 5). Nous remarquons que le calcul des solutions locales se base sur les informations du contexte de la transaction et les informations contenues dans la base de données (les relations de dépendance entre les cas d'utilisation 5, 1 et 4).

L'association mutuelle vise à trouver une solution mutuelle qui satisfait les critères de sécurité des deux participants. Le participant commence l'association mutuelle en envoyant une de ses solutions locales de sécurité à l'initiateur (le cas d'utilisation 6). L'initiateur compare la solution locale reçue du participant avec son propre ensemble de solutions locales en vue de trouver des solutions en commun (le cas d'utilisation 7 et la relation de dépendance entre les cas d'utilisation 5 et 7).

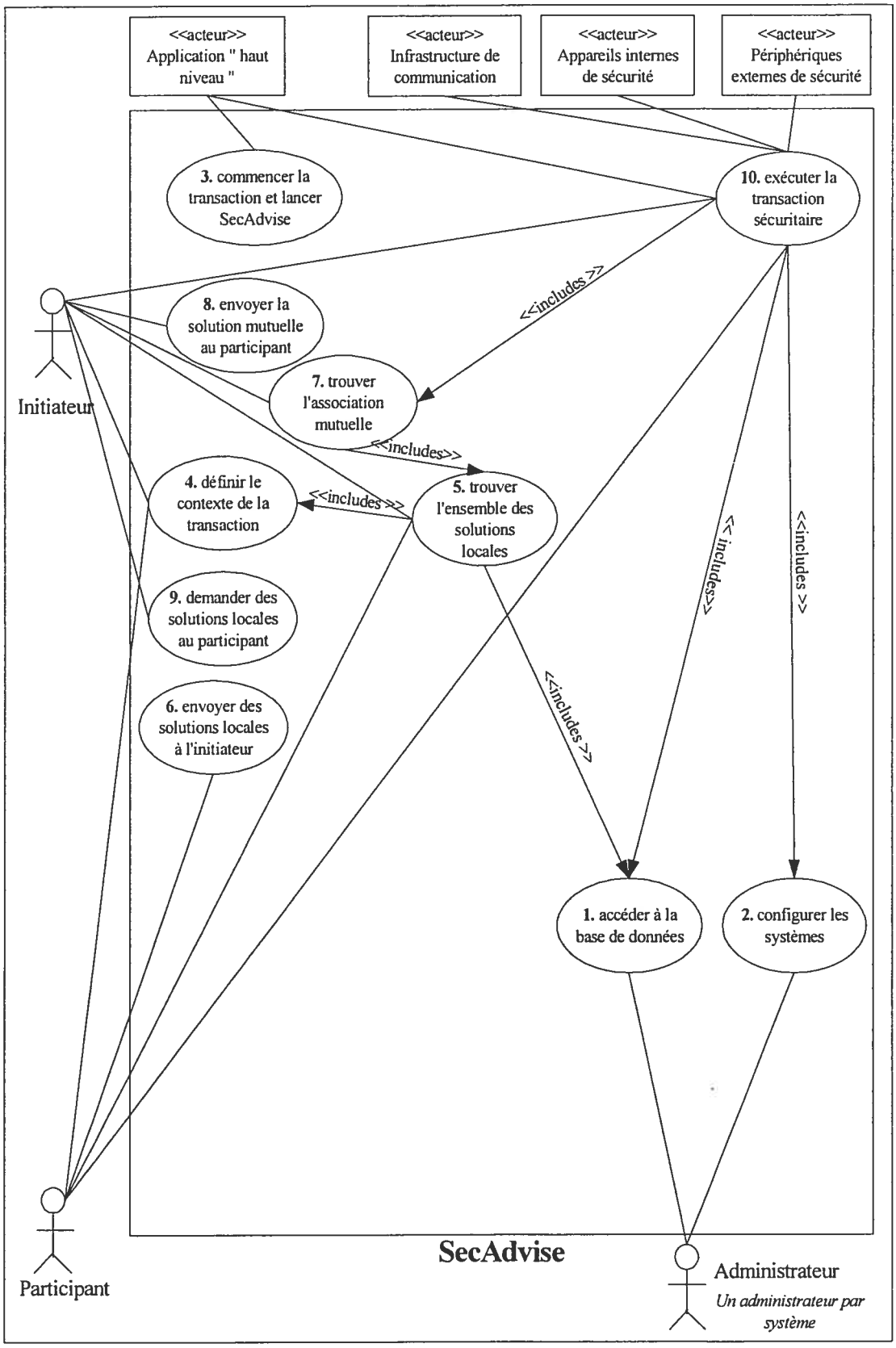

Figure 3.7 Le diagramme de cas d'utilisation du système

Si l'initiateur réussit à trouver une association mutuelle, il envoie la solution trouvée au participant (le cas d'utilisation 8). Sinon, l'initiateur demande au participant de lui envoyer d'autres alternatives de solutions locales (le cas d'utilisation 9).

Lorsque la solution mutuelle existe, les applications des deux participants exécutent la transaction sécurisée avec cette solution (le cas d'utilisation 10). Dépendamment du type de solution trouvée, ce cas d'utilisation accédera aux informations de la base de données et aux informations des configurations.

Nous remarquons aussi que l'exécution de la transaction sécurisée implique l'infrastructure de communication et, selon la solution en question, les appareils internes et/ou externes de sécurité.

3.3.3 Le diagramme de paquetage (*package*)

Le rôle du paquetage est de représenter des sous-systèmes où chacun est un sous-ensemble cohésif de la totalité du système. La figure 3.8 montre les principales formes de paquetage du programme.

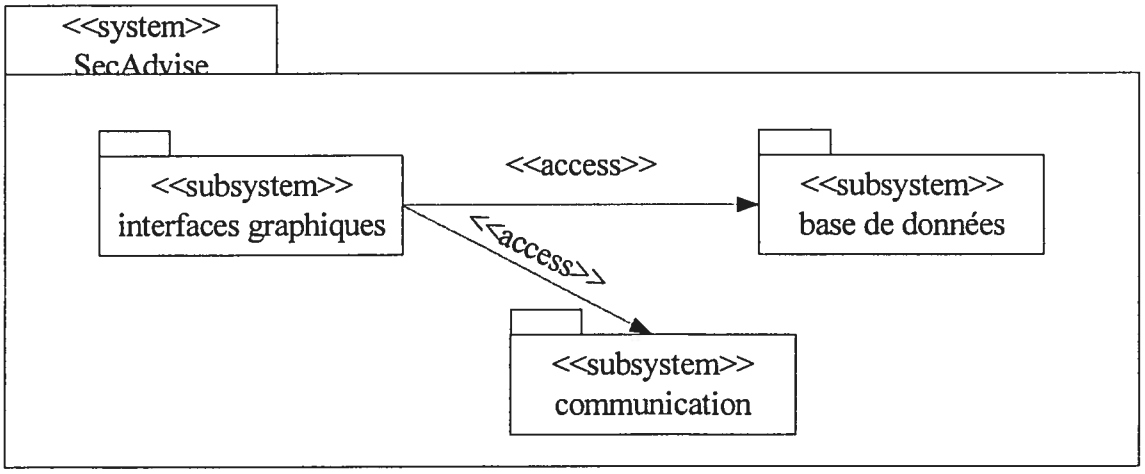

Figure 3.8 Le diagramme de paquetage du système

3.3.4 Les diagrammes de classe

Dans un système orienté objets, le diagramme de classe représente les classes du programme et leurs relations mutuelles [TAP02].

3.3.4.1 Le paquetage de la communication

La figure 3.9 montre les classes du paquetage de la communication, c'est la méthode *main()* du programme qui crée la classe de l'initiateur du gestionnaire de la communication. La classe du contexte de la transaction fait partie de ce paquetage parce que le contexte sera envoyé de l'initiateur au participant. Tous les objets qui envoient des messages utilisent la classe de l'implantation du gestionnaire de la communication pour le faire.

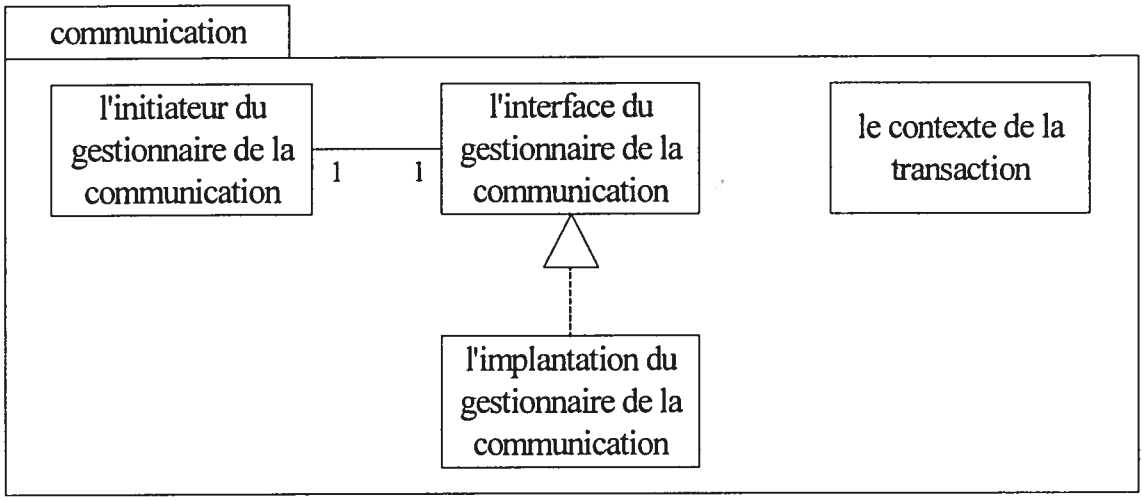

Figure 3.9 Le diagramme de classe du paquetage de la communication

3.3.4.2 Le paquetage des interfaces graphiques

La figure 3.10 montre les classes du paquetage des interfaces graphiques. Dans ce paquetage, on a la classe de la méthode *main()* du programme qui crée la fenêtre initiale de SecAdvise. À chacune des classes « fenêtre » de ce paquetage correspond une classe « action fenêtre » et on note que les actions de quelques fenêtres incluent la création d'autres fenêtres au besoin.

3.3.4.3 Le paquetage de la base de données

La figure 3.11 montre les classes du paquetage de la base de données. La plupart des classes ont la tâche d'importer des informations de la base de données au programme. Tous les objets du programme qui interagissent avec la base de données utilisent la classe du gestionnaire de la base de données pour le faire.

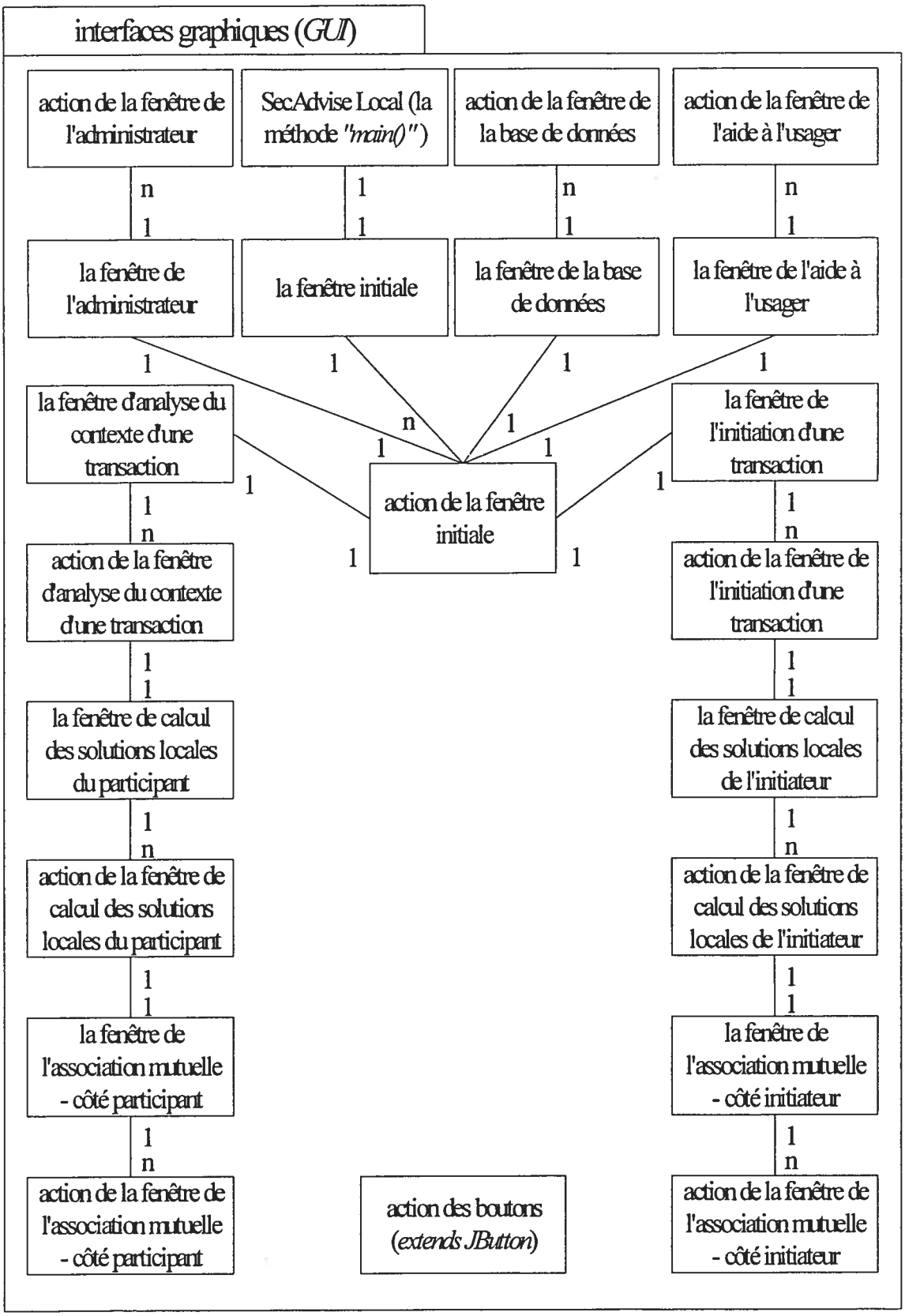

Figure 3.10 Le diagramme de classe du paquetage des interfaces graphiques

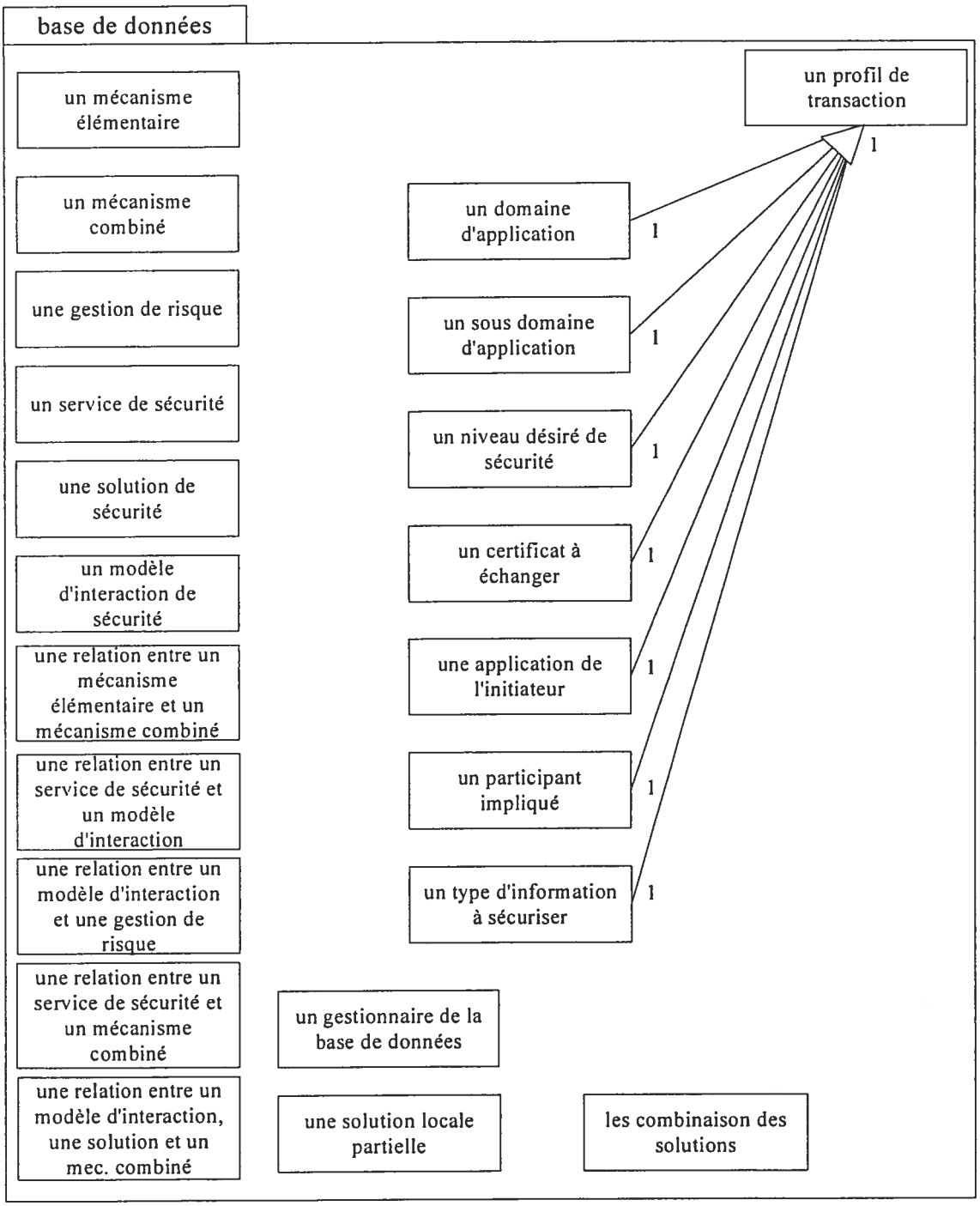

Figure 3.11 Le diagramme de classe du paquetage de la base de données

3.3.5 Le diagramme d'activité

Le diagramme d'activité décrit des processus logiques où chaque processus met en évidence une séquence de tâches et les décisions qui gouvernent quand et comment ces tâches sont réalisées [TAP02]. Les figures 3.12, 3.13 et 3.14 montrent le diagramme

d'activité global de SecAdvise. Nous rappelons que SecAdvise a trois utilisateurs potentiels : l'initiateur de la transaction, le participant choisi par l'initiateur et l'administrateur du système (figure 3.1). Nous remarquons dans la figure 3.12 comment les choix de l'usager dans la fenêtre initiale vont décider du cours des événements selon le rôle qu'il joue. La figure 3.13 met l'accent sur les activités d'un initiateur d'une transaction et la figure 3.14 met l'accent sur les activités d'un participant dans une transaction.

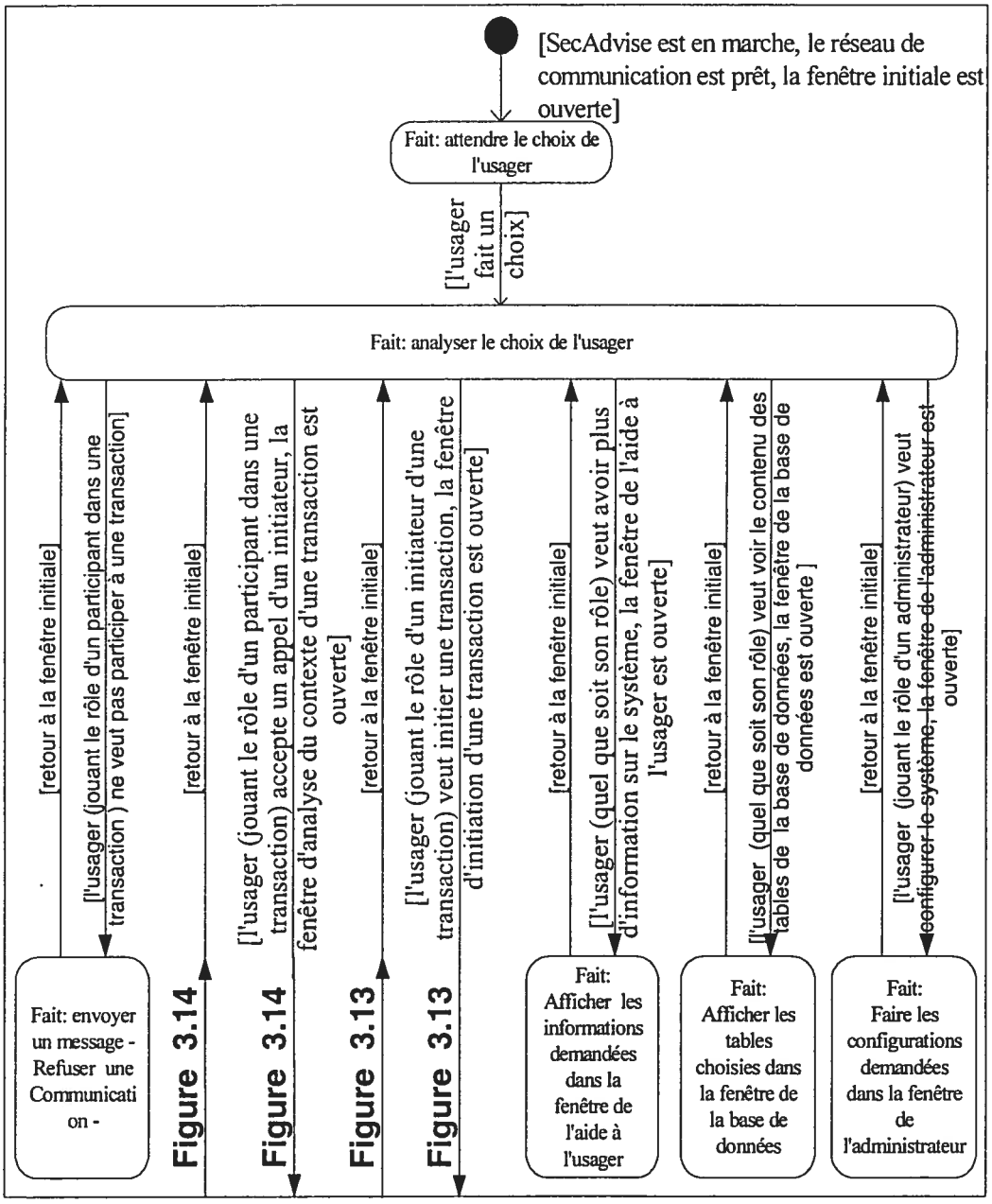

Figure 3.12 Le diagramme d'activité initial d'un usager

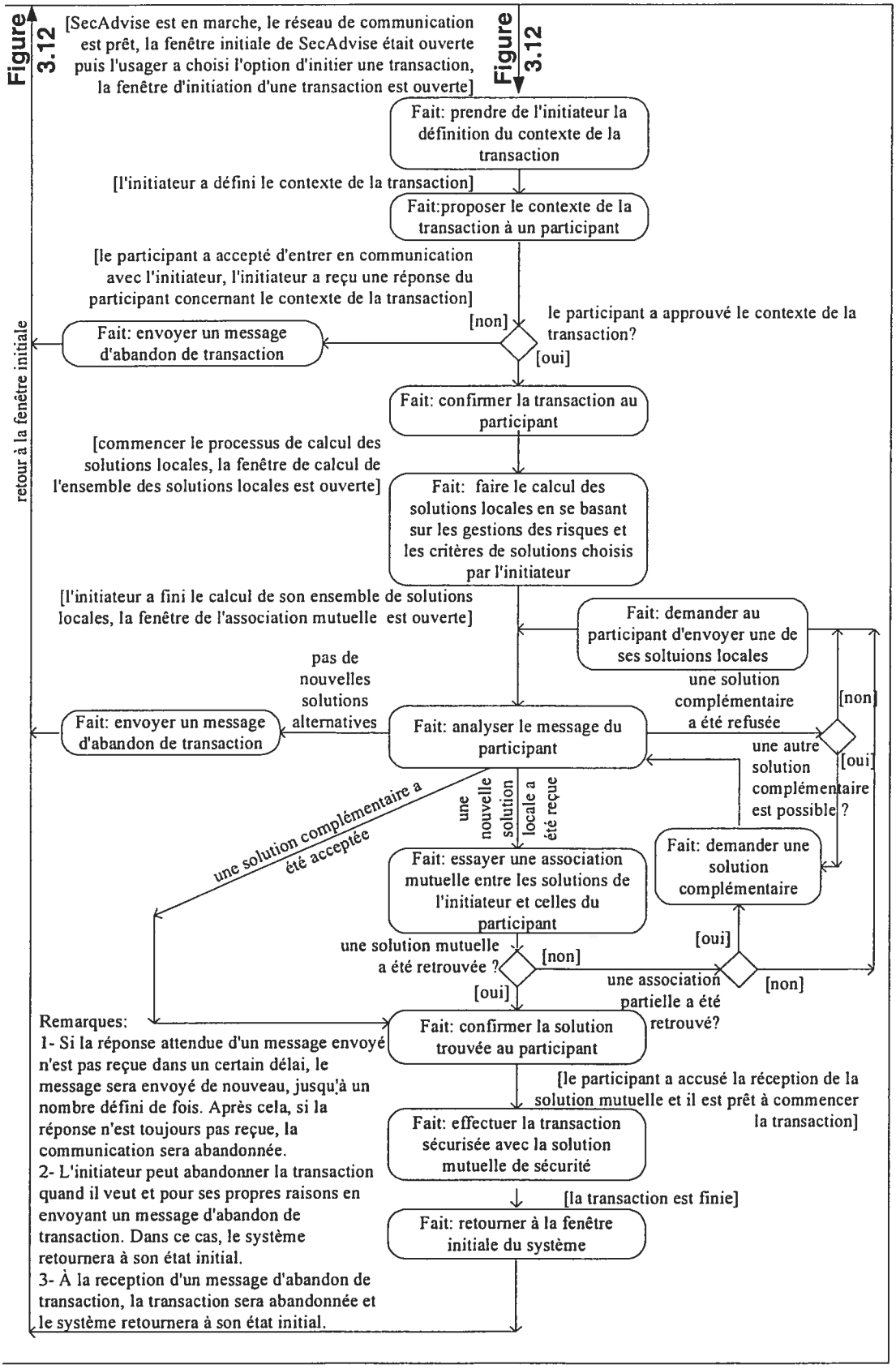

Figure 3.13 Le diagramme d'activité d'un initiateur

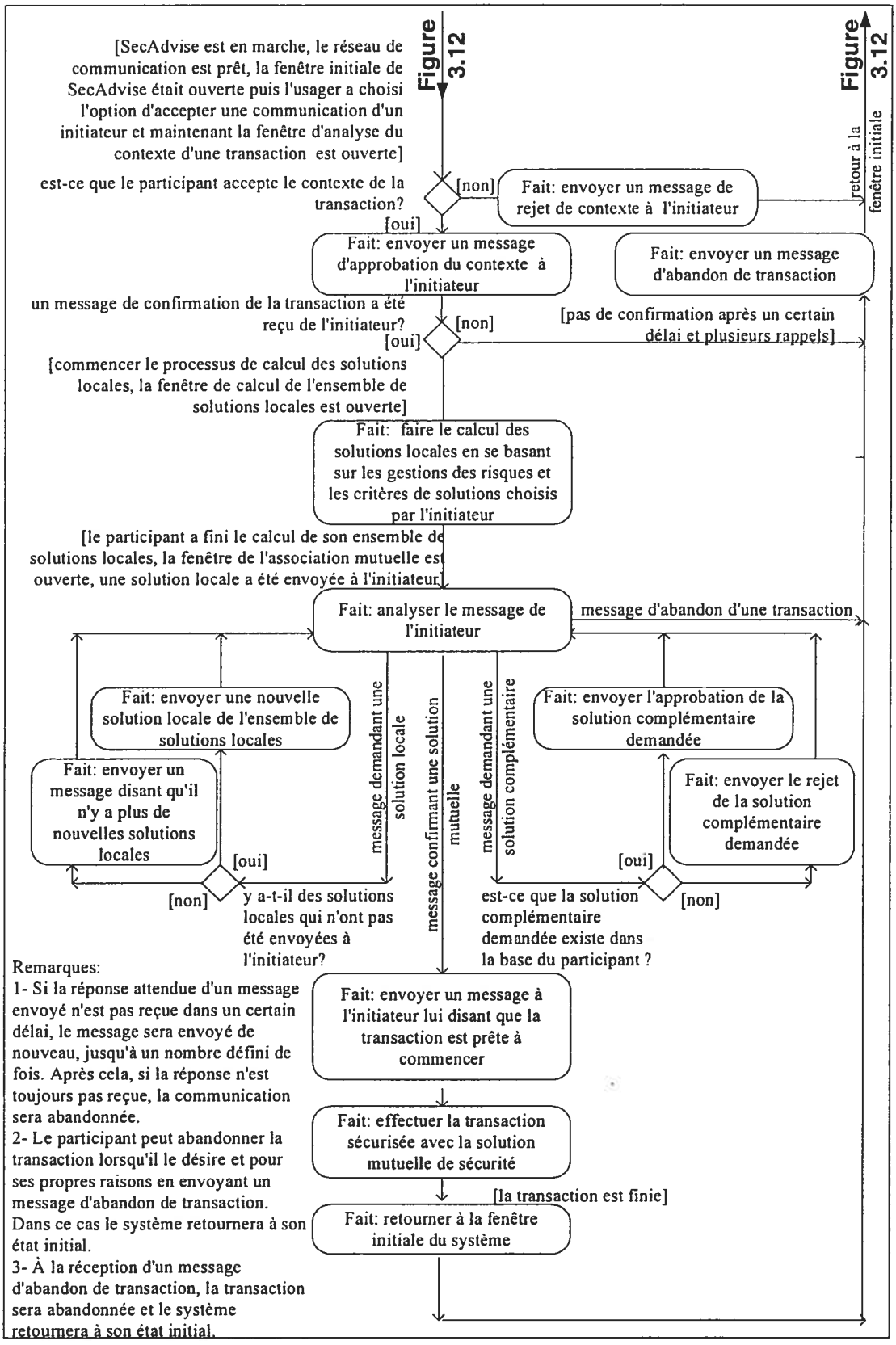

Figure 3.14 Le diagramme d'activité d'un participant

3.3.6 Le diagramme de séquence

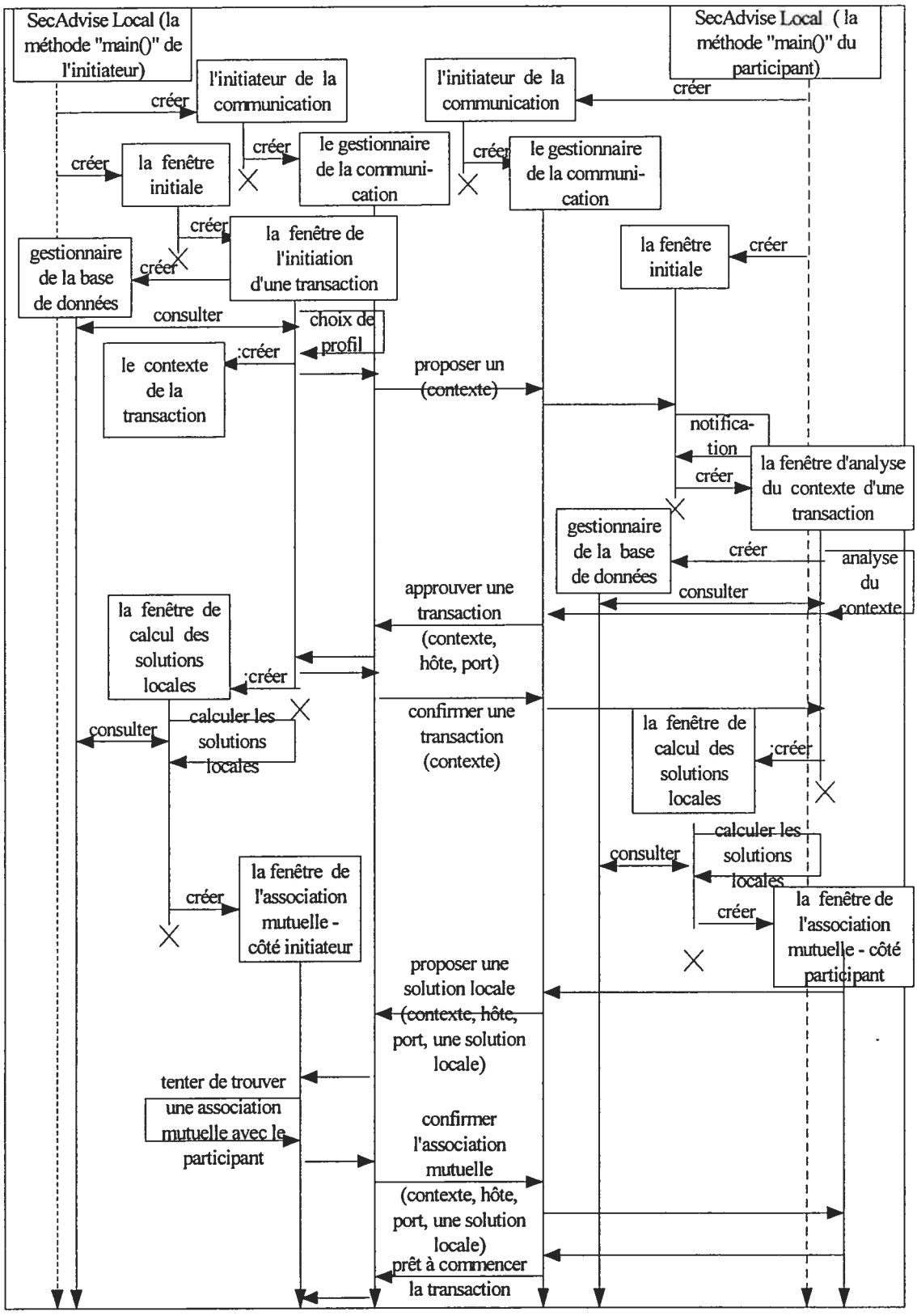

Figure 3.15 Le diagramme de séquence d'une association mutuelle réussie

Le diagramme de séquence dévoile le comportement de la communication entre les parties du système . La figure 3.15 montre le diagramme de séquence d'une tentative réussie d'association mutuelle entre un initiateur et un participant. Nous montrons seulement les objets principaux pour simplifier la figure.

3.4 Le modèle de la base de données

Parmi les différents modèles de base de données (relationnel, à objet, etc.), nous avons choisi d'utiliser le modèle relationnel qui est basé sur les sciences mathématiques. L'architecture d'une base de données relationnelle à deux différentes perceptions : un niveau conceptuel et un niveau externe [CJD98], [GG99].

3.4.1 Le niveau conceptuel

Les modèles conceptuels n'ont pas une représentation concrète sur ordinateur et servent uniquement à saisir les données et à les structurer, non à les conserver [CJD98], [GG99]. Parmi les différents modèles conceptuels (UML, entité–relation, etc.), nous avons choisi d'utiliser le modèle entité-relation.

La base de données est essentiellement constituée de deux parties : la première contient les éléments de la plate-forme de sécurité et la deuxième contient les profils des transactions. Ces deux parties sont combinées pour trouver la solution optimale aux problèmes de sécurité d'une transaction entre deux participants. La figure 3.16 montre la partie qui contient les éléments de la plate-forme de sécurité. C'est principalement dans cette partie que le calcul de l'ensemble des solutions locales de sécurité va s'effectuer. Nous remarquons la correspondance directe entre les entités et les associations de la figure 3.16 et celles de la figure 3.3, montrant les composantes du modèle de sécurité CEN/TC 224 –ISO/TC 68/SC 6 et les relations entre celles-ci.

La figure 3.17 montre la partie qui contient les profils des transactions. Un profil est une combinaison définie des différents éléments du contexte d'une transaction. Le tableau 3.2 montre un exemple des valeurs possibles recherchées des tables pour une transaction de paiements.

Variable	Valeur	Variable	Valeur
domaines_applications	sécurité des échanges	profils	paiement sécurisé
domaines_transactions	paiement sécurisé électronique	sous_domaines_ transactions	paiement par carte de crédit
types_mesures_securité	mesure technique	certificats-à-échanger	X509
info_à_sécuriser	juste la transaction	niveau_désiré_sécurité	100%>=couverture>75%
applications_initiateur	application X de paiement par carte de crédit	gestions_risques	protection de l'authentification contre la divulgation et contre la répétition d'informations aux différents vérificateurs
couches_osi	couche application	menaces_vulnérabilité	divulgation et répétition
services_sécurité	authentification	services_sécurité_ répartis-osi	authentification des entités paires
modèles_interaction_ sécurité	authentification classe 4	actifs_ressources	information de l'authentification
mécanismes_combinés	signature digitale	participants	client X, marchand Y
solutions	SET		

Tableau 3.2 Un exemple des valeurs possibles pour une transaction

3.4.2 Le niveau externe

Un sous-langage de données, intégré dans les langages hôtes, se constitue d'un langage de description de données et d'un langage de manipulation de données. Un langage de description de données permet de créer, de mettre à jour et de détruire la base de données, tandis qu'un langage de manipulation de données permet de manipuler les données [CJD98], [GG99]. Parmi les différents sous-langages de données, nous avons choisi d'utiliser le langage SQL (*Structured Query Language*) qui peut être utilisé en mode intégré à des langages hôtes comme C ou Java.

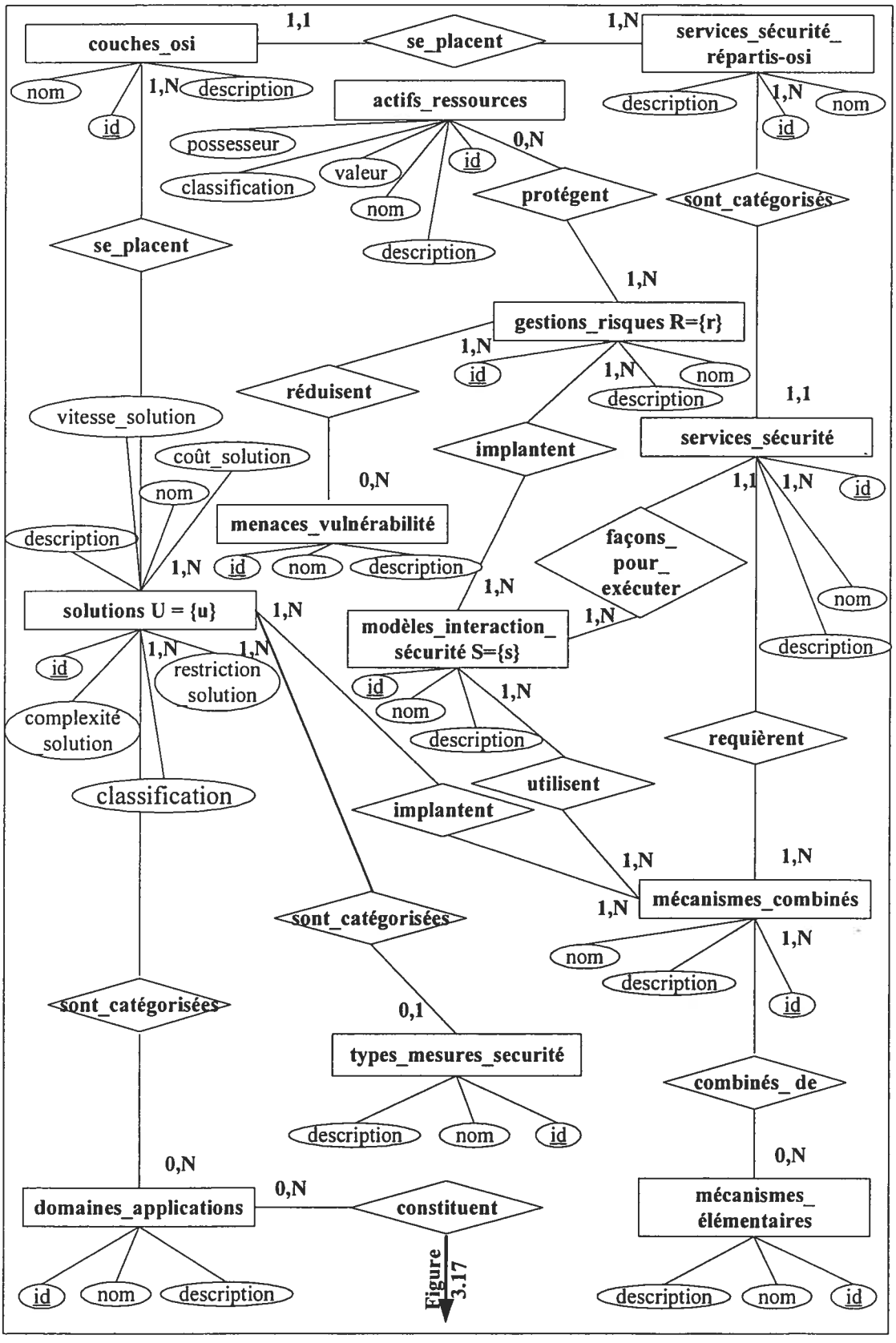

Figure 3.16 Un modèle entité-relation de la base de données de la plate-forme de sécurité

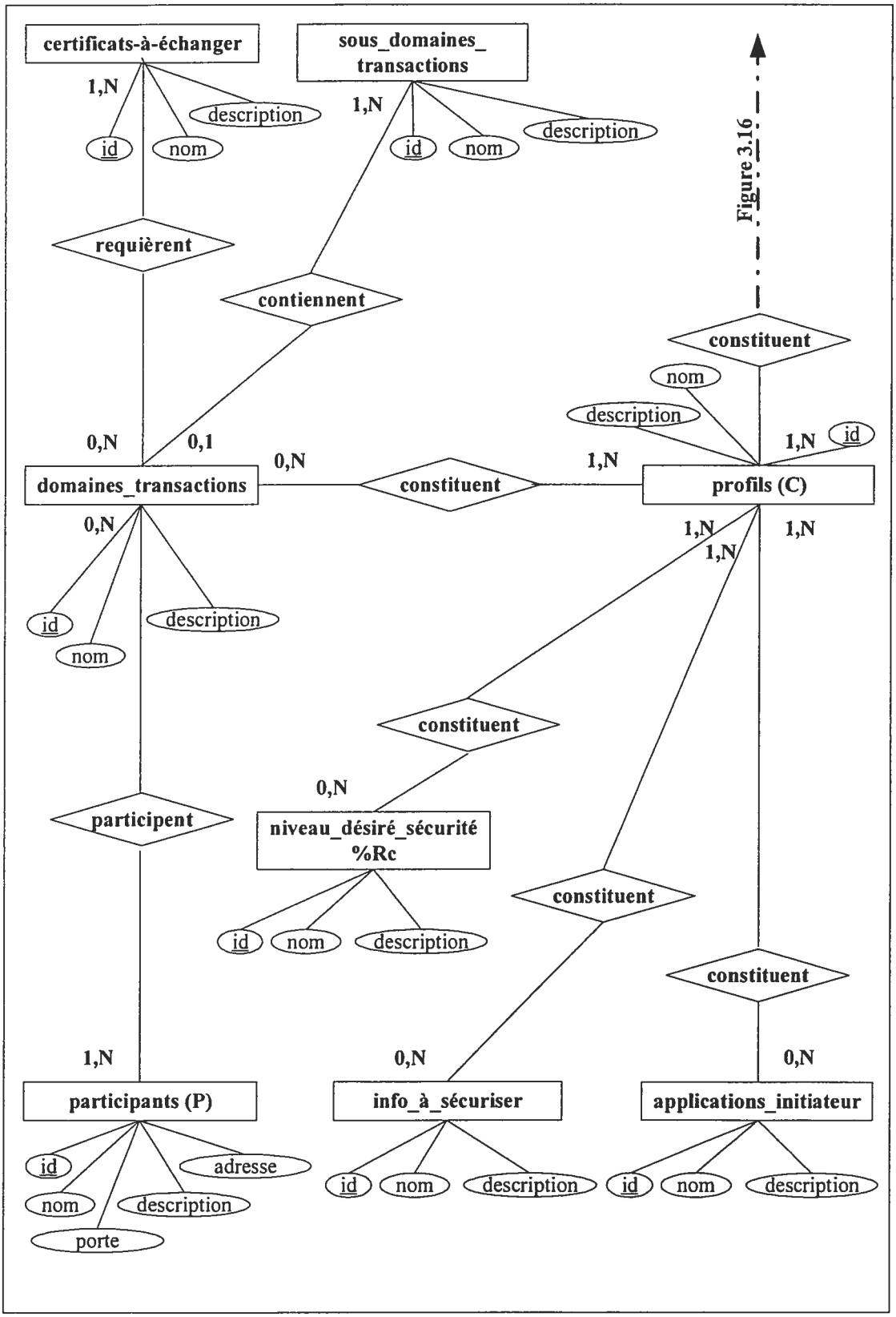

Figure 3.17 Un modèle entité-relation de la base de données des profils des transactions

3.5 Revue de la modélisation formelle

Le tableau 3.3 montre la modélisation formelle du modèle comme elle a été proposée dans [RS02] et [RS02a].

Symbole	Signification
c	La communication (transaction) à sécuriser. C'est le contexte/transaction d'affaires à exécuter et ayant besoin d'être sécurisé.
P	L'ensemble des participants potentiels dans une communication sécuritaire. $p \in P$
P_c	L'ensemble de tous les participants qui sont impliqués dans c. $p_c \in P(P)$
U	L'ensemble de toutes les unités de confiance (*Trust Unit; TU*). $u \in U$
S	L'ensemble des services de sécurité non décomposables. $s \in S$
S_c	L'ensemble des services de sécurité requis par la communication c. $S_c \in P(S)$
S_m	L'ensemble des services de sécurité fournis par un mécanisme m. $S_m \in P(S)$
R	L'ensemble de tous les risques de sécurité non décomposables, $\forall r \in R, \forall u \in U$, ou u couvre entièrement r ou u ne couvre pas r.
R_c	L'ensemble de risques de sécurité à couvrir dans la transaction /contexte c. C'est l'espace de problème de confiance (*Trust Problem Space ; TPS*). $R_c \in P(R)$
R_u	L'ensemble de risques de sécurité couverts entièrement par u. $R_u \in P(R)$
$P^T_{m,p}$	L'ensemble de tous les participants requis pour fournir un mécanisme m au participant p. Par exemple, une agence de certification. $P^T_{m,p} \in P(P), p \in P, m \in M$
$A_{u,p}$	L'ensemble des participants auxquels les participants p font confiance et qui peuvent jouer le rôle d'une autorité certifiante dans un mécanisme de sécurité ou dans un u. $A_{u,p} \in P(P), p \in P, u \in U$ Si l'unité de confiance (*TU*) n'a pas besoin d'une troisième partie de confiance, on considère pour simplifier le processus d'association entre les unités de confiance que : $A_{u,p} = P$
U_p	L'ensemble des unités de confiance disponibles à un participant. $U_p \in P(U), p \in P$
$\bar{U}_P$	L'ensemble des unités de confiance disponibles à tous les participants. Les unités de confiance u de cet ensemble utilisent le même espace de confiance. En d'autres termes, les participants font confiance à une ou plusieurs autorités certifiantes communes. $\bar{U}_P \in P(U), \forall p \in P ; \bar{U}_P = \{u \in \bigcap_{p \in P} U_P \mid \bigcap_{p \in P} A_{u,p} \neq \varnothing\}$

$\tilde{U}_C$	L'ensemble minimal des unités de confiance couvrant les risques de sécurité de la transaction / contexte c. Cet ensemble appartient à l'ensemble des unités de confiance disponibles à tous les participants t.q. les risques associés au contexte sont couverts entièrement par l'ensemble minimal des unités de confiance disponibles pour tous les participants. $\tilde{U}_C \in P(U)$ $\tilde{U}_C = \left\{ U \in P(\bar{U}_{Pc}) \middle\| R_C \subseteq \bigcup_{u \in U} R_u \wedge \|U\| = \min_{U' \in P(\bar{U}_{Pc})} \|U'\| \right\}$

Tableau 3.3 La modélisation formelle de SecAdvise, adaptée de [RS02] et [RS02a].

Le tableau 3.4 montre les révisions que nous avons apportées à la modélisation formelle et les justifications de ces modifications. Le schéma de la base de données des figures 3.16 et 3.17 montre les ensembles P, C, U, S et R, ainsi que le niveau de couverture des risques $\chi = \%R_c$.

Symbole	Signification
C	Nous précisons C en lui donnant un sens plus global que la communication (transaction) à sécuriser. Nous considérons que C est l'ensemble des profils des transactions à exécuter. Un profil est une combinaison définie des différents éléments du contexte d'une transaction. Dans notre programme, ces profils peuvent être prédéfinis préalablement ou composés par l'initiateur au moment de la transaction. $c \in C$
U	Nous appliquons le modèle de confiance de Robles dans le contexte de SecAdvise et nous considérons donc que U est l'ensemble de toutes les solutions de sécurité au lieu de l'ensemble de toutes les unités de confiance. $u \in U$
S	Nous précisons l'ensemble S en le considérant comme étant l'ensemble des modèles d'interaction de sécurité non décomposables au lieu de l'ensemble des services de sécurité non décomposables. Les modèles d'interaction sont des moyens pour exécuter les services de sécurité. Comme le montre l'annexe A, Un service de sécurité peut être exécuté par plusieurs modèles d'interaction de sécurité. Un modèle d'interaction de sécurité assure la gestion d'un risque. $s \in S$
S_c	L'ensemble des modèles d'interaction de sécurité requis par le profil de la transaction. $S_c \in P(S)$

S_u	L'ensemble des modèles d'interaction de sécurité fournis par une solution u. $S_u \in P(S)$
R	Pour préciser le modèle, au lieu de considérer R comme étant l'ensemble de risques de sécurité à couvrir dans la transaction/contexte, on considère qu'il est l'ensemble des gestions des risques non décomposables. Comme montre la figure 2.4 du chapitre 2 une gestion d'un risque est une mesure (protection, prévention, détection, etc.) qui vise à protéger les actifs d'un participant (information, etc.) en réduisant ou en éliminant la vulnérabilité de ces actifs ou encore, en repoussant les menaces s'attaquant aux aspects vulnérables de ces actifs. Comme le montre l'annexe A, les standards et les spécifications de sécurité offrent différentes gestions des risques. Par exemple, la protection contre tous les types de répudiation en utilisant les techniques de chiffrement symétrique est parmi les gestions de risques offertes par la spécification SET (*Secure Electronic Transaction specification*). $\forall r \in R, \forall u \in U,$ soit que la solution u décrit le modèle d'interaction s qui fournit entièrement la gestion de risque r ou que la solution u ne décrit pas le modèle d'interaction s du tout.
R_c	L'ensemble des gestions des risques de sécurité requis dans c. $R_c \in P(R)$
R_u	L'ensemble des gestions des risques de sécurité couverts entièrement par les modèles d'interaction décrits dans la solution u. $R_u \in P(R)$
$P^T_{A,U}$	SecAdvise est une architecture générale et les solutions qu'il suggère peuvent être de types différents. Donc, nous avons décidé de combiner les ensembles : $P^T_{m,p}$ et $A_{u,p}$ définis dans [RS02] et [RS02a] dans un ensemble plus global. Celui-ci est l'ensemble des participants P qui font confiance aux participants A. Les participants A peuvent fournir, si nécessaire, une certification pour une solution u. C'est-à-dire que nous considérons de manière plus générale que toute solution de sécurité que les deux participants acceptent d'utiliser entre eux, que cela soit un certificat, un standard ou autre, est en principe fourni par une troisième partie à laquelle les deux participants font confiance. $P^T_{A,U} \in P(P)$ t.q. $u \in U$
U_p	L'ensemble des solutions de sécurité disponibles pour un participant dans sa base de données. $U_p \in P(U)$, $p \in P$

$\bar{U}_{Pc}$	Nous avons décidé de modifier les symboles et de ne plus utiliser le symbole u dans les formules afin d'éliminer l'ambiguïté avec $u \in U$ déjà définit. Nous avons ajouté à cette formule deux autres conditions (2 et 3). L'ensemble des solutions disponibles à tous les participants dans le contexte du profil en question c. α_A est une solution fournit par un parti $A \in P(P)$ auquel les deux participants font confiance : $\bar{U}_{Pc} = \{\alpha_A \in \cap U_{Pc}\}$ $U_{Pc} \in P(U)$, $U_{Pc}=U_p$ t.q. $p \in P_c$ $\bar{U}_{Pc} \in P(U)$, $\bar{U}_{Pc}=U_p$ t.q. $p \in P_c$, $\forall p \in P(\bar{U}_{Pc} \in P(U))$ Pour que $\bar{U}_{Pc} \neq \varnothing$ il faut que : 1. $\cap \overset{T}{P}_{A,U} \neq \varnothing \ \forall \ \alpha_A \in \bar{U}_{Pc}$ 2. $P_c \neq \varnothing$ 3. $\cap U_{Pc} \neq \varnothing$
$\tilde{U}_c^*$	Nous introduisons une nouvelle notation qui est l'ensemble des solutions locales d'un participant. Cet ensemble est l'ensemble maximal des solutions qui couvrent un pourcentage défini des risques de la transaction et qui satisfont aux critères définis des choix de solutions. β_i^* est un élément de cet ensemble et peut aussi être un ensemble de solutions dont la cardinalité égale μ_i^*. $\beta_i^* \in \tilde{U}_c^*$, $\left\|\beta_i^*\right\| = \mu_i^*$ Nous avons inclus χ qui est le pourcentage désiré de couverture des risques défini par l'initiateur de la communication et accepté par le participant $\chi = \% R_c$ Nous avons inclus δ^*, qui est un critère désiré de choix des solutions. Celui-ci est défini par le participant P_c. β_i^* satisfait seulement aux critères $\sum \delta_{Pc}^*$ du participant en question. $\tilde{U}_c^* = \underset{i=1...n}{\{\beta_i^* \in P(\bar{U}_{Pc})}$ t.q. (β_i^* couvre min χ) $\wedge$ (β_i^* satisfait $\sum \delta_{Pc}^*)\}$ Pour que $\tilde{U}_c^* \neq \varnothing$ il faut que $\bar{U}_{Pc} \neq \varnothing$

$\tilde{U}_c$	Cet ensemble est l'ensemble des solutions mutuelles. Il est défini comme étant l'ensemble minimal des solutions qui couvrent un pourcentage défini des risques de la transaction et qui satisfont aux critères définis des choix de solutions. β_i est un élément de cet ensemble et peut être aussi un ensemble de solutions dont la cardinalité égale μ_i . χ est un pourcentage désiré de couverture des risques défini par l'initiateur et accepté par le participant $\chi = \% R_c$. δ^* est un critère désiré de choix des solutions défini par un participant P_c . $\beta_i \in \tilde{U}_c$, $\|\beta_i\| = \mu_i$ $\tilde{U}_c = \{\beta_i \in P(\bar{U}_{Pc})$ t.q. β_i couvre min $\chi \wedge \beta_i$ satisfait $\sum_{\forall P_c} \delta^*_{P_c} \wedge \|\beta_i\| = \min(\mu_i)\}$ $_{i=1 \ldots n}$ Pour que $\tilde{U}_c \neq \varnothing$ il faut que : $\cap \bar{U}_{Pc} \neq \varnothing$ Nous notons que c'est seulement dans le cas de l'association directe que : $\tilde{U}_c \in \cap \tilde{U}^*_c$ Dans le cas de l'association indirecte, l'initiateur compose la solution mutuelle à partir de ses solutions et de celles reçues des autres participants et donc : $\beta_i \in \bar{U}_{Pc} \ \forall P_c$

Tableau 3.4 Revue de la modélisation formelle de SecAdvise

Chapitre 4. Réalisation et implantation

Le programme, qui a été écrit en Java, se concentre à tester l'aviseur SecAdvise dans le domaine de la sécurité des échanges électroniques.

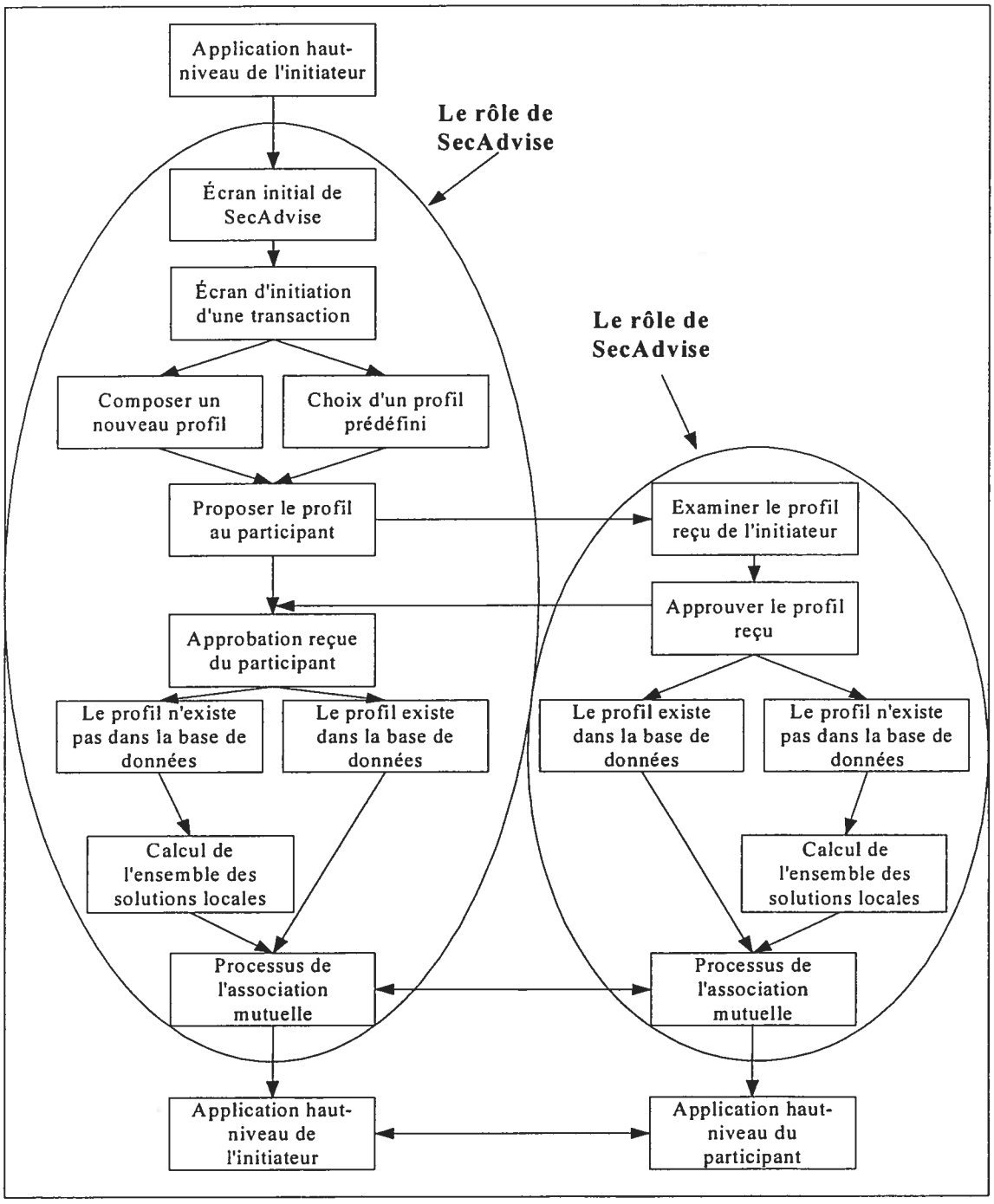

Figure 4.1 Le rôle de SecAdvise dans la sécurisation d'une transaction

Afin de clarifier le cycle d'une transaction qui implique SecAdvise, nous divisons le rôle de SecAdvise dans la sécurisation d'une transaction sur un réseau ouvert en plusieurs étapes principales que nous montrons dans la figure 4.1.

Selon notre conception et comme le montre la figure 4.1, c'est l'initiateur de la transaction qui définit le contexte de la transaction, il peut choisir un profil prédéfini de la base de données ou composer un nouveau profil au besoin. Ensuite, l'initiateur envoie le contexte au participant de son choix et attend l'approbation. Si le participant accepte le contexte, les deux côtés calculent l'ensemble de leurs solutions locales de sécurité et s'échangent des informations dans le but de trouver une solution mutuelle à utiliser pour sécuriser la transaction en question.

4.1 Les interfaces graphiques de l'usager

Nous dévoilons progressivement les interfaces graphiques du prototype par la simulation d'une tentative d'association de solutions mutuelles entre deux participants dont l'un sera l'initiateur de la transaction. La figure 4.2 montre la fenêtre initiale que chaque participant détient dès qu'il met son programme en marche.

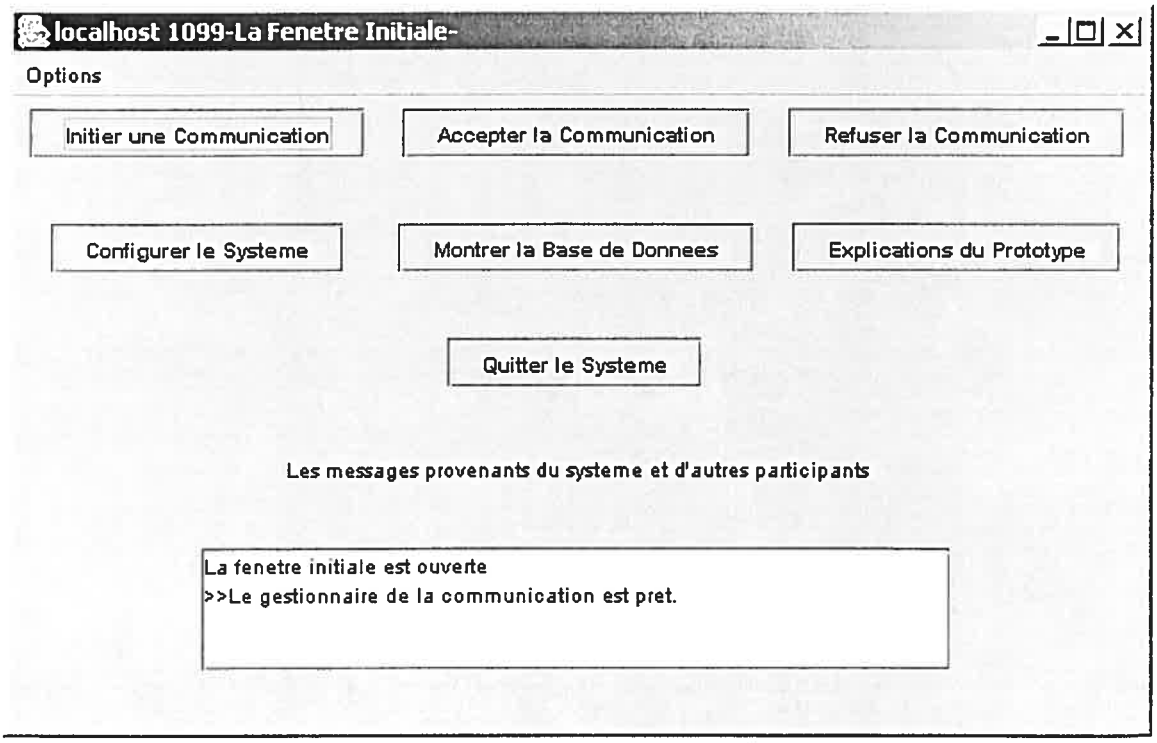

Figure 4.2 La fenêtre initiale de SecAdvise

Le bouton « Initier une Communication » de la figure 4.2 ouvrira la fenêtre de l'initiation d'une transaction montrée à la figure 4.3.

Par l'intermédiaire de la fenêtre de l'initiation d'une transaction, l'initiateur de la communication définira le contexte de la transaction voulue et le proposera au participant de son choix. De son côté, le participant choisi sera notifié de la réception d'un nouvel appel dans sa fenêtre initiale respective, et pourra choisir entre accepter la communication ou la refuser en envoyant un message approprié; en cas d'indisponibilité par exemple.

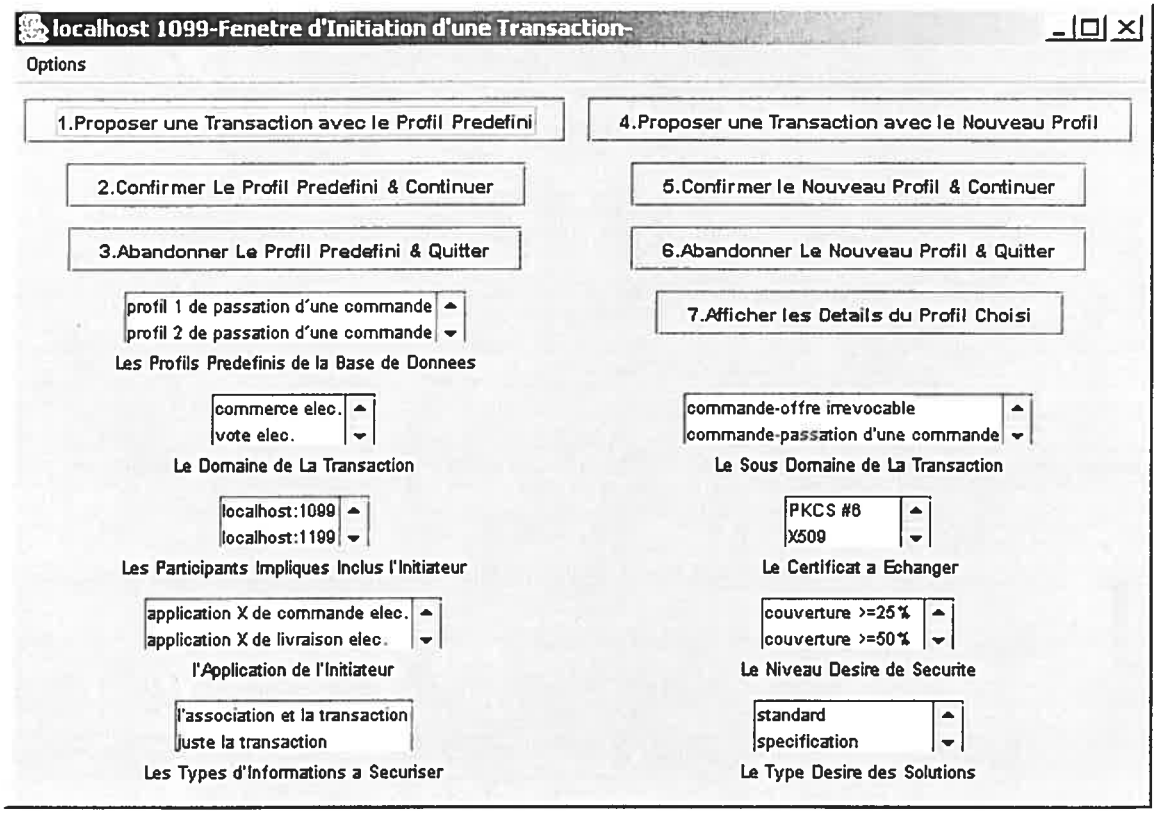

Figure 4.3 La fenêtre d'initiation d'une transaction

Après avoir accepter d'entrer en communication avec l'initiateur, le participant va procéder à l'analyse du contexte envoyé par l'initiateur dans la fenêtre de l'analyse du contexte d'une transaction qui est montrée à la figure 4.4. Ainsi, le participant pourra accepter ou rejeter le contexte de la transaction en envoyant un message approprié.

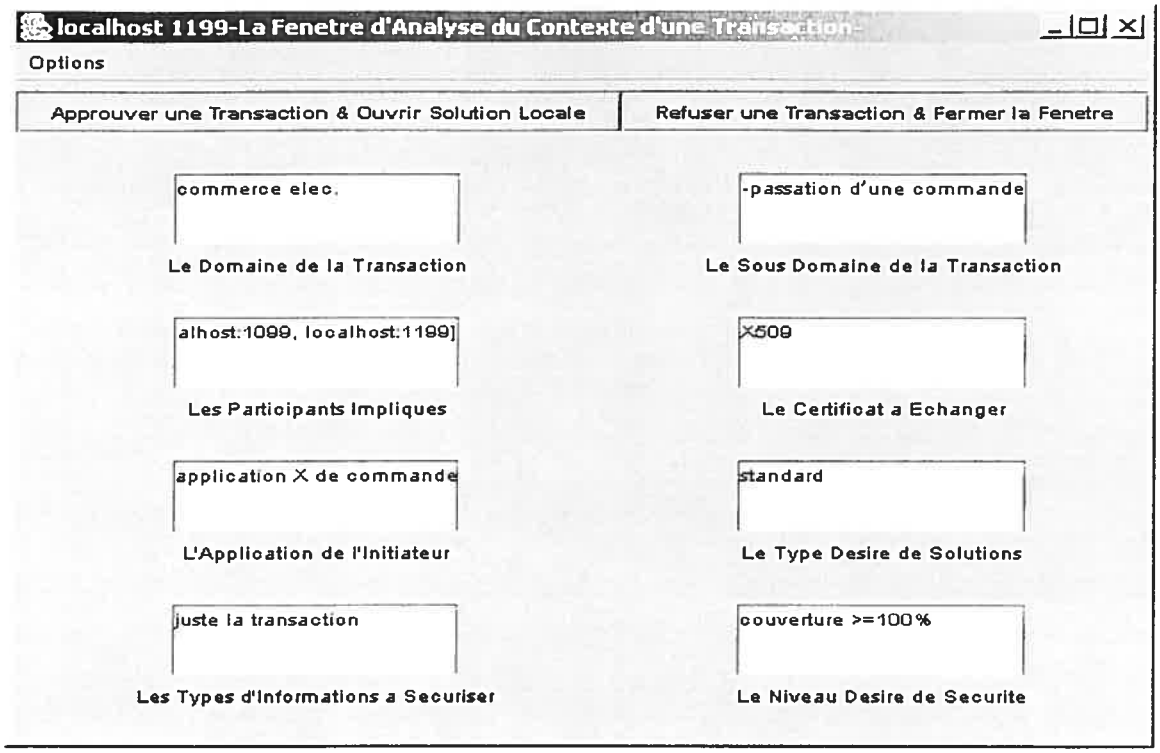

Figure 4.4 La fenêtre d'analyse du contexte d'une transaction

Du côté du participant, le refus du contexte de la transaction remet le système à l'état initial tandis que l'approbation du conteste ouvrira la fenêtre de calcul de l'ensemble des solutions locales qui est montrée à la figure 4.5.

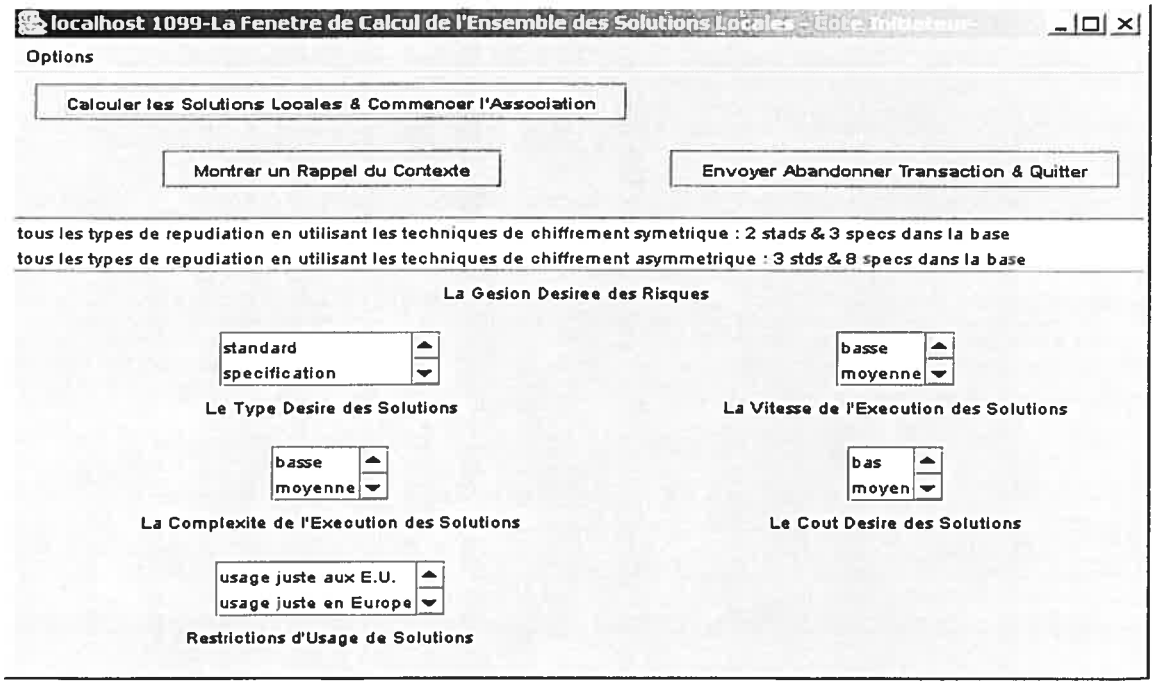

Figure 4.5 La fenêtre de calcul de l'ensemble des solutions locales

C'est dans la fenêtre de calcul de solutions locales que le participant sélectionnera les moyens désirés de gestion des risques. Le résultat de ce calcul sera un ensemble de solutions locales optimales à utiliser pour sécuriser la transaction. L'initiateur, de son côté, ayant reçu l'approbation du participant sur le contexte, enverra un message de confirmation de la transaction avant de commencer, lui aussi, le calcul de l'ensemble des solutions locales dans la fenêtre de calcul de l'ensemble des solutions locales similaire à celle montrée à la figure 4.5.

On note ici que chaque parti a la liberté de définir ses moyens de gestion de risques et ses critères d'inclusion des solutions dans l'ensemble des solutions locales. Par exemple, la complexité d'exécution des solutions, etc. On note aussi que si le profil de la transaction est déjà défini dans la table des profils de la base de données, alors l'ensemble des solutions locales sera cherché de la base de données sans calcul et on passera directement à la fenêtre de l'association mutuelle.

Dès que le participant terminera son calcul de solutions locales, il ouvrira sa fenêtre d'association de solutions mutuelles montrée à la figure 4.6 et enverra ses solutions locales à l'initiateur, une par une, en vue de trouver une association mutuelle avec lui.

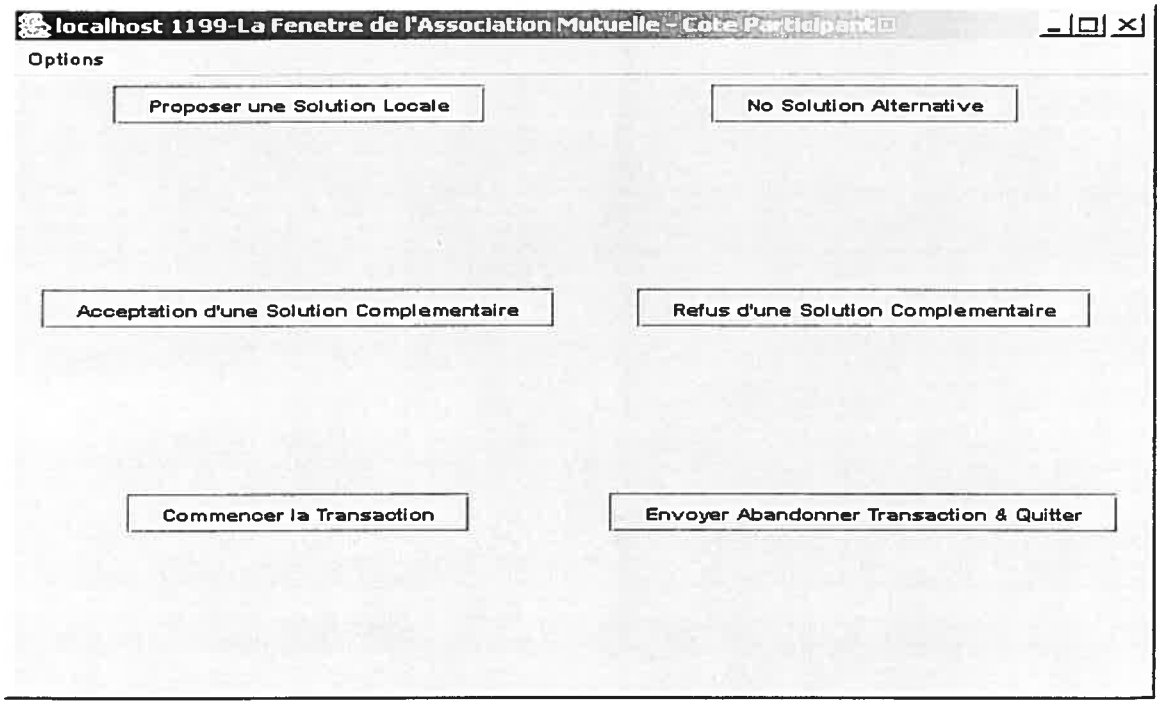

Figure 4.6 La fenêtre de l'association mutuelle – participant

L'initiateur aussi terminera son calcul de solutions locales et ouvrira sa fenêtre d'association de solutions mutuelles montrée à la figure 4.7.

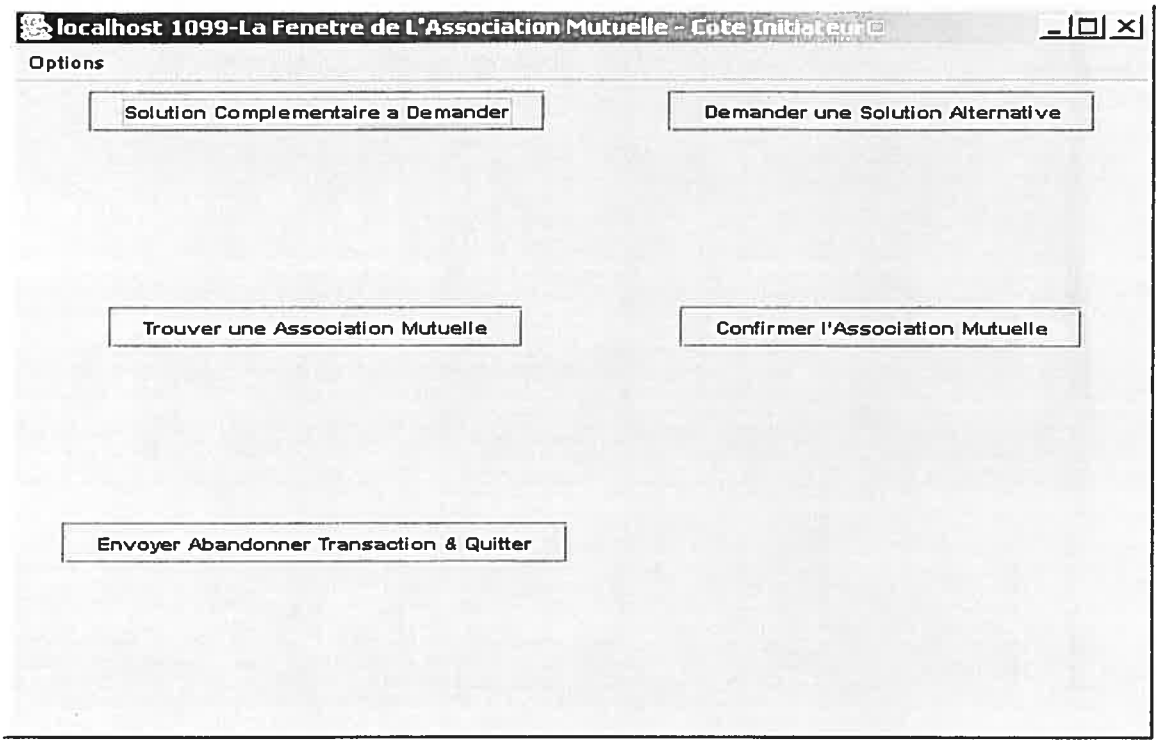

Figure 4.7 La fenêtre de l'association mutuelle – initiateur

L'initiateur commencera la procédure d'association aussitôt qu'il recevra une des solutions locales envoyée par le participant.

La transaction sera annulée dans le cas où une solution mutuelle satisfaisante pour les deux partis n'aurait pu être trouvée. Aussi, n'importe lequel des deux usagers a la possibilité d'arrêter et d'annuler la transaction pour des raisons de son choix en envoyant un message d'annulation de transaction.

Aussi, le prototype a trois autres interfaces usagers d'utilité générale :

1. L'interface de l'administrateur montré à la figure 4.8 qui permet à l'administrateur de réaliser les différentes configurations du système.
2. L'interface de l'aide à l'usager montré à la figure 4.9 qui présente aux usagers les différentes fonctionnalités du système.
3. L'interface de la base de données montrée à la figure 4.10 qui présente aux usagers le contenu de la base de données.

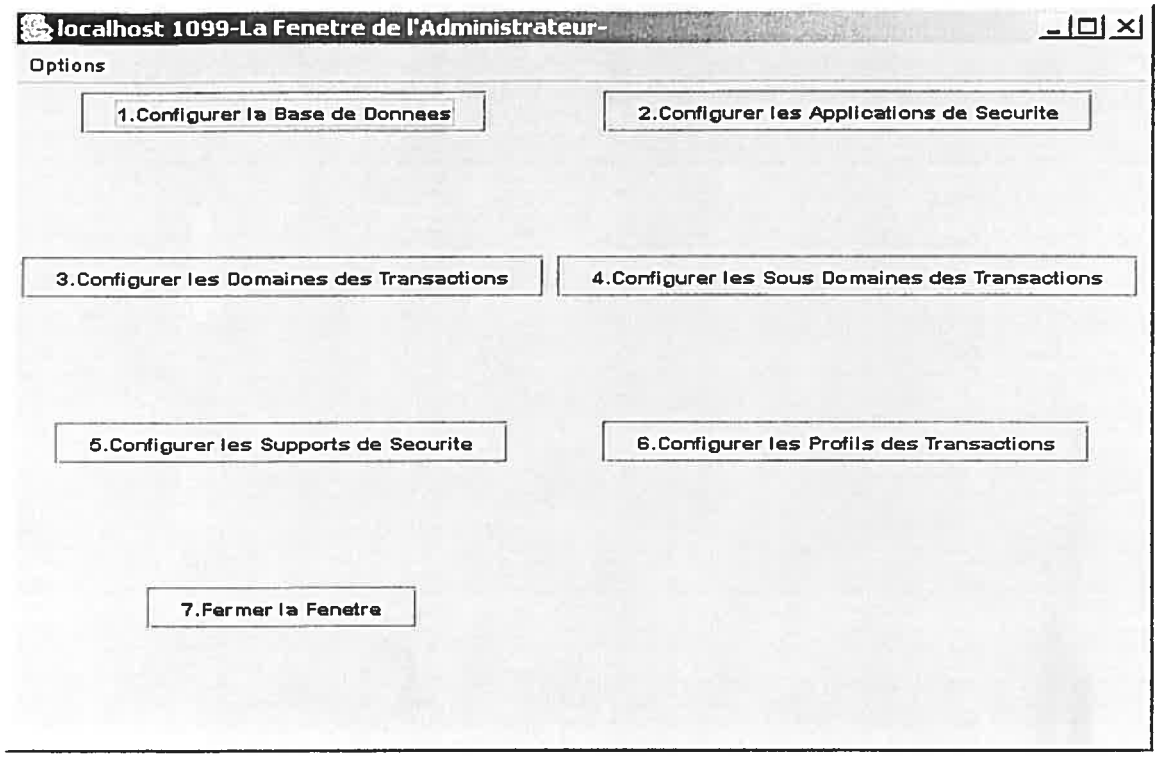

Figure 4.8 La fenêtre de l'administrateur

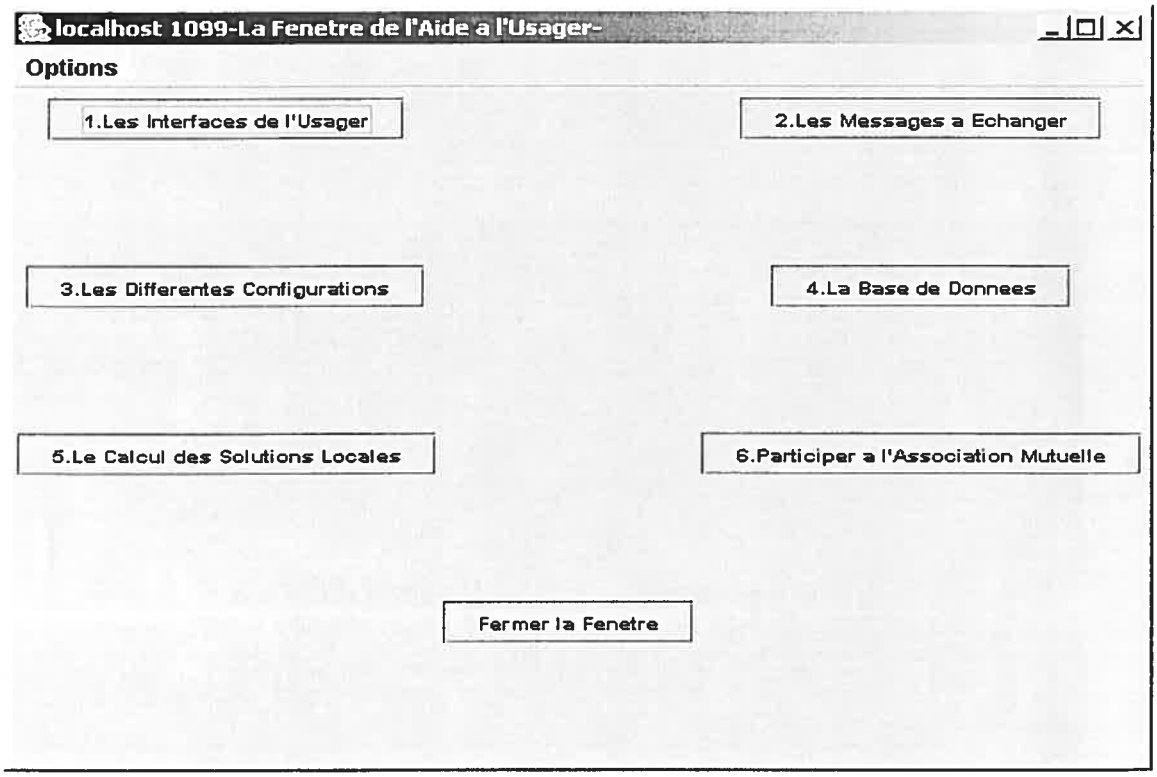

Figure 4.9 La fenêtre de l'aide a l'usager

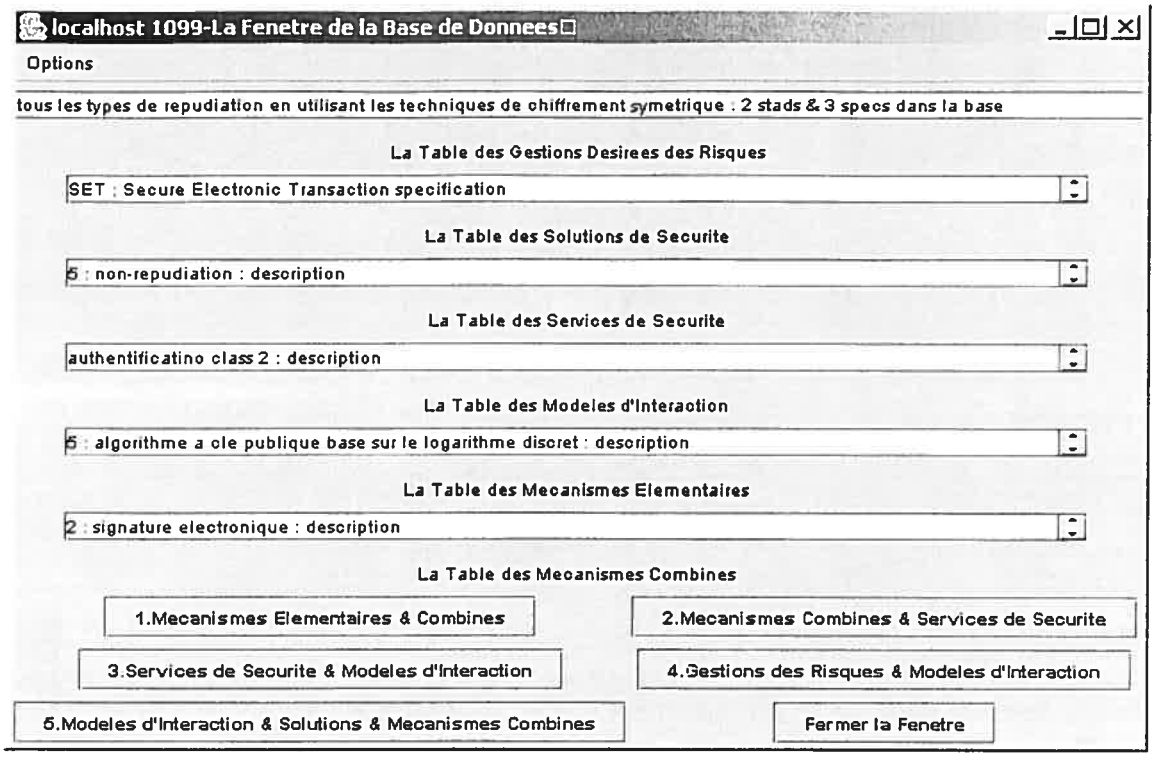

Figure 4.10 La fenêtre de la base de données

4.2 Concevoir le calcul de l'ensemble des solutions locales

L'usager de SecAdvise utilisera la fenêtre montrée à la figure 4.5 pour définir les éléments de calcul de l'ensemble des solutions locales. L'initiateur de la communication et le participant sélectionneront, indépendamment l'un de l'autre, la gestion désirée des risques (R_c) ainsi que d'autres critères de choix de solutions ($\sum\delta^*$) comme la complexité d'exécution des solutions, la vitesse de l'exécution des solutions, etc. Après avoir saisi les différents choix de l'usager, le programme cherchera, dans la base de données, les modèles d'interaction appropriés (S_c) aux gestions des risques. Un exemple est donné dans le tableau 4.1. Nous remarquons la correspondance entre le calcul de l'ensemble des solutions locales et les principes du modèle de sécurité CEN/TC 224 – ISO/TC 68/SC 6 de la figure 3.3 ; les modèles d'interaction de sécurité sont des façons d'exécuter les services de sécurité en utilisant les mécanismes de sécurité. Les modèles d'interaction de sécurité sont choisis selon les gestions des risques dans le but de protéger les actifs de l'usager, ils sont décrits dans les standards et les spécifications de sécurité.

Les gestions des risques choisies par l'utilisateur (R_C)	Le modèle d'interaction approprié dans la base de données (Sc)
Protection de l'authentification contre la divulgation d'informations.	Classe d'authentification n° 1.
Protection du contenu sémantique des données par des transformations cryptographiques (chiffrement).	Confidentialité de l'information assurée par les techniques d'application (*mapping techniques*).
Protection contre tous les types de répudiation en utilisant les techniques de chiffrement asymétrique.	La non répudiation par l'utilisation de techniques asymétriques.

Tableau 4.1 Les gestions des risques et les modèles d'interaction

Le programme cherchera aussi dans la base de données toutes les solutions de sécurité (U) décrivant au moins un de ces modèles d'interaction et satisfaisant les autres critères de choix de solution. Le résultat de recherche dans la base servira à construire la matrice de calcul de l'ensemble des solutions locales. C'est une matrice de dimension m x n, où m est égal au nombre de solutions recherchées et n est égal au nombre de modèles d'interaction. Les valeurs des cases de la matrice sont (1) quand la solution couvre le modèle d'interaction en question, (0) si ce n'est pas le cas. Le tableau 4.2 est un exemple de cette matrice.

	Classe d'authentification n° 1	Confidentialité de l'information assurée par les techniques d'application (*mapping techniques*)	La non répudiation par l'utilisation de techniques asymétriques
ISO/IEC 9594	1	0	0
ISO 10202	1	0	0
ISO 10126	0	1	0
ANSI X3.92	0	1	0
ANSI X3.106	0	1	0
ISO/IEC 7816	0	0	1
ISO/IEC 9796	0	0	1
ISO/IEC 14888	0	0	1

Tableau 4.2 Matrice de calcul de l'ensemble des solutions locales

Les différentes combinaisons des lignes sont susceptibles d'être des éléments (β_i^*) dans l'ensemble des solutions locales. Par exemple, pour la matrice du tableau 4.2, il y aura 92 combinaisons susceptibles d'être analysées selon la formule :

$$\text{Nombre de combinaisons} = \sum_{n=3,2,1} \frac{m!}{n!(m-n)!} = \frac{8!}{3!5!} + \frac{8!}{2!6!} + \frac{8!}{1!7!} = 92$$

La cardinalité de chaque combinaison est ($\|\beta_i^*\| = \mu_i^*$). La méthode de calcul examine les combinaisons par ordre croissant selon leur cardinalité. Le programme calculera le pourcentage de risques ($\%\ R_c$) couverts de chaque combinaison de solutions :

$$\text{Résultat partiel} = \text{XOR (lignes de solutions constituant la combinaison)}$$

$$\text{Pourcentage de risques couverts} = \frac{\text{nombre de (1) dans Résultat partiel}}{\text{nombre de modèles d'interaction}} \times 100$$

C'est le niveau de couverture des risques choisi par l'initiateur (χ) qui décidera de l'inclusion ou de l'exclusion de chaque combinaison de solutions dans l'ensemble final de solutions locales. Par exemple, dans la matrice du tableau 4.2 présenté précédemment :

- Si le pourcentage désiré de couverture des risques est supérieur à 30 %, alors aucune solution ne sera retenue sans être combinée avec une autre couvrant un modèle d'interaction différent, car aucune solution ne couvre seule plus de 30 % des modèles d'interaction.
- De même, si le pourcentage désiré de couverture de risques est égal ou inférieur à 30 %, alors l'ensemble des solutions locales aura les huit solutions, car chacune d'entre elles couvre individuellement au moins un modèle d'interaction parmi les trois.

Pour simplifier, nous avions supposé que les risques avaient la même importance dans le pourcentage de la couverture, mais ce n'est pas nécessairement vrai. Pour tenir compte de la réalité, le programme final doit prendre cela en considération et donner à l'usager la possibilité de mesurer l'importance des risques.

Autre information qu'on peut déduire de cette matrice :

- Le total des valeurs des lignes nous donne le nombre de modèles d'interaction (et, par le fait même, le nombre de risques) couverts par les solutions.
- Le total des valeurs des colonnes nous donne le nombre de solutions disponibles couvrant les modèles d'interaction.

4.3 L'implantation de la base de données

Pour implanter le schéma de la base de données des figures 3.16 et 3.17 du chapitre 3, nous avons choisi d'utiliser un serveur de base de données *MySql Version 4.0.10. gamma. MySql* est un logiciel libre sous la licence GNL (*General Public License*), il fournit simultanément à plusieurs usagers et à plusieurs fils d'exécution un serveur de base de données SQL (*Structured Query Language*) rapide et efficace. Le driver JDBC (*Java Data Base Connectivity*) que nous avons utilisé pour le serveur est *MM.MySQL 2.0.14.*

4.3.1 Le gestionnaire de la base de données

La figure 4.11 montre le constructeur de la classe du gestionnaire de la base de données (*public class DBManager*) et les méthodes qui assurent les relations entre Java et *MySql*. Les autres méthodes de la classe du gestionnaire de la base de données serviront essentiellement à afficher des données à l'usager et à construire la matrice de calcul de l'ensemble des solutions locales.

```
Public class DBManager{
  private static DBManager instance = new DBManager();
  private static String url =
   "jdbc:mysql://localhost:3306/secadvise";
  private DBManager(){
    try{
      Class.forName("org.gjt.mm.mysql.Driver");
    }
    catch(Exception e){
      e.printStackTrace();}
    }
```

```
  private static Connection getConnection(){
    try{
      return DriverManager.getConnection(url, "root", "");
    }
    catch(SQLException ex){
      ex.printStackTrace();
      return null;}
    }
  public static DBManager getInstance(){
    return instance;}
  //les autres méthodes de la classe
}//end classe
```

Figure 4.11 La classe du gestionnaire de la base de données

4.3.2 Les affichages de données

Il y aura deux types d'affichage de données. Le premier type affiche (dans la fenêtre de l'initiation d'une transaction) le contenu des tables des éléments de profil des transactions. Par exemple, dans la figure 4.12, on montre l'appel de la méthode qui affichera la liste des participants possibles. La figure 4.13 montre en détail la méthode (*getParticipantsInvolved()*) de la classe du gestionnaire de la base de données.

```
DBManager dBManager = DBManager.getInstance();
ParticipantsInvolved[]participantsList =
dBManager.getParticipantsInvolved();
```

Figure 4.12 Appel d'une méthode du gestionnaire de la base de données

```
public static ParticipantsInvolved[] getParticipantsInvolved(){
  Collection participantsInvolved = new ArrayList();
  ParticipantsInvolved[] array = null;
  try{
    Connection con = getConnection();
    Statement stmt = con.createStatement();
    ResultSet rs = stmt.executeQuery("SELECT * FROM
      participants_involved");
    while (rs.next()){
      int id = rs.getInt(1);
```

```
        String name = rs.getString(2);
        String description = rs.getString(3);
        String ipAddress = rs.getString(4);
        int port = rs.getInt(5);
        ParticipantsInvolved participantInvolved = new
          ParticipantsInvolved(id, name, description, ipAddress,
          port);
        participantsInvolved.add(participantInvolved);
      }
      int length = participantsInvolved.size();
      array = new ParticipantsInvolved[length];
      int index = 0;
      for (Iterator i = participantsInvolved.iterator();
        i.hasNext();){
        Object item = i.next();
        array[index] = (ParticipantsInvolved) item;
        index++;
      }
    }
    catch (Exception e){
      e.printStackTrace();
    }
    return array;
}
```

Figure 4.13 Une méthode de la classe du gestionnaire de la base de données

Le deuxième type d'affichage de données permet de visualiser dans la fenêtre de la base de données le contenu des tables de sécurité. Les méthodes et leurs appels ressemblent aux figures 4.12 et 4.13 vues antérieurement.

4.3.3 La matrice de calcul des solutions locales

Finalement, une suite de requêtes servent à construire la matrice de calcul des solutions locales. La figure 4.14 montre la requête qui cherche les modèles d'interaction

appropriés aux gestions des risques choisies par l'usager. Le résultat de la requête sera affecté à la première ligne de la matrice de calcul de l'ensemble des solutions locales.

```
String sqlStatement = "SELECT * " +
  "FROM risks_rel_security_interaction_models rel,
  security_interaction_models sim " +
  "WHERE rel.risks_id in ";
String interactionsIds = "(";
for (int i = 0; i < selectedRisks.length; i++){
  interactionsIds += ((Risk)selectedRisks[i]).getId();
  if (i < selectedRisks.length - 1){
    interactionsIds += ", ";
  }
}
interactionsIds += ")";
sqlStatement += interactionsIds + " and
  sim.id=rel.security_interaction_models_id";
```

Figure 4.14 La requête qui cherche les modèles d'interaction de sécurité

Les requêtes qui suivent, dans la figure 4.15, chercheront les solutions qui décrivent ces modèles d'interaction. On remarque les critères de choix de solutions.

```
for (int index = 1; index <= selectedRisks.length; index++){
  String sqlStatement = "SELECT * " + " FROM
  sol_rel_sec_int_mod_and_com_mec rel,
  solutions sol "  +  " WHERE
  rel.security_interaction_models_id in ";
String interactionId = "(" +matrice[0][index] + ")";
sqlStatement +=interactionId+" and sol.id=rel.solutions_id";
sqlStatement += "and sol.solutions_type='" +
  solutionChosenType + "'";
sqlStatement += "and sol.solutions_cost='" +
  solutionChosenPrice + "'";
sqlStatement += "and sol.solutions_speed='" +
  solutionChosenSpeed + "'";
sqlStatement += "and sol.solutions_complexity='" +
```

```
  solutionChosenComplextiy + "'";
sqlStatement += "and sol.solutions_restrictions='" +
  solutionChosenRestrictions + "'";
}
```

Figure 4.15 Les requêtes qui cherchent les solutions optimales

4.4 Concevoir l'association mutuelle

Les participants dans une transaction se servent des messages du protocole de communication, que nous avons défini dans 3.2.3, pour s'échanger leurs solutions. Selon notre conception, c'est l'initiateur de la communication qui a principalement la tâche de trouver l'association mutuelle cherchée en comparant son ensemble de solutions locales avec celui du participant. Ce dernier enverra donc ses solutions à l'initiateur une à la suite de l'autre. Nous avons vu dans la section 4.3 que les éléments de l'ensemble de solutions locales peuvent, eux aussi, être des ensembles de solutions. Nous allons analyser les résultats possibles d'une tentative d'association mutuelle.

4.4.1 Concevoir l'association mutuelle directe

Nous commençons par analyser la situation où la solution envoyée par le participant (β_i^*) est un élément de l'ensemble des solutions locales de l'initiateur ($\exists \beta^*_{i_{initiateur}}$ t.q. $\beta^*_{i_{participant}} = \beta^*_{i_{initiateur}}$). Dans ce cas, l'initiateur envoie un message qui confirme l'association mutuelle trouvée. Nous montrons un exemple de ce cas dans la figure 4.16.

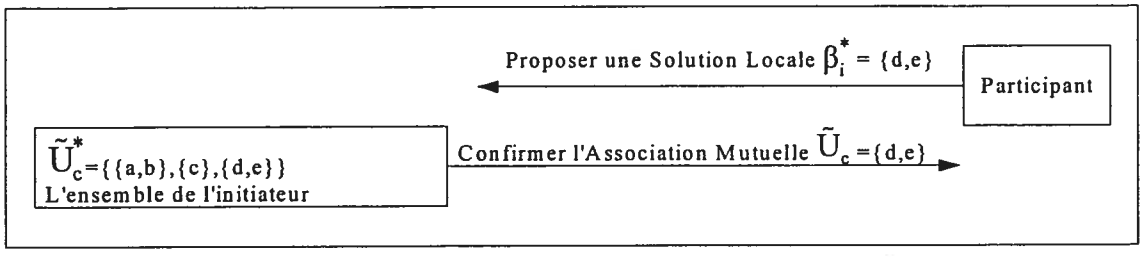

Figure 4.16 Association mutuelle directe

Dans la conception de l'association mutuelle, nous tenons compte de la modélisation formelle que nous avons révisée dans le tableau 3.4. Alors, dans le cas de l'association

directe, la condition suivante de la formule de l'association mutuelle du chapitre 3 est satisfaite :

L'ensemble des solutions mutuelles $\tilde{U}_c \in \cap \tilde{U}_c^*$

Aussi, la condition ($\|\beta_i\| = \min(\mu_i)$) de la formule de l'association mutuelle du chapitre 3 est satisfaite parce que les combinaisons de solutions sont envoyées du participant à l'initiateur par ordre croissant de cardinalité.

4.4.2 Concevoir l'association mutuelle indirecte

Ici, nous analysons la situation où la solution (β_i^*) envoyée par le participant n'existe pas dans l'ensemble des solutions locales de l'initiateur. C'est dans ce cas que l'initiateur essaie de composer une solution mutuelle. Pour montrer le processus que nous avons choisi d'appliquer, nous donnerons deux exemples suivis du cas général.

4.4.2.1 Cas de l'association mutuelle partielle – initiateur :

La solution de l'initiateur est une partie de la solution envoyée par le participant ($\beta^*_{i_{initiateur}} \subset \beta^*_{i_{participant}}$). Dans ce cas, l'initiateur cherche les solutions complémentaires ($\beta^*_{i_{participant}} - \beta^*_{i_{initiateur}}$) dans sa base de données ($U_{initiateur}$), et au cas où il les trouve, confirme l'association mutuelle ($\beta^*_{i_{participant}}$) au participant.

Si l'initiateur n'arrive pas à composer une solution mutuelle, alors il envoie un message demandant une solution alternative. Nous montrons un exemple de ce cas dans la figure 4.17.

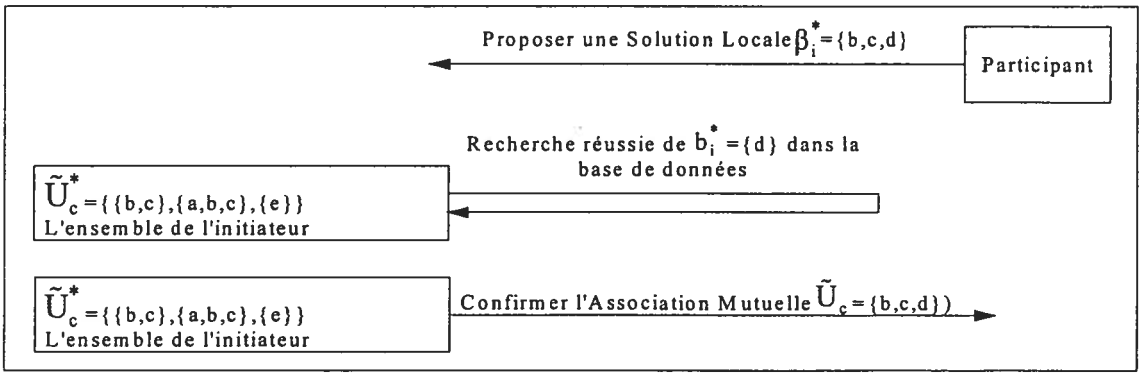

Figure 4.17 Association mutuelle partielle - initiateur

4.4.2.2 Cas de l'association mutuelle partielle – participant :

La solution envoyée par le participant est une partie d'une des solutions de l'ensemble de l'initiateur ($\beta^*_{i_{participant}} \subset \beta^*_{i_{initiateur}}$). Nous montrons un exemple de ce cas dans la figure 4.18.

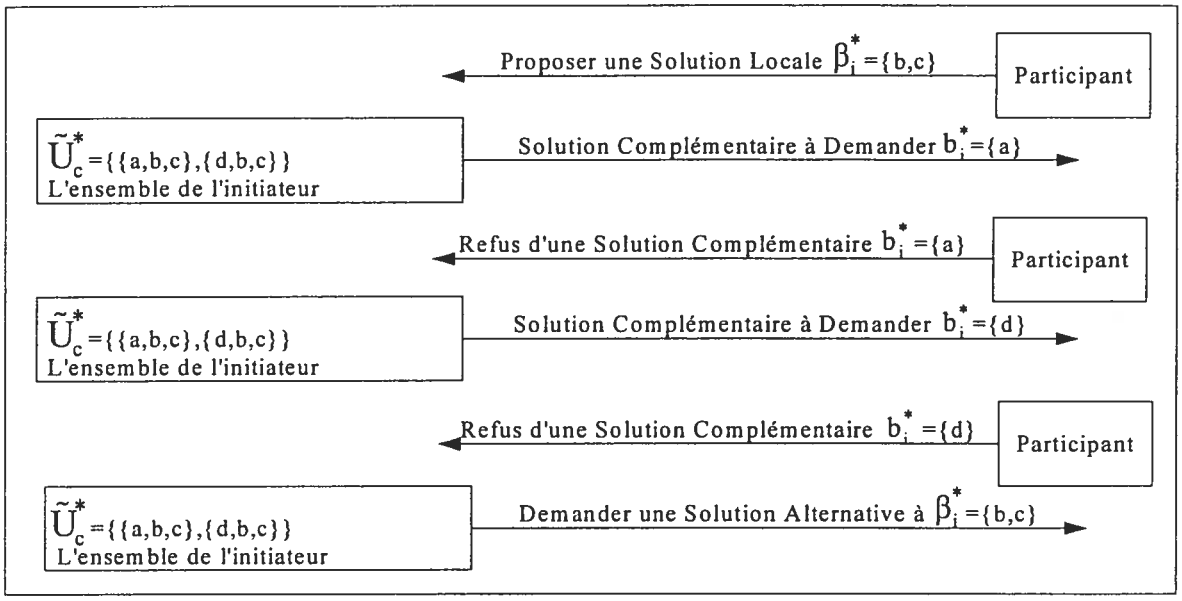

Figure 4.18 Association mutuelle partielle – participant

L'initiateur envoie des messages demandant au participant s'il est possible d'inclure les solutions complémentaires ($\beta^*_{i_{initiateur}} - \beta^*_{i_{participant}}$). C'est le participant, dans ce cas, qui tentera de trouver les solutions complémentaires dans sa base de données ($U_{participant}$) et qui confirmera ensuite à l'initiateur le résultat de cette recherche. Si l'initiateur n'arrive pas à composer une solution mutuelle, alors il envoie un message demandant une solution alternative.

4.4.2.3 Cas général de l'association mutuelle indirecte :

Le cas général de l'association indirecte est lorsque la solution envoyée par le participant ($\beta^*_{i_{participant}} = \sum b^*_{i_{participant}}$) est différente de toutes les solutions de l'ensemble de l'initiateur ($\forall \beta^*_{i_{initiateur}} = \sum b^*_{i_{initiateur}}$; $\beta^*_{i_{participant}} \neq \beta^*_{i_{initiateur}}$).

Dans ce cas, l'initiateur confirme que ($\beta^*_{i_{initiateur}} \cup \beta^*_{i_{participant}}$) est une solution mutuelle si : ($\forall b^*_i,\ b^*_i \notin \beta^*_{i_{initiateur}} \wedge b^*_i \in \beta^*_{i_{participant}}$), l'initiateur cherche la solution (b^*_i) dans sa base de données et la trouve

et

($\forall b^*_i,\ b^*_i \in \beta^*_{i_{initiateur}} \wedge b^*_i \notin \beta^*_{i_{participant}}$), l'initiateur envoie un message au participant lui suggérant l'inclusion de la solution complémentaire (b^*_i) dans la solution mutuelle composée et reçoit son approbation à la suggestion.

Si nous regardons de nouveau la modélisation formelle du tableau 3.4, nous remarquons que dans le cas de l'association indirecte, l'initiateur peut assurer la satisfaction de la condition ($||\beta_i|| = \min\ (\mu_i)$) seulement si le participant lui envoie tout son ensemble de solutions locales.

4.5 La communication entre les entités

Pour assurer la communication entre les entités de SecAdvise, nous avons choisi d'utiliser la technologie Java RMI (*Remote Methods Invocation*). Cette technologie fournit les mécanismes permettant une communication bilatérale entre deux objets écrits en Java résidants dans deux machines virtuelles Java (*Java Virtual Machine; JVM*) distantes.

Les applications RMI sont des applications d'objets distribués (*Distributed Object Application*) composées de deux programmes séparés : l'application serveur qui crée des objets et fournit leur référence à un registre RMI, et l'application client qui obtient les références des objets du registre RMI avant d'invoquer les méthodes de ces objets à distance.

Un attribut important de RMI c'est qu'elle permet de transmettre de manière dynamique le code et les données des objets d'un client à un serveur, et ce, même si les classes de ces objets ne sont pas définies chez le serveur [AW03]. Nous avons choisi cette

technologie pour effectuer la communication entre les entités de SecAdvise à cause de son efficacité et de sa facilité d'implantation. Dans notre prototype, chaque entité de SecAdvise comprendra les deux programmes, celui de client et celui de serveur, et jouera les deux rôles selon les besoins du protocole de communication.

Chapitre 5. L'expérimentation du modèle

5.1 Les scénarios de test

Pour les tests du prototype, nous utilisons un ordinateur *Intel Pentium III* qui a un processeur 400 MHz, une mémoire 384 MB et le système d'exploitation *Windows XP Professional.*

Nous exécutons deux programmes de SecAvise sur le même ordinateur (*local host*) en utilisant deux ports différents : le port 1099 et le port 1199. La plate-forme Java sur l'ordinateur en question est Java™ 2 SDK (*Standard Development Kit) Standard Edition* (*build 1.4.1_03*).

Nous évaluons le prototype de SecAdvise dans des scénarios de transaction de commerce électronique. Nous avons alimenté la table des solutions de la base de données avec 24 solutions que nous avons choisies parmi les standards et les spécifications les plus utilisés dans le domaine des échanges électroniques selon [CEN99].

Nous avons préparé dans le tableau A.1 de l'annexe A une liste qui montre les services de sécurité, les mécanismes (élémentaires et combinés) de sécurité, les modèles d'interaction de sécurité $S=\{s\}$ et les gestions des risques $R=\{r\}$ avec lesquelles nous avons alimenté la base de données.

Dans la section A.5 de l'annexe A, nous avons préparé un résumé qui donne la description des 24 standards et spécifications $U=\{u\}$ alimentés dans la base de données, les gestions des risques $R=\{r\}$ offertes par ces solutions, les mécanismes (élémentaires et combinés) de sécurité et les différents services de sécurité que ces solutions fournissent.

5.2 Les expérimentations

5.2.1 Les transactions du commerce électronique

La figure 5.1 montre une illustration fonctionnelle des étapes et des rôles des entités participantes dans des transactions du commerce électronique [CEN99].

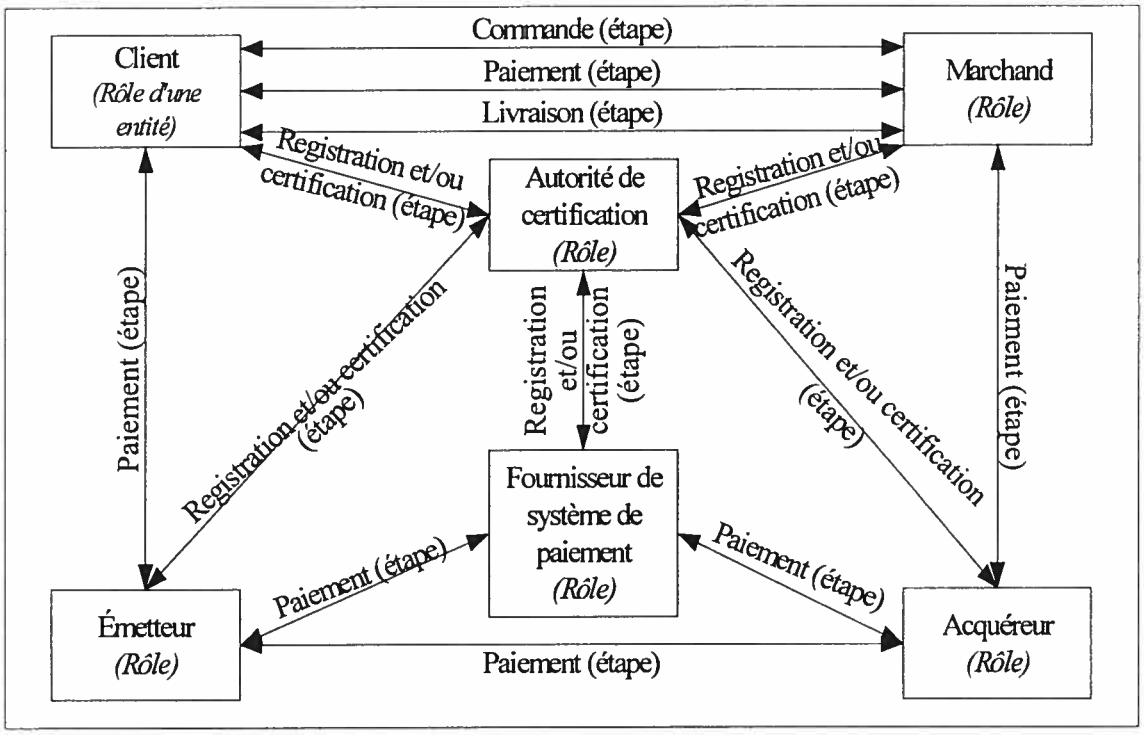

Figure 5.1 Étapes et rôles des entités dans des transactions du commerce électronique, traduit de [CEN99]

Chaque étape du commerce électronique se divise en plusieurs activités. Par exemple, l'étape de livraison comporte l'activité de gestion de livraison et l'activité de livraison électronique; chacune des activités requiert des services de sécurité spécifiques.

Le tableau 5.1 montre les activités des étapes du commerce électronique et les services de sécurité qu'elles requièrent [CEN99].

Si nous appliquons notre modélisation formelle de SecAdvise précisée dans le chapitre 3, nous remarquons que les lignes de ce tableau sont des éléments des profils de transaction du commerce électronique (c).

besoins des activités	authentification	contrôle d'accès	confidentialité de données	intégrité de données	non – répudiation
besoins généraux à toutes les étapes					
besoins généraux	√		√		√
étape de commande					
besoins généraux	√				
offre irrévocable					√
placement d'ordre					√
acceptation d'ordre					√
étape de livraison					
gestion livraison	√	√		√	√
livraison réseau	√			√	√
étape de paiement					
besoins généraux	√	√		√	
administration	√	√		√	√
chargement	√			√	√
instruction de paiement	√	√			√
autorisation	√				√
transfert de valeur	√	√			
livraison du reçu					√
saisie de données et dépôt	√	√		√	√

Tableau 5.1 Les services de sécurité des activités du commerce électronique, adapté de [CEN99]

La figure 5.2 montre des solutions communes à appliquer pour sécuriser les étapes du commerce électronique [CEN99]. Nos tests couvrent certaines activités du commerce électronique et démontrent comment SecAdvise choisit les solutions pour sécuriser les activités en question. Pour simplifier, nous avons considéré que les critères de choix de solutions ont des valeurs neutres et que les combinaisons de solutions fonctionnent ensemble.

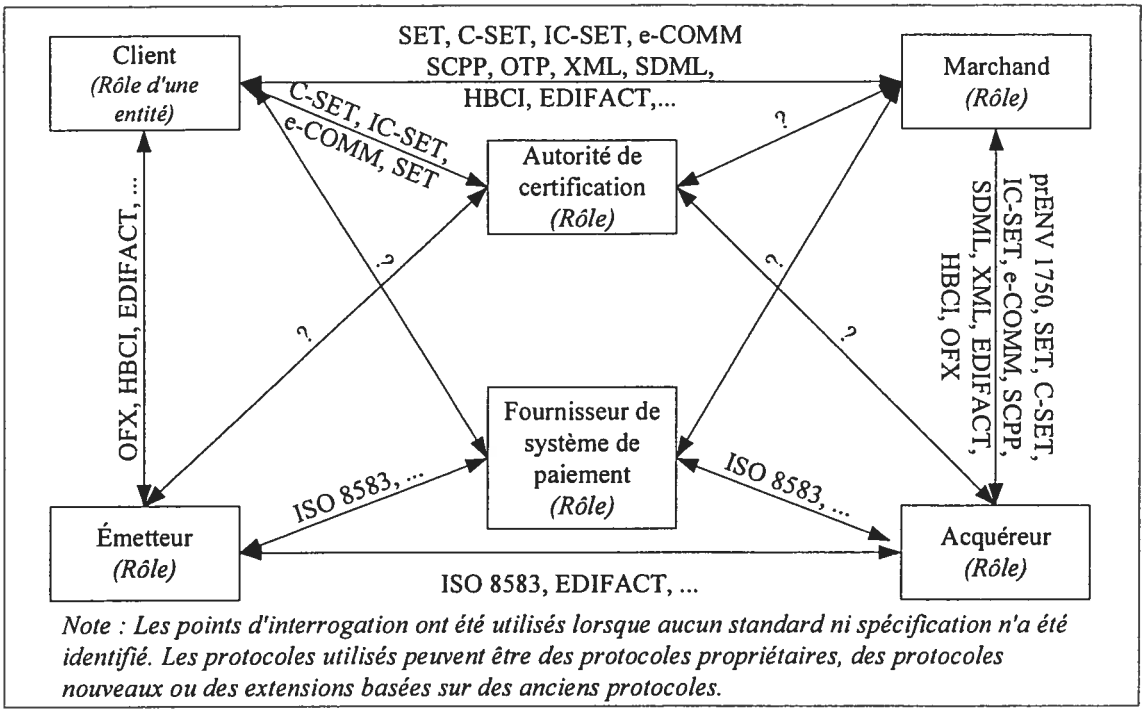

Figure 5.2 Solutions communes dans des transactions de commerce électronique, traduit de [CEN99]

5.2.2 Test et analyse d'une activité de commande

Nous avons choisi de commencer par tester l'activité de passation de commande qui confirme que le client adhère aux conditions de commande proposées par le marchand. La figure 5.3, tirée de [CEN99], montre une activité de passation de commande dans un scénario - type utilisé dans les ventes aux enchères.

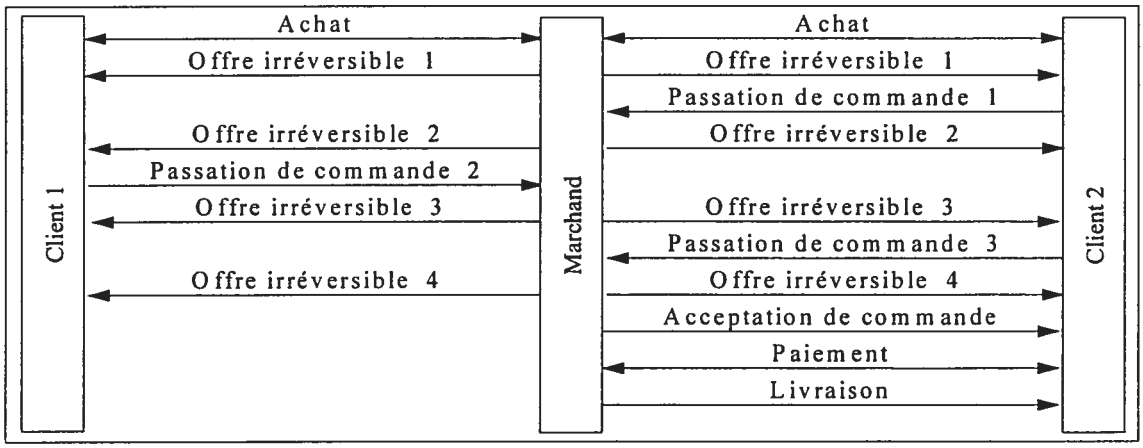

Figure 5.3 Placement d'activité de passation de commande dans un scénario de commande, traduit de [CEN99]

Si nous regardons le tableau 5.1 nous remarquons que toutes les activités de l'étape de commande ont les mêmes besoins de sécurité : l'authentification et la non-répudiation.

Le marchand et le client choisissent les gestions des risques convenables aux risques qu'ils envisagent sur ces services de sécurité. Pour ce test, nous supposons que c'est le client qui initie la transaction de commande. Nous avons décrit ce test dans le tableau 5.2.

Tester SecAdvise dans une activité de commande
Le contexte de la transaction défini par le client (initiateur / localhost : 1099)
Le type désiré des solutions : Standard.
L'application de l'initiateur : Application X de commande électronique.
Le domaine de la transaction : Commerce électronique.
Le sous-domaine de la transaction : Commande-passation d'une commande.
Les participants impliqués incluant l'initiateur : localhost : 1099, localhost : 1199.
Le certificat à échanger : X509.
Le type d'information à sécuriser : Seulement la transaction.
Le niveau désiré de sécurité : Couverture >=100%.
Gestions de risques et critères de solutions choisis par le client (localhost : 1099)
Gestions désirées des risques : Protection de l'authentification contre la divulgation et contre la répétition d'informations aux différents vérificateurs et protection contre tous les types de répudiation en utilisant les techniques de chiffrement asymétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.
La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.
Gestions de risques et critères de solutions choisis par le marchand (localhost : 1199)
Gestions désirées des risques : Protection de l'authentification contre la divulgation d'informations et protection contre tous les types de répudiation en utilisant les techniques de chiffrement asymétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.
La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.

Tableau 5.2 Le test de SecAdvise dans une activité de commande

L'ensemble de solutions locales du client calculé par le système a six solutions possibles: [ISO/IEC 7816 & ISO/IEC 9594, ISO 7816 & ISO/IEC 9798, ISO/IEC 9594 & ISO/IEC 9796, ISO/IEC 9594 & ISO/IEC 14888, ISO/IEC 9796 & ISO 9798, ISO 9798 & ISO/IEC 14888]. L'ensemble de solutions locales du marchand calculé par le système a six solutions possibles : [ISO/IEC 7816 & ISO/IEC 9594, ISO/IEC 7816 & ISO 10202, ISO/IEC 9594 & ISO/IEC 9796, ISO/IEC 9594 & ISO/IEC 14888, ISO/IEC 9796 & ISO 10202, ISO 10202 & ISO/IEC 14888].

Le cheminement de l'association mutuelle procède comme suit : Le marchand envoie sa première solution locale qui est (ISO/IEC 7816 & ISO/IEC 9594) au client. Le client trouve cette solution dans son ensemble de solutions locales, la confirme et la présente au marchand comme étant la solution mutuelle trouvée.

En général, les standards et les spécifications de sécurité offrent différents services de sécurité. Alors, nous remarquons que diminuer le niveau requis de couverture de risques diminue le nombre de solutions dans les combinaisons de solutions, c'est-à-dire les éléments des ensembles des solutions locales des participants. Cela a pour résultat de diminuer le nombre de solutions dans les combinaisons de solutions dans la solution mutuelle trouvée. Pour le démontrer, nous répétons le test avec une couverture de risques >=50 % au lieu de 100 %. Dans ce cas, l'ensemble de solutions locales du client calculé par le système a cinq solutions possibles : [ISO/IEC 7816, ISO/IEC 9594, ISO/IEC 9796, ISO 9798, ISO/IEC 14888]. L'ensemble de solutions locales du marchand calculé par le système a cinq solutions possibles : [ISO/IEC 7816, ISO/IEC 9594, ISO/IEC 9796, ISO 10202, ISO/IEC 14888].

Le cheminement de l'association mutuelle procède comme suit : La première solution mutuelle trouvée est (ISO/IEC 7816) qui assure les services de sécurité des deux types d'authentification exigés par les deux participants, mais qui n'offre pas le service de non-répudiation.

Le programme actuel laisse l'initiateur choisir le niveau de couverture de risques sans lui donner la possibilité de limiter le nombre de solutions nécessaires pour sécuriser la

transaction. Donc, en exigeant une haute couverture de risques, les participants devront être prêts à utiliser plusieurs solutions simultanément.

5.2.3 Test et analyse d'une activité de livraison

Pour notre prochain test de SecAdvise, nous avons choisi de tester l'activité de la livraison électronique qui est la réception de produits intangibles par l'intermédiaire de réseaux de données. La figure 5.4, tirée de [CEN99], montre une activité de livraison dans un scénario de commande du type utilisé par les entreprises de commande. Il se fait par courrier électronique et permet à ces dernières de présenter leur catalogue sur les réseaux ouverts (*mail order companies*).

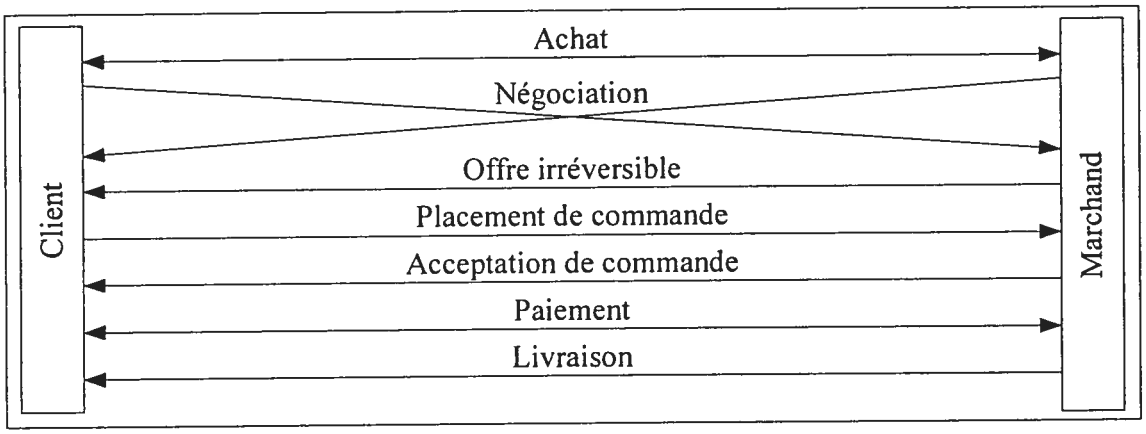

Figure 5.4 Placement d'activité de livraison dans un scénario typique de commande, traduit de [CEN99]

En regardant le tableau 5.1, nous remarquons que l'activité de livraison électronique demande au moins les services de sécurité d'authentification, d'intégrité de données et de non-répudiation. Pour ce test, le marchand et le client choisissent les gestions des risques convenables aux risques qu'ils envisagent sur ces services de sécurité et nous supposons que c'est le marchand qui initie la transaction. Nous avons décrit ce test dans le tableau 5.3.

Tester SecAdvise dans une activité de livraison
Le contexte de la transaction
Le type désiré des solutions : Spécification.
L'application de l'initiateur : Application X de livraison électronique.
Le domaine de la transaction : Commerce électronique.
Le sous-domaine de la transaction : Livraison électronique.

Les participants impliqués incluant l'initiateur : localhost : 1099, localhost : 1199.
Le certificat à échanger : X509.
Le type d'information à sécuriser : Seulement la transaction.
Le niveau désiré de sécurité : Couverture >=100%.
Gestions de risques et critères de solutions choisis par le marchand
Gestions désirées des risques : Protection de l'authentification contre la divulgation et la répétition d'informations au même vérificateur, détection de la modification non autorisée de données par l'utilisation de techniques cryptographiques et protection contre tous les types de répudiation en utilisant les techniques de chiffrement asymétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.
La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.
Gestions de risques et critères de solutions choisis par le client
Gestions désirées des risques : Protection de l'authentification contre la divulgation et la répétition d'informations au même vérificateur, prévention d'accès aux supports de transmission de données (contrôle de routage) et protection contre tous les types de répudiation en utilisant les techniques de chiffrement asymétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.
La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.

Tableau 5.3 Le test de SecAdvise dans une activité de livraison

L'ensemble de solutions locales du marchand calculé par le système a une solution : [S/MIME]. L'ensemble de solutions locales du client calculé par le système a une solution : [IPSec & S/MIME].

Le cheminement de l'association mutuelle procède comme suit : Le client envoie sa solution locale (IPSec & S/MIME) au marchand. Le marchand cherche cette solution dans son ensemble de solutions qui n'a que la solution (S/MIME) et n'arrive pas à faire une association. Alors, le marchand cherche la solution complémentaire (IPSec) dans sa

base de données et lorsqu'il la trouve, confirme (IPSec & S/MIME) comme solutions à utiliser pour sécuriser la transaction.

Nous remarquons dans ce test que les choix des gestions de risques d'un participant peuvent obliger l'autre participant à utiliser des solutions de sécurité dont il n'a pas besoin et qui ne sont pas nécessairement conformes à ses critères de choix de solutions. Pour donner un exemple de cela, nous répétons le même test avec différentes gestions de risques du côté client. Nous avons décrit ce nouveau test dans le tableau 5.4.

Gestions de risques et critères de solutions choisis par le client
Gestions désirées des risques : Protection de l'authentification contre la divulgation et la répétition d'informations au même vérificateur, prévention d'accès aux supports de transmission de données (contrôle de routage) et protection contre tous les types de répudiation en utilisant les techniques de chiffrement symétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.
La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.

Tableau 5.4 Le test de l'activité de livraison avec des gestions différentes des risques

L'ensemble de solutions locales du client calculé par le système contient trois combinaisons de solutions : [C-SET & IPSec & S/MIME, EMV & IPSec & S/MIME, IC-SET & IPSec & S/MIME].

Le cheminement de l'association mutuelle procède comme suit : Le client envoie sa première solution locale (C-SET & IPSec & S/MIME) au marchand. Le marchand cherche avec succès les solutions complémentaires (C-SET) et (IPSec) dans sa base de données et confirme (C-SET & IPSec & S/MIME) comme solutions à utiliser pour sécuriser la transaction.

Le test du tableau 5.4 montre que la solution mutuelle trouvée exige que le marchand utilise deux solutions de plus à la solution initialement proposée par son système pour sécuriser ses propres risques. Nous pouvons ajuster la conception du programme en

donnant aux utilisateurs la possibilité de définir la quantité et la qualité des solutions supplémentaires qu'ils sont prêts à utiliser en surplus afin d'entreprendre la transaction en question.

5.2.4 Test et analyse d'une activité de paiement

Nous testons SecAdvise dans une activité de paiement électronique. La figure 5.5, tirée de [CEN99], montre un scénario de paiement du type utilisé dans les systèmes traditionnels de paiement par carte. Par exemple, Visa et MasterCard sont des systèmes de paiement qui suivent ce scénario. Nous testons l'activité d'autorisation qui implique le marchand et l'acquéreur. Nous supposons que le marchand est l'initiateur de cette transaction. Selon le tableau 5.1, l'activité de l'autorisation demande au moins deux services de sécurité : l'authentification et la non-répudiation. Nous supposons que l'acquéreur n'a pas la solution (S/MIME) dans sa base de données. Nous avons décrit ce test dans le tableau 5.5.

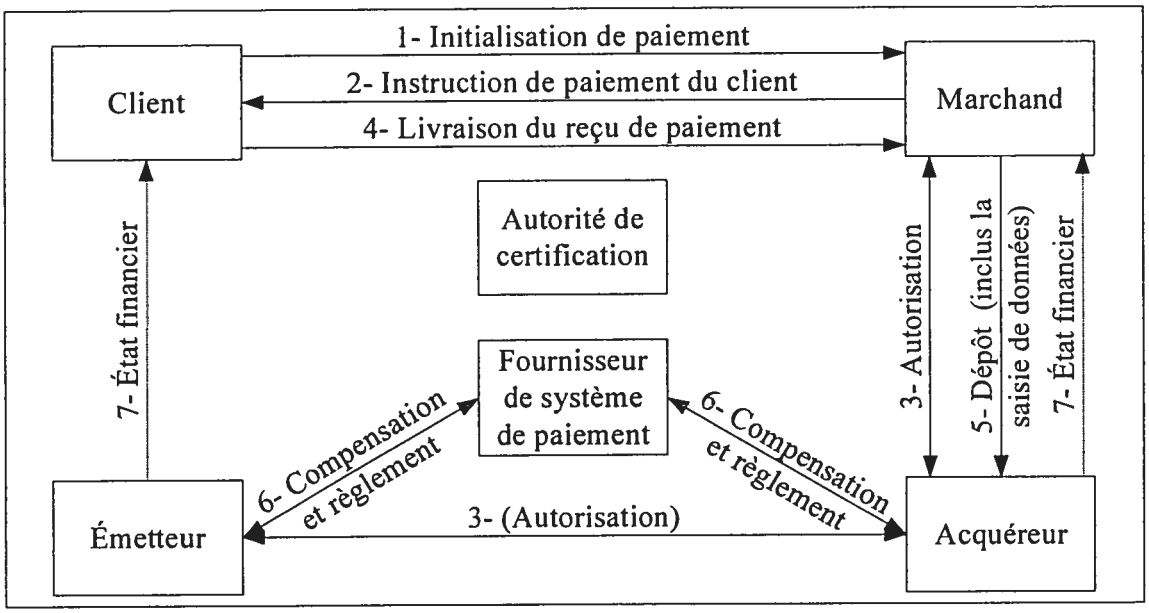

Figure 5.5 Les activités d'un scénario typique de paiement, traduit de [CEN99]

Tester SecAdvise dans une activité de paiement
Le contexte de la transaction
Le type désiré des solutions : Spécification.
L'application de l'initiateur : Application X de paiement électronique.
Le domaine de la transaction : Commerce électronique.

Le sous- domaine de la transaction : Autorisation.
Les participants impliqués incluant l'initiateur : localhost : 1099, localhost : 1199.
Le certificat à échanger : X509.
Le type d'information à sécuriser : Seulement la transaction.
Le niveau désiré de sécurité : Couverture >=100%.
Gestions de risques et critères de solutions choisis par le marchand (initiateur)
Gestions désirées des risques : Protection de l'authentification contre la divulgation et la répétition d'informations au même vérificateur et protection contre tous les types de répudiation en utilisant les techniques de chiffrement asymétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.
La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.
Gestions de risques et critères de solutions choisis par l'acquéreur (participant)
Gestions désirées des risques : Protection de l'authentification contre la divulgation et la répétition d'informations au même vérificateur ou aux différents vérificateurs et protection contre tous les types de répudiation en utilisant les techniques de chiffrement symétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.
La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.

Tableau 5.5 Le test de SecAdvise dans une activité d'autorisation

L'ensemble de solutions locales du marchand calculé par le système a une solution : [S/MIME]. L'ensemble de solutions locales de l'acquéreur calculé par le système a une solution : [C-SET, IC-SET, EMV & PGP, EMV & SET, EMV & TLS/SSL].

Le cheminement de l'association mutuelle procède comme suit : L'acquéreur envoie au marchand sa solution locale (C-SET), le marchand demande à l'acquéreur la possibilité d'inclure la solution complémentaire (S/MIME) dans la solution mutuelle. L'acquéreur refuse cette solution complémentaire car il ne l'a pas dans sa base de données. Alors, le marchand demande l'acquéreur une autre solution locale alternative. L'acquéreur envoie

toutes ses solutions locales une par une sans que le marchand n'arrive à faire une association mutuelle pour la même raison. La transaction ne peut pas être effectuée.

Nous remarquons dans ce test que les participants n'ont pas trouvé une association mutuelle et que, si les participants désirent vraiment exécuter la transaction, ils doivent modifier le contexte et/ou leurs gestions désirées des risques et/ou leurs critères de choix de solutions avant d'essayer à nouveau de faire une association. Notre programme actuel ne guide pas les utilisateurs dans cette modification et ils doivent recommencer le processus en espérant que la solution mutuelle existe. En effet, dans ce test, changer le type de solutions désirées de « spécifications » à « standards » suffit pour trouver une association; c'est ce que nous démontrons dans le test du tableau 5.6. Le programme n'anticipe pas cela lorsqu'il n'a pas les gestions exigées des risques des deux participants ni les noms et les caractéristiques des solutions disponibles dans leurs bases de données. S'échanger ces informations a l'avantage de faciliter les associations qui ne réussissent pas à la première tentative et le désavantage de nuire à la sécurité des systèmes des participants.

Tester SecAdvise dans une activité de paiement
Le contexte de la transaction
Le type désiré des solutions : Standard.
L'application de l'initiateur : Application de paiement électronique.
Le domaine de la transaction : Commerce électronique.
Le sous-domaine de la transaction : Autorisation.
Les participants impliqués incluant l'initiateur : localhost : 1099, localhost : 1199.
Le certificat à échanger : X509.
Le type d'information à sécuriser : Seulement la transaction.
Le niveau désiré de sécurité : Couverture >=100%.
Gestions de risques et critères de solutions choisis par le marchand (initiateur)
Gestions désirées des risques : Protection de l'authentification contre la divulgation et la répétition d'informations au même vérificateur et protection contre tous les types de répudiation en utilisant les techniques de chiffrement asymétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.

La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.
Gestions de risques et critères de solutions choisis par l'acquéreur (participant)
Gestions désirées des risques : Protection de l'authentification contre la divulgation et la répétition d'informations au même vérificateur ou aux différents vérificateurs et protection contre tous les types de répudiation en utilisant les techniques de chiffrement symétrique.
Restriction d'usage de solution : Pas de restriction.
La vitesse de l'exécution des solutions : Moyenne.
La complexité de l'exécution des solutions : Moyenne.
Le coût désiré des solutions : Moyen.

Tableau 5.6 Le deuxième test de SecAdvise dans une activité d'autorisation

L'ensemble de solutions locales du marchand calculé par le système a six solutions possibles : [ISO/IEC 7816 & ISO/IEC 9594, ISO/IEC 7816 & ISO/IEC 9798, ISO/IEC 9594 & ISO/IEC 9796, ISO/IEC 9594 & ISO/IEC 14888, ISO/IEC 9796 & ISO/IEC 9798, ISO/IEC 9798 & ISO/IEC 14888]. L'ensemble de solutions locales de l'acquéreur calculé par le système a six solutions possibles : [ISO/IEC 7816 & ISO/IEC 9798, ISO/IEC 7816 & ISO 10202, ISO/IEC 7816 & ECBS TCD 110, ISO/IEC 9797 & ISO/IEC 9798, ISO/IEC 9797 & ISO 10202, IS/IEC 9797 & ECBS TCD 110] .

Le cheminement de l'association mutuelle procède comme suit : L'acquéreur envoi au marchand sa première solution qui est (ISO/IEC 7816 & ISO/IEC 9798). Le marchand trouve la solution (ISO/IEC 7816) dans la combinaison (ISO/IEC 7816 & ISO/IEC 9594) de ces solutions.

Le marchand vérifie s'il a la solution (ISO/IEC 9798) dans sa base de données et lorsqu'il la trouve; il demande à l'acquéreur s'il est possible d'inclure le reste de sa combinaison de solution, c'est-à-dire la solution complémentaire (ISO/IEC 9594). Lorsque l'acquéreur confirme l'inclusion de cette solution complémentaire, le marchand confirme la combinaison (ISO/IEC 7816 & ISO/IEC 9594 & ISO/IEC 9798) comme solution mutuelle.

5.3 Conclusion des expérimentations

Dans les six tests précédents, l'algorithme du programme a réussi à trouver une solution mutuelle, lorsqu'elle existait, appropriée pour sécuriser les transactions de commerce électronique entre deux participants tout en tenant compte de leurs besoins individuels de sécurité. Nous avons alimenté la table des profils de la base de données avec les tests précédents. Au-delà de la démonstration du programme en marche, nous avons utilisé des tests visant à identifier des problèmes potentiels de la conception du système. Nous ajoutons à cela quelques conclusions tirées des tests :

1. Le programme selon notre conception a quatre critères de choix de solution : les restrictions d'usage, la vitesse de l'exécution, la complexité de l'exécution et le coût désiré. Pour simplifier, nous avons considéré que ces critères ont des valeurs moyennes pour toutes les solutions de la base de données et qu'il n'y pas de restriction légale sur l'usage des solutions. L'effet de nos suppositions est que ces critères sont neutres pour l'ensemble des solutions locales trouvées. En général, augmenter le nombre de critères et/ou le nombre de valeurs que chacun des critères peut prendre diminue le nombre de solutions de sécurité dans un contexte donné et donc, diminue la probabilité de trouver une association mutuelle.

2. Le choix des solutions d'une combinaison ne tient compte que des services de sécurité offerts par les solutions. Pour tenter de simplifier, nous avons supposé que les combinaisons de solutions peuvent être appliquées ensembles pour sécuriser une transaction. Pour que le programme soit fonctionnel, les effets réciproques des solutions doivent être soigneusement vérifiés, tel que cela est partiellement fait dans [FZ03], qui présente un modèle de validation automatique de la composition d'un ensemble de mécanismes de sécurité. Prendre ce point en considération réduira le nombre de solutions possibles à combiner et donc, réduira le nombre d'éléments des ensembles de solutions locales des participants et la probabilité de trouver une association mutuelle.

3. Les types de solutions avec lesquelles nous avons alimenté la base de données sont catégorisés en standards et spécifications. Pour un programme plus précis, nous devons faire une catégorisation plus profonde qui sépare les solutions spécifiques à certains contextes. Par exemple, distinguer les solutions spécifiques au contexte de paiement par monnaie électronique, de celles spécifiques au contexte de paiement par carte de crédit, etc. Cela va aussi avoir l'effet de diminuer le nombre de solutions disponibles pour chaque contexte.

4. Le participant envoie à l'initiateur les éléments de son ensemble de solutions locales un après l'autre. Si l'initiateur n'arrive pas à faire une association avec une solution quelconque envoyée par le participant, il tentera de construire une solution mutuelle à partir de cette solution en cherchant celles qui sont complémentaires dans sa base de données et/ou en demandant au participant d'ajouter des solutions complémentaires au besoin. Cependant, le reste de l'ensemble des solutions locales du participant peut contenir des solutions meilleures. Donc, le fait de ne pas s'échanger l'ensemble complet des solutions locales à des avantages du côté de la confidentialité et de la sécurité, mais il est possible qu'il nuise au résultat final.

Chapitre 6. Conclusion

6.1 Analyse des résultats

Pour conclure, voici les points principaux que l'on peut retirer de ce travail :

- La quantité et la qualité des solutions dans la table de solutions de la base de données des participants sont des facteurs très importants pour la réussite de l'association mutuelle. Par exemple, avec un nombre plus grand de solutions, l'ensemble de solutions locales qui couvre les risques d'une transaction aura plus d'éléments et, par la suite, la possibilité de trouver une association mutuelle entre les deux participants augmentera. Du côté de la qualité des solutions, il est, par exemple, plus efficace d'avoir dans la base de données des solutions qui offrent différents services de sécurité. Cela diminue le nombre des éléments dans les combinaisons de solutions.

- Nous avons alimenté la table de solutions de la base de données par 12 standards et 12 spécifications de sécurité. Chacune de ses solutions offre quelques services de sécurité qu'on peut exécuter par différents mécanismes combinés de sécurité. Nous pouvons enrichir la table de solutions en ajoutant les mécanismes élémentaires de sécurité. Ceux-ci offrent également des services de sécurité et peuvent être exécutés par différents mécanismes combinés. Par exemple, la fonction de compression, qui est un mécanisme élémentaire, peut être exécutée par le sceau, qui est un mécanisme combiné, pour fournir l'authentification. Le tableau A.2 de l'annexe A montre les mécanismes élémentaires qui peuvent être utilisés pour implanter les mécanismes combinés de sécurité. Le tableau A.3 de l'annexe A montre les services de sécurité qui peuvent être fournis par les mécanismes combinés de sécurité.

- Les interactions mutuelles des services de sécurité donnent plus de flexibilité aux choix de solutions locales. Par exemple, les mécanismes de l'authentification de

l'origine de données peuvent être utilisés pour supporter la non-répudiation. Le tableau A.4 de l'annexe A montre les interactions entre les services de sécurité.

- Le modèle bien défini de confiance de Robles a facilité la tâche de trouver la logique du calcul de la solution locale. De plus, la programmation de l'association mutuelle était facilitée par la flexibilité de la technologie RMI. Par contre, nous pensons que définir les gestions appropriées des risques et les associer aux solutions de sécurité convenables est une étape délicate et très importante pour la validité du modèle.

- Les contenus des bases de données des participants peuvent être différents, mais il est essentiel pour le fonctionnement correct de SecAdvise que les participants respectent une lexicologie uniforme des aspects de sécurité incluant les noms et les buts des solutions. Il n'est pas utile ni sécuritaire d'avoir une solution mutuelle qui n'a pas la même signification pour les différents participants impliqués.

- Le calcul de la solution locale risque d'utiliser beaucoup de mémoire de l'ordinateur, car il implique des combinaisons de solutions. Avec n modèles d'interaction de sécurité et m solutions de sécurité couvrant au moins un de ces modèles d'interaction, il y aura le nombre suivant de combinaisons à examiner :

$$\text{Nombre de combinaisons} = \sum_{n \in \mathbb{N}^*} \frac{m!}{n!(m-n)!}$$

- SecAdvise a l'avantage d'être un modèle d'architecture générale qui n'est pas limité par les services de sécurité qu'il offre, ni par le domaine d'application, ni par le type de transaction. Néanmoins, nous avons supposé que les utilisateurs des entités SecAdvise se font confiance mutuellement et cela n'est pas toujours évident dans le monde des affaires et peut limiter l'utilisation du système. Une autre limite possible est le fait que les entités communicantes doivent avoir le

même programme installé sur leurs systèmes respectifs pour pouvoir faire leurs échanges.

- Les facteurs économiques tels que le nombre d'usagers potentiels, leurs intérêts spécifiques et les coûts qu'ils sont prêts à investir dans leurs systèmes et ainsi de suite, n'ont pas été pris en considération. D'après [CEN01], il n'existe pas encore une base informatique de confiance pour le commerce électronique, ni suffisamment de bases légales sécuritaires à travers les frontières internationales. En outre, les usagers et les développeurs n'accordent pas suffisamment d'importance aux besoins de sécurité.

6.2 Atteinte des objectifs et Conclusion

Nous rappelons que les objectifs de SecAdvise consistent à contourner les problèmes d'interopérabilité et de compatibilité, à réduire la difficulté et le coût associés à la gestion de l'interopérabilité, à évaluer et réduire les risques de sécurité et à augmenter la confiance des utilisateurs [RS02]. Notre travail vise précisément à vérifier la possibilité d'atteindre ces objectifs par SecAdvise.

Nous avons conçu un logiciel basé sur l'approche SecAdvise en donnant aux utilisateurs deux possibilités pour évaluer les risques de sécurité :

1. La première possibilité consiste à laisser l'utilisateur décider et choisir les gestions des risques et le niveau minimal de couverture de risques qu'il trouve convenables.
2. La deuxième possibilité consiste à laisser l'utilisateur choisir un profil prédéfini de transactions. Dans le système final, les profils sont stockés par un administrateur expérimenté dans le système.

Notre conception du calcul de l'ensemble des solutions locales dans 4.2 et de l'association mutuelle dans 4.4 assure un choix des solutions qui satisfont le niveau de sécurité demandé par les utilisateurs. En outre, notre conception assure que le choix des solutions est approprié au contexte et aux risques locaux. Les solutions choisies sont

optimales, car le choix des solutions prend en considération des critères bien définis comme le coût, la vitesse, etc. Les combinaisons contenant le moins de solutions sont insérées dans l'ensemble des solutions locales d'abord et, par le fait même, sont échangées et évaluées en premier. Donc, par ce qui précède, nous avons démontré que SecAdvise réduit les risques et augmente la confiance des utilisateurs.

Nous avons démontré par les résultats des tests du chapitre 5 que SecAdvise améliore l'interopérabilité et aide les systèmes à trouver des moyens sécuritaires et optimaux pour effectuer des transactions. Cependant, les tests ont démontré que la négociation mutuelle doit être plus élaborée que la conception proposée.

Nous pensons que SecAdvise a de nombreux avantages, mais les tests qui ont suivi la conception et l'implantation ont démontré qu'il y a place à l'amélioration :

- En ce qui concerne le contexte de la transaction, nous pensons qu'il serait utile de donner aux usagers la possibilité de négocier entre eux le contexte de la transaction à entreprendre.
- En ce qui concerne le calcul de l'ensemble des solutions locales, nous pensons qu'il serait avantageux de donner aux usagers plus de contrôle pour choisir les caractéristiques des solutions, par exemple, le nombre maximal de solutions à utiliser ensemble.
- En ce qui concerne l'association mutuelle, nous pensons que le protocole de communication devrait donner aux usagers la possibilité d'échanger plus d'informations, si nécessaire, afin de faciliter les associations non réussies.
- Nous pensons aussi que le protocole de communication devrait être modifié par une approche de divulgation nulle afin d'éviter l'espionnage.

6.3 Travaux futurs

Pour les travaux futurs, nous suggérons les points suivants :

1. Raffiner la conception en retournant consulter les sections 6.1, 6.2 ainsi que les conclusion du chapitre 5.

2. Enrichir le contenu de la base de données. Par exemple, ajouter des services de sécurité spécifiques aux domaines d'application puisque le programme couvre actuellement les services de sécurité généraux. Par exemple, l'anonymat du payeur et la non traçabilité de la transaction de paiement sont des services de sécurité du domaine de paiement du commerce électronique qui peuvent être effectués par la signature invisible *blind signature*.
3. Compléter l'architecture du SecAdvise. Par exemple, Introduire les fonctions CRUD (*Create/Retrieve/Update/Delete*) dans la fenêtre de l'administrateur puisque le programme montre le contenu de la base de données, mais ne laisse pas l'usager modifier son contenu. On peut aussi introduire d'autres éléments du modèle de sécurité comme la politique de sécurité, les certificats, les clés, etc.
4. Tester le programme en effectuant des transactions complètes qui impliquent l'usage des mécanismes de sécurité choisis dans l'étape de l'association mutuelle.

Bibliographie

[ABW99] Andrew B. Whinston. *Interoperability in Global Electronic Commerce -- Senate Hearing on The Role of standards in the Growth of Global Electronic Commerce.* Subcommittee on Science, Technology and Space, Committee on Commerce, Science and Transportation, United States Senate, Washington, WA, USA, 1999

Available from www.senate.gov/~commerce/hearings/1028whi.pdf

[AW03] Ann Wollrath and Jim Waldo. *The Java™ Tutorial -- Trail -- RMI.* Sun Microsystems, Inc., Santa Clara, CA, USA, 2003.

Available from http://java.sun.com/docs/books/tutorial/rmi/

[CEN01] *Workshop agreement CWA 14228 -- Summaries of some Frameworks, Architectures and Models for Electronic Commerce.* European Committee for Standardization, Brussles, Belgium, 2001.

Available from http://www.cenorm.be/cenorm/businessdomains/businessdomains/informationsocietystandardizationsystem/published+cwas/cwa14228.pdf

[CEN99] *N 43 -- Report of the CEN/TC 224 -- ISO/TC 68/SC 6 Project on "Card related secure commercial and financial transactions on open networks".* European Committee for Standardization, Brussels, Belgium,1999.

Available from http://docbox.etsi.org/usergroup/open/Archive/Security/info9908.doc

[CSH99] Cay S. Horstmann and Gary Cornell. *Core Java 2 Volume I -- Fundamentals.* Sun Microsystems Press, A Prentice Hall Title, Palo Alto CA, USA, 1999.

[FH02] Frédéric Halter, Alain Grossmann and Jérôme Tollet. *Smart-IS A.M. -- Accompanying Measure for Accelerating Electronic Business and New Transactional Information Systems Project -- Security Solutions Review.* Information Societies Technologies (IST), Brussles, Belgium, 2002.

Available from http://www.smartis.org/minutes/other/ssr.pdf

[FZ03] Fathya Zemmouri. *Un modèle de validation automatique de mécanismes de sécurisation des communications.* Mémoire de maîtrise, Université de Montréal, Montréal, Qc, Canada, 2003.

[CJD98] Chris J.Date. *Introduction aux Bases de Données, 6e Édition.* Édition Vuibert, 1998

[GG99] Georges Gardarin. *Bases de Données : Objet et Relationnel.* Édition Eyrolles, Chapitre 4, 1999

[JC02] Jacques Claviez. *Sécurité Informatique -- Sécurité Des Systèmes d'Information et Sécurité Internet.* Editions J.C.i.inc, Ste-Agathe, Qc, Canada, 2002.

[MB00] Malgorzata Bienkowska. *Faire des affaires sur Internet – Rapport d'analyse.* Écoles Des hautes Études Commerciales, Montréal, Qc, Canada,2000

Available from http://members.tripod.com/~AMFIBIA/mypagef/projets/faire_des_affaires_doc.html

[MB98] Martin Bryan and Man-Sze Li. *OII Guide to Electronic Payment -- Information on the European Commission's Opens Information Interchange Services and how to use it.* On behalf of The European Commission Information Society – DG, Brussels, Belgium, 1998.

Available from http://www.diffuse.org/oii/en/e-pay.html

[RS02] Rima Saliba. *SecAdvise – un aviseur de mécanismes de sécurité.* Mémoire de maîtrise, Université de Montréal, Montréal, Qc, Canada, 2003.

[RS02a] Rima Saliba, Gilbert Babin and Peter Kropf. *Secadvise -- A Security Mechanisme Advisor.* Distributed Communities on the Web (DCW 2002), LNCS 2468, Springer, Berlin, pages 35–40, Sydney, Australia, 2002.

Available form http://www.cse.unsw.edu.au/~dcw2002/preliminary/A16.pdf

[SC02] *How the internet works -- Part 1.* Smart Computing Reference Series, Vol. 6, Issue 6, Summer 2002, Sandhills Publishing Company, Lincoln, NE, USA, 2002.

[SM01] Stuart McClure, Joel Scambray and Georges Kurtz. *Hacking Exposed: Network Security Secrets and Solutions-- Third Edition.* McGraw-Hill / Osborne, Berkeley, CA, USA, 2001.

[SR01] Serge Robles, Stefan Poslad, Joan Borell and John Bigham, *A practical trust model for agent-oriented electronic business applications.* in Proc. Of the 4th Int'l Conf. on Electronic Commerce Research (ICECR-4), volume 2, pages 397-406, Dallas, TX, USA, 2001.

[TAP02] Thomas A. Pender. *UML Weekend Crash Course.* Wiley Publishing, Inc., IN, USA, 2002.

[VH00] Vesna Hassler. *Security Fondamentals for E-commerce.* Computer Security Series, Artech House, MA, USA, 2001.

Note : *Pour la traduction des termes techniques de ce mémoire, nous avons surtout utilisé les informations contenues dans le site portail de l'Union européenne (Europa.eu.int/eurodicautom) et le grand dictionnaire terminologique de l'Office de la langue française du Québec (www.olf.gouv.qc.ca)*

Annexe A. Services et solutions de sécurité

A.1 Services et mécanismes de sécurité

Nous avons préparé dans le tableau A.1 une liste qui montre les services de sécurité, les mécanismes (élémentaires et combinés) de sécurité, les modèles d'interaction de sécurité $S=\{s\}$ et les gestions des risques $R=\{r\}$ avec lesquelles nous avons alimenté la base de données de notre programme.

La référence [CEN99] contient une explication détaillée de chacun des termes. Les codes seront utilisés dans les tableaux des résumés des solutions de sécurité de la section A.5 de l'annexe A pour montrer les services fournis par les différents standards et spécifications de sécurité.

Code	Services de Sécurité	Security Services
SS-1	Intégrité des données	Data integrity
SS-2	Authentification	Authentification
SS-3	Non-répudiation	Non repudiation
SS-4	Contrôle d'accès	Access control
SS-5	Confidentialité des données	Confidentiality
Code	Mécanismes élémentaires	Elementary mechanisms
ME-1	Fonction de compression	Hash function
ME-2	Fonction cryptographique de contrôle	Cryptographic check function
ME-3	Algorithme de chiffrement a clé secrète	Secret key encryption algorithm
ME-4	Algorithme à clé publique basé sur la factorisation	Public key encryption algorithm based on factorization
ME-5	Algorithme à clé publique base sur le logarithme discret	Public key algorithm based on discrete logarithm
ME-6	Algorithme à clé publique base sur le logarithme de courbes elliptiques	Public key algorithm based on elliptic curve logarithm
ME-7	Algorithme à connaissance nulle	Zero knowledge algorithm
ME-8	Voies dimensionnellement isolées	Physically isolated channels
ME-9	Réplication de données	Data replication
ME-10	Acheminement	Routing

ME-11	Algorithme de remplissage	Padding algorithm
ME-12	Hordotage	Time stamping
ME-13	Génération de numéros véritablement aléatoires	True random number generation
ME-14	Génération de numéros pseudo-aléatoires	Pseudo-random number generation
ME-15	Génération de numéros séquentiels	Sequence number generation
ME-16	Génération de numéros uniques	Unique number generation
Code	Mécanismes combinés	Combined mechanisms
MC-1	Sceau	Seal
MC-2	Signature numérique	Digital signature
MC-3	Réplication de données	Data replication
MC-4	Contrôle de routage	Routing control
MC-5	Chiffrement	Encipherment
MC-6	Remplissage de trafic	Traffic padding
MC-7	Authentification à apport de connaissance nulle	Authentication with zero knowledge
Code	Modèles d'interaction de sécurité	Security Interaction Models
MI-1	Classe d'authentification n 1	Authentification class 1
MI-2	Classe d'authentification n 2	Authentification class 2
MI-3	Classe d'authentification n 3	Authentification class 3
MI-4	Classe d'authentification n 4	Authentification class 4
MI-5	Confidentialité de l'information assurée par la prévention d'accès	Confidentiality provision through access prevention
MI-6	Confidentialité de l'information assurée par les techniques d'application	Confidentiality provision through mapping techniques
MI-7	Intégrité de l'information assurée par la cryptographie symétrique ou asymétrique	Integrity provision through symmetric & asymmetric cryptography
MI-8	Intégrité de l'information assurée par le contexte	Integrity provision through context
MI-9	Intégrité de l'information assurée par la détection et l'accuse de réception	Integrity provision through detection and acknowledgment
MI-10	Intégrité de l'information assurée par la prévention	Integrity provision through prevention
MI-11	La non répudiation par l'utilisation de techniques symétriques	Non-repudiation using symmetric techniques
MI-12	La non-répudiation par l'utilisation de	Non-repudiation using asymmetric

	techniques asymétriques	techniques
Code	Gestions de risques	Risk Managements
GR-1 Auth.	Protection de l'authentification contre la divulgation d'informations	Protection of authentication against disclosure
GR-2 Auth.	Protection de l'authentification contre la divulgation et la répétition d'informations aux différents vérificateurs	Protection of authentication against disclosure and replay on different verifiers
GR-3 Auth.	Protection de l'authentification contre la divulgation et le répétition d'informations au même vérificateur	Protection of authentication against disclosure and replay on the same verifier
GR-4 Auth.	Protection de l'authentification contre la divulgation et le répétition d'informations au même vérificateur ou aux différents vérificateurs	Protection of authentication against disclosure and replay on the same verifier or different verifiers
GR-5 Conf.	Protection contre les attaques sur le droit d'accès visant la divulgation des informations cachées	Protection against attacks on access right aiming the disclosure of hiding information
GR-6 Conf.	Protection du contenu sémantique des données par des transformations cryptographiques (chiffrement)	Protection of the semantics content of data by cryptographic transformation (encipherment)
GR-7 Conf.	Protection des informations, qui peuvent être dérivées par l'observation du flux de trafic, par l'utilisation du remplissage de données	Protection of the information that might be derived from observation of traffic flows by data padding
GR-8 Integ	Détection de la modification non autorisée de données par l'utilisation de techniques cryptographiques	Detecting unauthorized modification of data by using cryptographic techniques
GR-9 Integ.	Détection de la modification non autorisée de données par la réplication de données dans plusieurs zones de mémorisation	Detecting unauthorized modification of data by replication of data in several storage areas
GR-10 Integ.	Détection de la modification non autorisée de données par la réplication de données en temps différents	Detecting of unauthorized modification of data by replication of data at different times
GR-11 Integ.	Détection de la modification non autorisée de données par la répétition de l'envoi de données jusqu'a la réception d'un accusé de réception	Detecting of unauthorized modification of data by repeatedly sending the data until acknowledgment

GR-12 Integ.	Détection de la modification non autorisée de données par la répétition de l'envoi de données délimitée par la politique d'intégrité	Detecting of unauthorized modification of data by repeatedly sending the data until the integrity policy dictates
GR-13 Integ.	Prévention d'accès physique aux supports de stockage de données (contrôle d'accès)	Preventing physical access to data storage medium (access control)
GR-14 Integ.	Prévention d'accès aux supports de transmission de données (contrôle de routage)	Preventing physical access to data transmission media (routing control)
GR-15 N-Rep-S	Protection contre tous les types de répudiation en utilisant les techniques de chiffrement symétrique	Protection against several types of repudiation using cryptographic symmetric techniques
GR-16 N-Rep-As	Protection contre tous les types de répudiation en utilisant les techniques de chiffrement asymétrique	Protection against several types of repudiation using cryptographic asymmetric techniques

Tableau A.1 Les services et les mécanismes de sécurité, synthétisé de [CEN99]

A.2 Relation entre les mécanismes élémentaires et combinés

Le tableau A.2, tiré de [CEN99], montre les mécanismes élémentaires qui peuvent être utilisés pour implanter les mécanismes combinés de sécurité.

mécanismes combinés / mécanismes élémentaires	Sceau	Signature numérique	Réplication de données	Contrôle de routage	Chiffrement	Remplissage de trafic	Authentification à apport de connaissance nulle
Fonction de compression	X	X					
Fonction cryptographique de contrôle	X	X					
Algorithme de chiffrement a clé secrète	X				X		
Algorithme à clé publique basé sur la factorisation		X			X		
Algorithme à clé publique base sur le logarithme discret	Inconnu	X			X		
Algorithme à clé publique base sur le logarithme de courbes elliptiques	Inconnu	X			X		
Algorithme à connaissance nulle							X
Voies dimensionnellement isolées				X			
Réplication de données			X				
Acheminement				X			
Algorithme de remplissage	X	X			X	X	
Hordotage	X	X	X		X		
Génération de numéros véritablement aléatoires	X	X			X		X
Génération de numéros pseudo-aléatoires	X	X			X		X
Génération de numéros séquentiels	X	X			X		
Génération de numéros uniques	X	X			X		

Tableau A.2 les mécanismes élémentaires qui implantent des mécanismes combinés de sécurité, traduit de [CEN99]

A.3 Les services de sécurité offerts par les mécanismes de sécurité

Le tableau A.3 montre les services de sécurité qui peuvent être fournis par les mécanismes combinés de sécurité.

mécanismes combinés / service de sécurité	Sceau	Signature numérique	Réplication de données	Contrôle de routage	Chiffrement	Remplissage de trafic	Authentification à apport de connaissance nulle
Authentification	X	X			X		X
Intégrité des données	X	X	X	X			
Non répudiation	X	X					
Confidentialité des données					X	X	

Tableau A.3 les services de sécurité fournis par les mécanismes combinés de sécurité, synthétisé de [CEN99]

A.4 Les interactions entre les services de sécurité

Le tableau A.4 montre les interactions entre les différents services de sécurité.

	Contrôle d'accès	Confidentialité des données	Intégrité des données	Non-répudiation
Authentification	Quelques schémas de contrôle d'accès peuvent compter sur les résultats des services d'authentification	Les mécanismes d'authentification peuvent être utilisés pour la confidentialité de données	L'authenticité peut être utilisée pour supporter l'intégrité car elle implique l'intégrité des données. Sous certaines conditions, les mécanismes combinés qui fournissent l'intégrité de données peuvent être appliqués pour exécuter l'authentification L'intégrité de données peut-être utilisée en conjonction avec l'authentification pour fournir une assurance de la continuité de l'authentification et établir une corroboration de l'origine de données	Les mécanismes d'authentification de l'origine des données peuvent être utilisés pour supporter la non-répudiation Sous certaines conditions, les mécanismes combinés qui fournissent la non répudiation de données peuvent être appliqués pour exécuter l'authentification
Contrôle d'accès		Le contrôle d'accès peut interagir avec la confidentialité de données et créer des environnements confidentiels protégés	Le contrôle d'accès peut interagir avec l'intégrité de données et créer des environnements intègres protégés	Le contrôle d'accès peut supporter la non-répudiation
Confidentialité des données			La redondance en conjonction avec la confidentialité fournie par le chiffrement peut supporter l'intégrité	La confidentialité de données peut supporter la non-répudiation
Intégrité des données				L'intégrité de données peut supporter la non-répudiation

Tableau A.4 Les interactions entre les différents services de sécurité, synthétisé de [CEN99]

A.5 Résumé de solutions de sécurité

Dans la section suivante, nous avons préparé un résumé incluant la description des 24 standards et spécifications $U=\{u\}$ alimentant la base de données du programme, les gestions des risques $R=\{r\}$ offertes par ces solutions, les mécanismes (élémentaires et combinés) de sécurité ainsi que les différents services de sécurité fournis par ces solutions. Nous avons gardé le numéro de référence qui figure dans la référence [CEN99].

A.5.1 Standard - ISO/IEC 7816

Ref 07	ISO/IEC 7816 - Identification cards – Integrated circuit(s) cards with contacts 1994-06-15/1995-09-01/1995-11-16 /1996-05-15/ 1997-02-27 / 1997-06-26 / 1997-12-15 / 1998-01-07 /1998-07-31

Ce standard est la base des applications qui utilisent les cartes à circuit intégré ICC (*Integrated Circuit Cards*), incluant les cartes de paiement (débit, crédit et porte-monnaie électronique). De manière spécifique, les spécifications prEN 1546 et EMV sont fondées sur ce standard. Ce standard est constitué de dix parties qui couvrent différents aspects des cartes comme les caractéristiques physiques des cartes, la dimension, les commandes, le système de numérotation, les procédures d'enregistrement, les éléments des données utilisées dans les échanges interindustriels, le langage des requêtes SCQL (*Structured Card Query Language*), les commandes et les attributs de sécurité, le support de la signature électronique et de la cryptographie asymétrique et la vérification des certificats. [CEN99]

Relation avec le méc. élémentaire	Relation avec le mécanisme combiné	Gestions de risques offertes	Relation avec le modèle d'interaction de sécurité	Relation avec les services de sécurité
	MC-1	GR-8 Integ	MI-7	SS-1
	MC-2 avec récupération de message	GR-8 Integ	MI-7	
	MC-1	GR-15 N-Rep-S	MI-11	SS-3
	MC-2	GR-15 N-Rep-As	MI-12	
	MC-5			
				SS-2
				SS-4

A.5.2 Standard - ISO/IEC 8731

Ref 12	ISO 8731 – Banking – Approved algorithms for message authentication 1987-06-01 / 1992-09-15

Ce standard est constitué de deux parties. La première partie décrit l'algorithme DEA (*Data Encryption Algorithm*) comme méthode à utiliser pour le calcul de code d'authentification des messages MAC (*Message Authentification Code*). On peut aussi utiliser l'algorithme DEA pour calculer les sceaux (*seals*). L'algorithme DEA était publié sous le nom de ANSI X3.92. La deuxième partie de ce standard définit l'algorithme d'authentification des messages MMA (*Message Authentification Code*) comme méthode à utiliser pour le calcul de codes d'authentification des messages MAC. La deuxième partie de ce standard a des annexes qui donnent des exemples d'implantation de MAA et des tests [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-1	GR-8 Integ	MI-7	SS-1

A.5.3 Standard – ISO/IEC 9594

Ref 21	ISO/IEC 9594 – IT – OSI – The Directory 1995 / 1995-09-15 / 1996-04

La première partie de ce standard définit le répertoire (*The Directory*) comme une collection de systèmes ouverts qui coopèrent pour fournir une base de données logique d'informations sur un ensemble d'objets concrets. Ce standard définit une identification universelle pour les entités, fournit l'enregistrement et la recherche d'information sur les usagers et les ressources. C'est donc pour cette raison que les services du répertoire sont la fondation de l'interopérabilité des systèmes du commerce électronique. La partie huit de ce standard définit un schème de certification où le certificat fournit un lien de confiance entre l'identité d'une entité et ses données d'authentification. Les pages jaunes sont un exemple de l'utilisation de ce modèle dans l'Internet [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
ME-4				
	MC-1	GR-1 Auth.	MI-1	SS-2
	MC-1	GR-2 Auth.	MI-2	
	MC-2	GR-2 Auth.	MI-2	
	MC-1	GR-3 Auth.	MI-3	

A.5.4 Standard - ISO/IEC 9796

Ref 22	ISO/IEC 9796 - IT – Security techniques – Digital signature scheme giving message recovery 1991-09-15 / 1996-11-26 / 1997-07-12 / 1998-06-30

Ce standard décrit des schèmes de signatures digitales qui donnent une récupération des messages, c'est donc dire que la signature du message contient implicitement le message et que celui-ci sera récupéré au temps de vérification. Les parties de standard décrivent quatre méthodes différentes pour produire la signature : un mécanisme basé sur les systèmes cryptographiques à clé public du type RSA/Rabin, un mécanisme qui utilise une fonction de compression, un mécanisme qui utilise une fonction de contrôle et un mécanisme basé sur un algorithme discret. Ce standard est surtout pertinent pour les applications du commerce électronique basées sur les cartes à circuit intégré ICC (*Integrated Circuit Cards*) qui utilisent les techniques de signature à clé publique [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
ME-2 ME-5 ME-6 ME-11				
	MC-2 avec récupération de message	GR-8 Integ	MI-7	SS-1
	MC-2	GR-15 N-Rep-As	MI-12	SS-3

A.5.5 Standard – ISO/IEC 9797

Ref 23	ISO/IEC 9797 - IT – Security techniques – Message Authentication Codes (MACs) 1997-12-12

Ce standard spécifie six algorithmes généraux de codes d'authentification de messages MAC (*Message Authentification Code*) qui utilisent les mécanismes *(block cipher)* et celles avec fonction de compression. Ces algorithmes utilisent une clé secrète et un *(block cipher)* de longueur n bit pour calculer un code d'authentification de longueur m bit. Le standard a des annexes qui présentent des exemples de calcul avec différentes données et qui discutent du niveau de sécurité des algorithmes. Ce standard est pertinent pour protéger l'authenticité des messages du commerce électronique [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
ME-2 ME-11				
	MC-1	GR-8 Integ	MI-7	SS-1
	MC-1	GR-15 N-Rep-S	MI-11	SS-3

A.5.6 Standard – ISO/IEC 9798

Ref 24	ISO/IEC 9798 - IT – Security techniques – Entity authentication 1995-03-15 / 1997-08-01 / 1997-10-22 / 1998-04-25 / 1998-07-07

Ce standard spécifie l'authentification des entités. La première partie du standard est générale, elle spécifie un modèle d'authentification ainsi que les exigences et les contraintes d'utiliser les techniques de sécurité. Les autres parties de ce standard décrivent l'authentification des entités avec les mécanismes qui utilisent les algorithmes de chiffrement symétrique et asymétrique, les mécanismes qui utilisent les fonctions cryptographiques de contrôle et les mécanismes qui utilisent les techniques de connaissance nulle. Ce standard fournit une définition vaste des mécanismes de sécurité disponibles pour les besoins d'authentification des différents domaines incluant le commerce électronique [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
ME-7				
ME-12				
	MC-7			SS-2
	MC-1	GR-2 Auth.	MI-2	
	MC-2	GR-2 Auth.	MI-2	
	MC-5	GR-2 Auth.	MI-2	
	MC-1	GR-3 Auth.	MI-3	
	MC-2	GR-3 Auth.	MI-3	
	MC-5	GR-3 Auth.	MI-3	
	MC-1	GR-4 Auth.	MI-4	
	MC-2	GR-4 Auth.	MI-4	
	MC-5	GR-4 Auth.	MI-4	
	MC-7	GR-4 Auth.	MI-4	

A.5.7 Standard – ISO 10126

Ref 29	ISO 10126 – Banking – Procedures for message encipherment (wholesale) 1991-07-15 / 1991-11-01

Ce standard est constitué de deux parties. La première partie spécifie des procédures pour protéger au moyen du chiffrement des messages financiers. Ce standard est implicitement défini pour être utilisé

avec les algorithmes symétriques. La deuxième partie décrit l'implantation du standard en utilisant l'algorithme DEA (*Data Encryption Algorithm*). Ce standard peut être pertinent pour le chiffrement des messages du commerce électronique, surtout pour les techniques de remplissage définies lorsque l'algorithme DEA est utilisé au CBC mode (*Cipher Block Chaining)* [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
ME-3 ME-11				
	MC-5	GR-6 Conf.	MI-6	SS-5

A.5.8 Standard – ISO 10202

Ref 31	ISO 10202 - Security architecture of financial transaction systems using ICCs (Integrated Circuit Cards) 996-02-01 / 1998-07-01 / 1998-07-15

Les huit parties de ce standard couvrent le cycle de vie des cartes à circuits intégrés, le processus des transactions, les relations entre les clés cryptographiques, les modules d'application de sécurité (*Security Application Module ; SAM*), l'usage des algorithmes, la vérification de l'identité du possesseur de la carte, la gestion des clés et autres principes généraux. Ce standard définit les requis minimaux de l'architecture de sécurité des systèmes des transactions financières basées sur les cartes à circuits intégrés. Ce standard fournit une base pour les conceptions et les implantations des applications du commerce électronique qui utilisent les cartes à circuits intégrés (*Integrated Circuit Cards; ICC*) [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
				Gestions clés
	MC-2	GR-1 Auth.	MI-1	SS-2
	MC-5	GR-1 Auth.	MI-1	
	MC-1	GR-4 Auth.	MI-4	
	MC-2	GR-4 Auth.	MI-4	
	MC-5	GR-4 Auth.	MI-4	

A.5.9 Standard – ISO/IEC 14888

Ref 49	ISO/IEC 14888 - IT – Security techniques – Digital signatures with appendix 1997-11-18 / 1998-09-10 / 1998-10-09

La première partie de ce standard spécifie plusieurs mécanismes de signature digitale avec appendices pour les messages de longueurs arbitraires. La deuxième partie spécifie la structure générale et les procédures fondamentales qui constituent la signature digitale et les processus de vérification des mécanismes de signature digitale avec appendices pour les messages de longueurs arbitraires. La troisième partie spécifie des mécanismes de signature digitale avec appendices basés sur l'usage des certificats. Ce standard est pertinent au commerce électronique lorsque la signature digitale est utilisée pour exécuter les services de sécurité [CEN99].				
Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
ME-7				
	MC-2	GR-8 Integ	MI-7	SS-1
	MC-2	GR-15 N-Rep-As	MI-12	SS-3

A.5.10 Standard – ECBS TCD110

Ref 64	ECBS TCD110 – The Interoperable Financial Sector-Electronic Purse 1998-06-19			
Les quatre parties de ce standard décrivent les porte-monnaie électroniques (*Intersector Electronic Purse*), ils donnent la description fonctionnelle détaillée, l'architecture de sécurité, la description des transactions, la circulation des messages et le dictionnaire de données. Le but de ce document est d'être une spécification d'implantation, contrairement au document prEN1546 qui donne plusieurs options. Ce document est très détaillé et fixe, surtout en ce qui concerne le contenu des échanges et des méthodes cryptographiques utilisées. Ce document peut être pris en considération lors de la définition des transactions de monnaie électronique du commerce électronique [CEN99].				
Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-3			
	MC-2	GR-4 Auth.	MI-4	SS-2

A.5.11 Standard – ANSI X3.92

Ref 69	ANSI X3.92 - DEA Data Encryption Algorithm 1981 (R1987)			
Ce standard (*Data Encryption Algorithm; DEA*) décrit le chiffrement symétrique et définit les tables de permutations et les tables de substitutions. Le document inclut des exemples de tests [CEN99].				
Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
ME-3				
	MC-5	GR-6 Conf.	MI-6	SS-5

A.5.12 Standard – ANSI X3.106

Ref 70	ANSI X3.106 - Modes of Operation for the Data Encryption Algorithm (DEA) (R 1996)

Ce document décrit des modes d'opération qui utilisent l'algorithme de chiffrement de données DEA. (*Data Encryption Algorithm*). Les trois modes décrits sont : (*Electronic Code Book; ECB, Cipher Block Chaining; CBC et Cipher Feed Back; CFB)* [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
ME-3 (DEA/DES)				
	MC-5	GR-6 Conf.	MI-6	SS-5

A.5.13 Spécification – C-SET

Ref 04	Chip-Secured Electronic Transaction-(C-SET)-Groupement des Cartes Bancaires "CB" 97-01-29

C-SET à l'initiative du GIC bancaire est un groupement prévoyant une expérimentation grandeur nature qui s'est créé en Europe pour adapter les spécifications SET aux cartes bancaires à puces. Ce document décrit l'architecture de sécurité de C-SET [MB00].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-2	GR-4 Auth.	MI-4	SS-2
	MC-1	GR-8 Integ	MI-7	SS-1
	MC-1	GR-15 N-Rep-S	MI-11	Mécanismes de SS-3 sont fournis
	MC-2	GR-15 N-Rep-As	MI-12	
				SS-5

A.5.14 Spécification – e-COMM

Ref 05	e-COMM Project – e-COMM consortium 1998-04-03

Ce document donne une vue d'ensemble technique du projet e-COMM [CEN99]. e-COMM à l'initiative du E-comm consortium (regroupant BNP, Crédit Lyonnais, Visa, France Télécom et Gemplus) est un groupement prévoyant une expérimentation grandeur nature qui s'est créé en Europe pour adapter les spécifications SET aux cartes bancaires à puce [MB00]. e-COMM est une solution pour les paiements sécuritaires sur Internet dont la révocation de ceux-ci est impossible. Le type de paiement est la carte de crédit à puces [FH02].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-1	GR-8 Integ	MI-7	SS-1
				SS-5
				SS-2
				SS-3

A.5.15 Spécification – EMV

Ref 06	EMV Specifications – EMV'96 - 1998-05-31

Ce sont des spécifications pour les paiements effectués par des cartes à circuits intégrés (*Integrated Circuit Cards; ICC*) [CEN99]. Ces spécifications privées, qui ont été développées par Europay MaterCard et Visa, définissent les procédures nécessaires pour effectuer des transactions de paiements dans un environnement d'échanges internationaux. Les trois parties de ce document décrivent les spécifications des systèmes de paiements pour les cartes à circuits intégrés, les spécifications des systèmes de paiements pour les terminaux des cartes à circuits intégrés et les spécifications des systèmes de paiements pour les applications des cartes à circuits intégrés [MB98].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-2	GR-8 Integ	MI-7	SS-1
	MC-1	GR-15 N-Rep-S	MI-11	SS-3
	MC-1	GR-15 N-Rep-As	MI-12	
	MC-2	GR-15 N-Rep-As	MI-12	
				SS-2

A.5.16 Spécification – GDSA

Ref 13	German Signature Act, Signature Ordinance and related Draft BSI manual for GDSA (GDSA) 1997-07-22 / 1997-10-22

Ce document contient trois parties : un acte de signature digitale qui vise à établir les conditions rendant celle-ci sécuritaire, une ordonnance qui définit les procédures administratives des licences et un manuel qui décrit les requis techniques et organisationnels ainsi que les façons de les remplir. Cet acte est une base bien connue pour que les signatures digitales soient légalement engageantes comme les activités de commandes. L'acte définit un modèle de sécurité complet mais ne considère pas les facteurs économiques [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-2	GR-8 Integ	MI-7	SS-1
	MC-2	GR-15 N-Rep-As	MI-12	SS-3

A.5.17 Spécification – HBCI

Ref 16	Home banking Computer Interface (HBCI) – German Banking Committee 1998-02-02

Ce document décrit les spécifications de l'interface (*Home banking Computer Interface ; HBCI*) [CEN99]. HBCI qui est un mécanisme de support des paiements électroniques. HBCI est un nouveau standard pour la communication et les échanges de transactions entre les systèmes intelligents des clients et les centres de calcul. Les spécifications HBCI couvrent les formats des messages qui échangent les informations entre les banques et leurs clients à domicile. La transmission des données est effectuée par une interface de données qui est basée sur une syntaxe flexible similaire à l'UN/EDIFACT [MB98]..

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
				SS-2
	MC-2	GR-8 Integ	MI-7	SS-1
	MC-2	GR-15 N-Rep-As	MI-12	SS-3
	MC-1			

A.5.18 Spécification – IC-SET

Ref 23	Interoperable C-SET (IC-SET) – Banksys / Groupement des Cartes Bancaires "CB" 1997-06-02

Ce document donne une description d'affaires (*business description*) des spécifications IC-SET [CEN99]. IC-SET est une spécification de mécanismes de paiement privée qui a été développée par le Groupement des Cartes Bancaires et Banksys pour effectuer les transactions de paiements électroniques sécuritaires basées sur les cartes à puces dans les réseaux ouverts. IC-SET supporte les applications de cartes bancaires de débit et de crédit, ainsi que les applications de porte-monnaie électronique. L'interopérabilité avec les différents systèmes domestiques de paiements de crédit et de débit par carte à puces est assurée en utilisant des interfaces au système SET et des convertisseurs de logiciels [MB98].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
				SS-5
	MC-2	GR-4 Auth.	MI-4	SS-2

	MC-1	GR-8 Integ	MI-7	SS-1
	MC-1	GR-15 N-Rep-S	MI-11	SS-3
	MC-2	GR-15 N-Rep-As	MI-12	

A.5.19 Spécification – IPSec

Ref 24	IP Security protocol (Ipsec) – RFC 2401 – RFC 2402 – RFC 2406 – RFC 2407 – RFC 2408 – RFC 2409 – RFC 2411 / 1998-11

La suite de protocoles Ipsec dans la couche IP est conçue pour fournir des services de sécurité de haute qualité et interopérable en se basant sur l'usage des techniques cryptographiques sur IPv4 et IPv6. Ces documents (*Request for Comments ; RFCs*) décrivent les concepts nécessaires pour établir une interopérabilité entre les mécanismes de sécurité au niveau de la couche IP. Ces concepts peuvent être utilisés dans le commerce électronique, mais ils sont spécifiques au protocole et ne peuvent pas être utilisés comme un standard indépendant du protocole. Les schémas de négociations ne sont pas adressés dans ces documents [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
				Gestion des clés
				SS-2
				SS-4
				SS-5
ME-10	MC-4	GR-14 Integ.	MI-10	SS-1
	MC-6			

A.5.20 Spécification – PGP

Ref 32	Pretty Good Privacy (PGP) – RFC 2440 1998-11

Le modèle PGP concerne la certification et le chiffrement, il est approprié pour la protection des courriers électroniques. Le modèle PGP peut être considéré comme une solution au problème de manque d'une autorité centralisée dans le réseau Internet, mais il est inapproprié pour un grand groupe d'usagers. Une confiance suffisante aux clés ne peut pas être accomplie. La distribution et le stockage des certificats par les usagers, ainsi que la révocation de certificats sont un problème.

L'usage de PGP dans le commerce électronique est difficile car il n'y a pas d'entité responsable de la résolution des disputes. Les intérêts des affaires, qui nécessitent être garanties par des contrats bien définis, peuvent ne pas être très bien protégés [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
				SS-3
	MC-2	GR-4 Auth.	MI-4	SS-2
	MC-1	GR-8 Integ	MI-7	SS-1

A.5.21 Spécification – PKCS

Ref 34	Public-Key Cryptography Standards (PKCS) – RSA Laboratories – PKCS#1,7,10 1993-11-01 PKCS#11 1997-12-22

Ces spécifications ont quatre patries : PKCS#1, 7, 10 et 11. PKCS#1 décrit une méthode pour le chiffrement des données en utilisant le système de chiffrement à clé publique RSA. PKCS#7 décrit une syntaxe générale pour les données sur lesquelles le chiffrement sera appliqué. PKCS#10 décrit une syntaxe pour les certificats. PKCS#11, qu'on appelle Cryptoki, définit une interface d'application pour les devises cryptographiques. Les spécifications PKCS sont largement utilisées pour la sécurisation sur Internet, particulièrement par S/MIME. Les applications (*secure e-mail*) et SET utilisent PKCS pour assurer la sécurité. Cryptoki est largement utilisé aussi, par exemple, dans le Communicateur de Netscape [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-5	GR-6 Conf.	MI-6	SS-5
	MC-2	GR-8 Integ	MI-7	SS-1
	MC-2	GR-15 N-Rep-As	MI-12	SS-2

A.5.22 Spécification – S/MIME

Ref 37	Secure /Multipurpose Internet Mail Extensions (S/MIME) 1997-11 / 1998-01-28 / 1998-02-16 / 1998-03

MIME fournit une structure générale pour les types de contenu des messages échangés sur Internet et permet des extensions pour les applications aux nouveaux types de contenu. S/MIME fournit une méthode pour sécuriser les messages MIME en utilisant le chiffrement et la signature digitale. S/MIME est utilisé pour les échanges avec le courrier électronique des certificats et des informations sécurisées. S/MIME peut être considéré pour l'interopérabilité de sécurité car il fournit une grande capacité de négociation d'algorithmes et de paramètres [CEN99].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-2	GR-3 Auth.	MI-3	SS-2

	MC-5	GR-6 Conf.	MI-6	SS-5
	MC-2	GR-8 Integ	MI-7	SS-1
	MC-2	GR-15 N-Rep-As	MI-12	SS-3

A.5.23 Spécification - SET

Ref 38	Secure Electronic Transaction specification – SET – MasterCard, Visa 1997-05-31 / 1997-09-24

Les quatre parties de ce document décrivent le protocole SET (*Secure Electronic Transaction*) et donnent une description d'affaires, un guide des programmeurs, les définitions formelles du protocole et un guide de l'interface externe [CEN99]. SET est un ensemble de spécifications publiques développées par Visa et MasterCard pour effectuer des transactions sécuritaires avec les cartes bancaires sur les réseaux ouverts. Les spécifications SET couvrent l'application des algorithmes cryptographiques, les messages des certificats, les formats des objets, les messages de l'achat, les messages de capture de données et les messages de protocole entre les participants [MB98].

Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
	MC-3			
ME-11	MC-2	GR-4 Auth.	MI-4	SS-2
	MC-5	GR-6 Conf.	MI-6	SS-5
	MC-6	GR-7 Conf.	MI-6	
	MC-2	GR-8 Integ	MI-7	SS-1
	MC-2	GR-15 N-Rep-As	MI-12	Les mécanismes de SS-3 sont fournis

A.5.24 Spécification – TLS & SSL

Ref 49	Transport layer Security (TLS & SSL) 1997-05-21

SSL est la spécification la plus utilisée pour la sécurisation des paiements du commerce électronique. SSL est implantée dans la plupart des fureteurs et des serveurs Web. SSL fournit aussi une spécification de sécurité interopérable destinée pour l'usage sur les réseaux ouverts. La spécification TLS vise à fournir une sécurité cryptographique, une interopérabilité entre les applications, une efficacité relative par l'usage des sessions et un modèle extensible capable d'inclure des nouvelles clés publiques et cryptographiques. La spécification TLS a la même fondation que SSL mais elle est publique [CEN99].				
Méc. Élém.	Méc. Com.	Gestions de risques offertes	Mod. Interaction	Serv. Sécurité
				SS-1 Le mécanisme de SS-3 est fournis
	MC-2	GR-4 Auth.	MI-4	SS-2
	MC-5	GR-6 Conf.	MI-6	SS-5

Note 1 : Quelques standards et spécifications ont des versions plus récentes.
Note 2: Quelques spécifications peuvent être obsolètes ou pas encore implantées.

Annexe B. Le protocole de communication

Le tableau B.1 montre une liste détaillée des messages du protocole de communication et leurs significations. Cette liste permet de construire les scénarios de communication entre les participants selon les besoins du déroulement de la transaction.

#	Nom du message	But du message
1	Proposer une transaction	Ce message envoyé de l'initiateur au participant de son choix transmet le contexte de la transaction voulue.
2	Refuser une communication	Ce message envoyé du participant à l'initiateur accuse la réception du message numéro (1) plus haut; il implique que le participant est présentement incapable de participer dans la communication.
3	Refuser une transaction	Ce message envoyé du participant à l'initiateur accuse la réception du message numéro (1) plus haut et indique à l'initiateur que le participant n'a pas approuvé le contexte de la transaction en cours. Dans le programme final, ce message peut transmettre la raison du refus pour que l'initiateur propose une version modifiée du contexte s'il désire vraiment effectuer la transaction avec ce participant.
4	Approuver une transaction	Ce message envoyé du participant à l'initiateur accuse la réception du message numéro (1) plus haut et indique à l'initiateur que le participant a approuvé le contexte de la transaction en cours et qu'il procédera au calcul de l'ensemble de ses solutions locales.
5	Confirmer une transaction	Ce message envoyé de l'initiateur au participant accuse la réception du message (4) plus haut et indique que l'initiateur procédera lui aussi au calcul de l'ensemble de ses solutions locales.
6	Proposer une solution locale	Ce message envoyé du participant à l'initiateur accuse la réception du message (5) plus haut ou du message (7) plus bas et transmet une solution locale.
7	Demander une solution alternative	Ce message envoyé de l'initiateur au participant accuse la réception du message (6) plus haut et confirme qu'une association mutuelle n'a pas encore été trouvée.
8	No solution alternative	Ce message envoyé du participant à l'initiateur peut être un accusé de réception du message (7) plus haut et indique que le participant n'a plus de solutions locales à proposer.
9	Confirmer l'association mutuelle	Ce message envoyé de l'initiateur au participant accuse la réception du message (6) plus haut et confirme que l'initiateur a trouvé une association mutuelle. Ce message transmet la solution mutuelle trouvée.

10	Solution complémentaire à demander	Ce message envoyé de l'initiateur au participant peut-être un accusé de réception du message (6) plus haut. Il transmet le nom d'une solution particulière et confirme qu'une association mutuelle peut être trouvée si le participant accepte d'inclure cette solution particulière dans son ensemble de solutions locales.
11	Accepter une solution complémentaire	Ce message envoyé du participant à l'initiateur accuse la réception du message (10) plus haut et indique que le participant accepte d'inclure dans son ensemble de solutions locales, la solution particulière envoyée par le message(10).
12	Refuser une solution complémentaire	Ce message envoyé du participant à l'initiateur accuse la réception du message (10) plus haut et indique que le participant refuse d'inclure dans son ensemble de solutions locales, la solution particulière envoyée par le message(10).
13	Commencer la transaction	Ce message envoyé du participant à l'initiateur accuse la réception du message (9) plus haut et indique que le participant est prêt à commencer la transaction avec la solution mutuelle trouvée
14	Abandonner une transaction	Il peut servir comme approbation aux messages suivants : -Message numéro (3) qui est Refuser une Transaction. -Message numéro (8) qui est No Solution Alternative Il peut aussi être envoyé par n'importe quel parti à n'importe quel moment simplement pour indiquer le désir de rompre la communication en cours sans expliquer les raisons. Une approbation du reçu de ce message n'est pas obligatoire.

Tableau B.1 Une liste détaillée des messages du protocole de communication et de leur signification