Université de Montréal

SecAdvise : un aviseur de mécanismes de sécurité

par

Rima Saliba

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

Mai 2003

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

SecAdvise : un aviseur de mécanismes de sécurité

présenté par:

Rima Saliba

a été évalué par un jury composé des personnes suivantes:

Stefan Wolf,	Président-rapporteur
Peter Kropf,	Directeur de recherche
Gilbert Babin,	Codirecteur
Claude Frasson,	Membre du jury

Mémoire accepté le: 9 mai 2003

Sommaire

La prolifération des systèmes incompatibles de commerce électronique impliquant différentes technologies de sécurité impose des choix difficiles à toutes les parties intéressées. Dans ce contexte, le but de cette recherche est de fournir la base nécessaire pour développer un aviseur de mécanismes de sécurité (*SecAdvise*), qui permettra d'intégrer les mécanismes de sécurité et le choix dynamique des divers mécanismes entre plusieurs parties souhaitant exécuter des transactions avec des risques mitigés ou réduits.

Un tel aviseur vise des buts multiples : surmonter les problèmes de compatibilité et d'interopérabilité, réduire les risques technologiques de sécurité et augmenter la confiance des utilisateurs dans les systèmes de commerce électronique.

Dans ce mémoire, nous avons commencé par identifier les risques, les services et les mécanismes de sécurité, et leur répartition dans le modèle OSI (*Open System Interconnection*). Nous avons aussi fait l'inventaire des systèmes de sécurité déjà existants. Ensuite, nous avons évalué ces systèmes, étudié l'impact de qualité de service de chaque couche sur les autres couches dans le modèle OSI et catégorisé ces systèmes afin de définir un aviseur préliminaire basé sur le modèle de confiance proposé par Robles et sur la répartition des mécanismes sur le modèle OSI.

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

Abstract

The proliferation of incompatible systems for electronic trade using various security technologies imposes difficult choices on all the concerned parties. In this context, the purpose of this research is to provide the necessary background to develop a security advisor for mechanisms (SecAdvise), which will make it possible to integrate security mechanisms and their dynamic selection in order for several parties to conduct business safely. Such an advisor aims multiple goals: overcoming compatibility and interoperability problems, reducing technological security risks, and increasing the confidence of the users in e-commerce systems.

In this thesis, we start by identifying the threats, the services, and the mechanisms of security, and their distribution in the OSI (Open System Interconnection) model. We also make an inventory of existing security systems. We then evaluate these systems, study the impact of their quality of service on the layers of OSI model, and categorize these systems to obtain a preliminary advisor based on the trust model of Robles and the distribution of the mechanisms on OSI model layers.

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

Table des matières

Liste des tableaux

Liste des figures

À mes très chers Elie, Josephine, Amal, Rola, Berthe et Amine

pour leur amour et leur soutien...

Remerciements

Mes plus grands remerciements reviennent à monsieur Peter Kropf, professeur à l'Université de Montréal, pour m'avoir donné l'occasion de faire partie de l'équipe du laboratoire de téléinformatique, ainsi que pour avoir supervisé cette recherche. Son souci du détail ainsi que ses encouragements m'ont beaucoup aidée tout au long de ce travail.

De même, un grand merci à Monsieur Gilbert Babin, mon codirecteur, professeur à HEC Montréal, pour sa grande disponibilité, sa persévérance, et pour m'avoir guidé durant cette recherche.

Que ce mémoire soit le modeste témoignage de ma reconnaissance et de mon admiration envers eux.

Je remercie vivement chacun des membres du jury d'avoir accepté d'être les juges de mon projet de maîtrise.

Mes remerciements vont aussi à mes très chers amis, qui étaient toujours disponibles durant les moments de détresse et de solitude. Merci beaucoup.

Enfin, je tiens à remercier mes parents et mes sœurs et frère qui m'ont toujours supportée, surtout dans les moments les moins faciles. Trouvez ici l'expression de ma profonde gratitude.

Chapitre 1. Introduction

1.1 Contexte du travail

L'Internet a connu ces dernières années un taux de croissance exceptionnel qu'aucun autre secteur de l'informatique ou des télécommunications n'a jamais atteint. L'interface World Wide Web avec laquelle un utilisateur peut naviguer entre les quelques milliers de serveurs qui constituent la toile d'araignée d'Internet crée de nombreuses opportunités pour les entreprises et présente un immense intérêt sur le plan commercial. D'ailleurs, l'Internet devient un moyen de plus en plus important pour le commerce électronique où les interactions complexes d'affaires impliquent des parties multiples, telles que les utilisateurs, les fournisseurs de services, les chaînes d'approvisionnement, les courtiers, les institutions financières ou organismes de réglementations et d'autres médiateurs et clients.

Clairement, toute transaction impliquant un transfert d'argent ou de fonds et employant des moyens électroniques doit être fortement sécurisée. Par exemple, il est risqué de confier son numéro de carte de crédit à un serveur. La résolution du problème de la sécurité de l'Internet conditionne donc l'essor du commerce électronique.

Plusieurs systèmes de sécurité ont été mis en application et sont opérationnels dans beaucoup d'applications de commerce électronique. Les mécanismes utilisés, les services de sécurité, les algorithmes cryptographiques, le montant d'argent impliqué dans une transaction, les parties concernées, etc., distinguent ces systèmes de sécurité.

1.2 Résultats attendus

Le foisonnement des systèmes de paiements électroniques et des systèmes de sécurité de commerce électronique, incompatibles entre eux, impose des choix difficiles à toutes les parties concernées. L'histoire a maintes fois démontré que l'essor du commerce exige un environnement stable et uniforme; or, même pour ce qui concerne un aspect simple du commerce électronique, par exemple les porte-monnaie, on ne compte pas moins de vingt systèmes commercialisés, tels que *E-cash*, *CyberCash*, *Mondex*, *Millicent*, *PAYCHIP*, *CyberCoin,* etc. [Sherif00], en Europe de l'Ouest seulement, ce qui prouve que le contexte est hautement instable. Dans ce contexte, le but de cette recherche est de fournir les bases nécessaires pour développer un aviseur de mécanismes de sécurité (*SecAdvise*), qui permettra d'intégrer les mécanismes de sécurité et de choisir dynamiquement divers mécanismes entre plusieurs parties souhaitant exécuter des transactions sans risque.

Un tel aviseur vise des buts multiples : surmonter des problèmes de compatibilité et d'interopérabilité, réduire des risques technologiques de sécurité et augmenter la confiance des utilisateurs dans les systèmes de commerce électronique.

1.3 Problématique et approche de recherche

Jusqu'ici, plusieurs initiatives, telles que SEMPER [Lacoste00], IOTP (*Internet Open Trading Protocol)* [Hassler01], et OBI (*Open Buying on the Internet*) [OBI99] ont essayé de faire converger les divers systèmes afin d'établir une architecture commune. Une autre approche propose un modèle de confiance pour des applications de commerce électronique [Robles01]. Ce modèle de confiance décrit une méthodologie pour définir des conditions de confiance et pour augmenter la protection et la confiance dans les systèmes de commerce électronique. Il suggère la définition d'un espace de problème de confiance TPS (*Trust Problem Space*). Ce TPS sera relié à une collection de mécanismes en corrélation, les unités de confiance TU (*Trust Units*), pour fournir des protections pour protéger des systèmes et des sous-systèmes, et pour augmenter la confiance dans ces systèmes ou ces sous-systèmes.

En outre, Vesna Hassler a identifié trois principales questions de sécurité [Hassler01]: risques de sécurité, mécanismes de sécurité et services de sécurité. Les attaques sur les systèmes peuvent être classifiées selon plusieurs types. Cette classification mène à une analyse complète des menaces les plus probables et des vulnérabilités des systèmes à ces menaces.

En nous basant sur l'analyse des risques, nous pouvons définir une politique de sécurité qui indique clairement ce qui doit être réparé. Les fonctions qui imposent la politique de sécurité, désignées sous le nom de services de sécurité, incluent l'authentification, le contrôle d'accès, la confidentialité, l'intégrité et la non-répudiation. Ces services sont mis en application par des mécanismes de sécurité, par exemple des algorithmes de chiffrage, des méthodes numériques de signature, des mécanismes d'échange d'authentification ou des mécanismes de contrôle d'accès. Ces mécanismes sont réalisés par des algorithmes cryptographiques et des protocoles de sécurité. Chaque service de sécurité mentionné ci-dessus peut être de différents types. Par exemple, un service d'authentification peut se fonder sur une authentification d'entité paire ou sur une authentification d'origine de données. Ces deux types emploient différents mécanismes de sécurité. Afin de mieux décrire les services de sécurité, nous définissons une matrice, qui est la combinaison des mécanismes de sécurité, des services de sécurité et du modèle de référence à sept couches d'OSI (*Open System Interconnection*) [ISOOSI94]. Cette matrice devrait permettre le choix d'un mécanisme donné afin de remplir une condition donnée de sécurité. Le modèle de référence OSI est employé pour réduire la complexité de la classification des différents mécanismes et services de sécurité, et facilite donc le processus de classification. Une fois que cette classification est atteinte, l'utilisation du modèle de Robles sera applicable [Robles01].

1.4 Structure du mémoire

Dans le chapitre 2, nous présentons les concepts et les mécanismes de sécurité de réseau nécessaires à la compréhension de la sécurité en général. Ce chapitre définit la terminologie utilisée pour décrire tous les services de sécurité requis afin d'assurer la sécurité des paiements électroniques, ainsi que prévenir les risques pouvant survenir sur les systèmes. Une description du modèle OSI sera aussi incluse dans ce chapitre.

Nous donnons dans le chapitre 3 quelques exemples des systèmes et mécanismes, et des services qu'ils fournissent pour les transactions de commerce électronique.

Le chapitre 4 fournit quelques architectures de sécurité existant dans le commerce électronique, ainsi qu'une comparaison entre ces architectures. On s'attaque en détail au modèle de confiance de Roble [Robles01], à SEMPER (*Secure Electronic Market Place for EuRope*) [Lacoste00], et IOTP (*Internet Open Trading Protocol*) [IOTP00].

Dans le chapitre 5, nous présentons la répartition des différents mécanismes de sécurité sur les couches du modèle OSI. Nous fournissons aussi l'architecture préliminaire de notre aviseur de sécurité, *SecAdvise*.

Dans le dernier chapitre, nous donnons la conclusion et identifions les travaux futurs pouvant découler de cette recherche.

L'annexe A contient une description détaillée du système de paiement SET, sur lequel l'aviseur *SecAdvise* sera évalué.

L'annexe B contient une liste non exhaustive des actifs à identifier dans l'analyse de risque.

L'annexe C présente un document de travail de l'analyse de risque.

Chapitre 2. État de l'art

2.1 Introduction

Dans ce chapitre, nous présentons la sécurité dans les réseaux. La terminologie employée est celle utilisée par l'ensemble des acteurs de la sécurité, qu'ils soient fournisseurs, utilisateurs ou concepteurs (laboratoires, organismes de normalisation). Nous définissons ainsi les principaux concepts de la sécurité.

Ensuite, nous décrivons succinctement les principales solutions apportées par les services (authentification, confidentialité, etc.) et les mécanismes de sécurité (chiffrement, signature électronique, etc.).

Enfin, nous présentons le modèle OSI avec ses sept couches ainsi que quelques exemples des protocoles au niveau de chaque couche.

2.2 Les menaces dans un réseau ouvert

Plusieurs types de menaces informatiques se rencontrent dans un réseau ouvert [Sherif00]. Les recommandations X.509 et X800 de l'UIT-T (Union internationale des télécommunications - Secteur de normalisation des télécommunications) signalent entre autres les dangers ou risques suivants :

- l'interception de l'identité d'un ou de plusieurs des intervenants par un tiers en vue d'un usage abusif;
- l'usurpation d'identité;
- la réexécution (*replay)* intégrale ou partielle d'une communication légitime antérieure après enregistrement;
- l'interception de données par un intrus ou un utilisateur non autorisé au moyen d'une observation clandestine des échanges pendant une communication ;

- la modification accidentelle ou intentionnelle du contenu des échanges par remplacement, insertion, suppression ou réorganisation de données d'utilisateur au cours d'une communication;
- la dénégation ou contestation d'un utilisateur d'avoir participé, partiellement ou entièrement, aux échanges d'une communication;
- le déni de service et l'impossibilité d'accès à des ressources habituellement mises à la disposition des utilisateurs autorisés à la suite d'un empêchement, d'une interruption de la communication ou de délais importants imposés à des opérations critiques;
- l'acheminement erroné d'un message prévu pour un usager vers un autre usager;
- l'analyse de trafic et l'examen des paramètres relatifs à une communication entre utilisateurs (c'est-à-dire absence ou présence, fréquence, sens, séquence, type, volume et autres).

L'objectif des services de sécurité est de minimiser les conséquences d'une telle erreur, sinon de la prévenir. Ainsi, il est clair que les objectifs de la sécurisation sont les suivants :

- interdire à un tiers non autorisé de lire ou de manipuler le contenu ou les séquences des messages échangés sans risquer d'être détecté. Plus particulièrement, ce tiers ne doit pas pouvoir rejouer d'anciens messages, remplacer des blocs d'informations ou mélanger les messages provenant d'échanges légitimes sans détection.
- entraver le truquage des pièces ou la génération de messages. Par exemple, des commerçants ou des centres de traitements peu scrupuleux ne doivent pas être capables de réutiliser les informations bancaires des clients pour générer des commandes frauduleuses ou se faire payer sans livrer les articles achetés. Réciproquement, les marchands doivent être protégés contre les révocations abusives de paiements ou les contestations malveillantes des commandes.
- satisfaire les conditions légales en vigueur pour valider les contrats et régler les litiges, notamment en matière de protection du consommateur et de la vie privée et des modalités d'exploitation des informations obtenues sur les clients pour des fins commerciales, des intervalles de révocation de paiements, etc.

- assurer l'accès aux services souscrits selon les contrats établis avec les fournisseurs.
- assurer le même niveau de service à tous les clients, quelle que soit leur localité géographique et ceci en dépit des variations climatologiques et atmosphériques (température, humidité, intempéries ou autres). Dans les climats où l'humidité et la température sont très variables, les infrastructures de traitement de l'information sont plus sensibles et risquent des dangers plus importants que celles placées dans des climats stables, d'où la nécessité de prendre en considération ces variations.

2.3 Services de sécurité

Les services de sécurité sont les propriétés que l'on souhaite obtenir du système de communication. L'ISO a défini des services de sécurité dans le document ISO7498. Nous ne présentons que les services mis en oeuvre pour assurer la sécurité de transactions commerciales électroniques.

2.3.1 Identification

Il s'agit de vérifier la relation entre des caractéristiques individuelles (par exemple, des mots de passe ou des clés de chiffrement) et les individus, afin de contrôler l'accès aux ressources du réseau ou aux services offerts. Une entité peut posséder plusieurs identificateurs distincts.

2.3.2 Authentification

Ce service permet d'authentifier les entités qui communiquent entre elles, préalablement à tout échange de données. Il a pour but de garantir l'identité des correspondants. On peut distinguer deux types :

- l'authentification de l'entité homologue qui assure que l'entité réceptrice qui est connectée est bien celle annoncée. Son principal objectif est la lutte contre le déguisement;
- l'authentification de l'origine qui assure que l'entité émettrice est bien celle prétendue.

2.3.3 Confidentialité des données

L'objectif de ce service est d'empêcher que les données soient compréhensibles par une entité tierce non autorisée, le plus souvent en état de fraude passive, c'est-à-dire en écoute de l'information sur le réseau.

On distingue :

- la confidentialité intégrale où l'ensemble des données transmises doit être protégé;
- la confidentialité d'un champ spécifique où la protection est assurée pour quelques données incluses dans une transmission.

2.3.4 Intégrité des données

Afin de prévenir contre les fraudes actives (brouillage, modification des données ou de l'identité, déguisement en émission ou en réception), ce service détecte les altérations partielles ou intégrales des données entre émetteur et récepteur.

2.3.5 Non-répudiation

On distingue deux types de non-répudiation:

- la non-répudiation à l'origine des données qui fournit au récepteur une preuve ou attestation empêchant l'émetteur de contester l'envoi ou le contenu d'un message effectivement reçu;
- la non-répudiation de la remise qui fournit à l'émetteur une preuve empêchant le récepteur de contester la réception ou le contenu d'un message effectivement remis.

2.3.6 Contrôle d'accès

Ce service assure que seules les entités autorisées peuvent accéder à des ressources protégées.

2.4 Mécanismes de sécurité

Ces mécanismes ont pour objet de réaliser les services de sécurité énumérés ci-dessus. Nous ne mentionnons que les mécanismes nécessaires et utiles pour la compréhension des différents services mis en oeuvre dans les chapitres suivants.

2.4.1 Chiffrement

Le chiffrement est l'opération qui consiste à transformer en tout ou en partie un texte dit clair en cryptogramme, message chiffré et protégé, grâce à une fonction intermédiaire paramétrable dite de cryptage. Si une ligne utilise des dispositifs de chiffrement, les données sont transmises sous forme brouillée, de manière à ce qu'elles ne puissent pas être reconstruites par un intrus.

Le mécanisme de chiffrement implique un mode de chiffrement voie par voie ou de bout en bout [Mel01], un couple de fonctions qui s'appliquent à des messages émis et reçus. L'ensemble repose sur un algorithme donné, un couple de clés associées et un mécanisme de distribution des clés.

A - Le chiffrement voie par voie dans le réseau

Il peut être réalisé au niveau de chacune des trois premières couches du modèle OSI (niveau physique, niveau liaison et niveau réseau). Ce mécanisme a l'avantage de libérer les couches supérieures et l'application de l'utilisateur des tâches de chiffrement puisque le service est fourni par l'infrastructure du réseau.

B - Le chiffrement de bout en bout

Ce mécanisme laisse en clair les informations de routage. Seules les données constituant l'information transmise sont chiffrées. Dans un réseau multinoeuds, le message traverse plusieurs noeuds et garde le même chiffrement depuis son émetteur jusqu'à son destinataire final.

2.4.1.1 Principes du chiffrement

Le mécanisme de chiffrement consiste à émettre un message X sous une forme secrète au moyen d'une clé K.

L'émetteur dispose d'un algorithme (ou fonction mathématique) E qui est largement connu et disponible, mais c'est la clé K qui demeure secrète et fournit la sécurité requise. E associe $E(K,X)$ à X et K. Le récepteur reçoit $E(K,X)$ (message chiffré émis) et le déchiffre au moyen de sa clé K' avec sa fonction D, qui associe X à $E(K,X)$ et K'.

On a alors la transformation $D(K', E(K,X)) = X$

Les fonctions E et D peuvent être secrètes ou publiques. Il en est de même pour les clés K et K'. L'existence d'un déchiffrement tient à la définition de l'algorithme donnant E et D et de la méthode produisant et répartissant les clés K et K'.

Les systèmes à clé secrète (on parle de chiffrement symétrique) forcent l'émetteur et le récepteur à utiliser la même clé secrète ($K=K'$). Les méthodes basées sur ces systèmes sont simples et performantes, mais le problème réside dans la communication des clés. En effet, si la clé est interceptée lors de sa communication au récepteur, tout message chiffré pourra être décodé par les pirates, à l'insu du destinataire.

Les systèmes à clé publique (on parle aussi de chiffrement asymétrique) ont en fait deux clés: la clé de chiffrement K (publique) et la clé de déchiffrement K' (secrète).

L'avantage de cette technique est que l'échange des clés est très sécuritaire puisque l'échange d'une clé publique représente beaucoup moins de risques que celle de la clé privée. Cette dernière n'est jamais partagée. De plus, contrairement au chiffrement symétrique, la non-répudiation est possible [Mel01].

2.4.2 Mécanismes associés aux services de sécurité

2.4.2.1 L'échange d'authentification

Il est différent suivant le niveau de confiance que les entités accordent au réseau et à son environnement. L'authentification des entités homologues peut se faire par:

- les mots de passe;
- lorsque les moyens de communication ne sont pas sûrs, il faut ajouter des procédures de chiffrement aux mots de passe.

2.4.2.2 Confidentialité

Le mécanisme qui permet d'obtenir ce service est généralement le chiffrement des données concernées à l'aide d'un algorithme cryptographique. Dans le cadre du chiffrement d'échanges réseau (chiffrement voie par voie), on utilise toujours, pour des raisons de performance, des algorithmes de chiffrement symétriques.

Si seules les données transportées sont chiffrées (chiffrement de bout en bout), un espion peut tout de même observer des caractéristiques extérieures au trafic transitant sur un réseau afin de tenter d'en tirer des informations : fréquence des transmissions, identités des tiers communicants, quantités de données transférées. Associées à des informations de nature différente (date de rendez-vous, actualité, etc.) ces éléments peuvent permettre aux adversaires de faire des déductions intéressantes. On parle de *protection contre l'analyse du trafic* lorsqu'on tente d'empêcher l'analyse du trafic en cachant les adresses source et destination, la taille des paquets, la fréquence des échanges ou autres.

2.4.2.3 Authenticité (intégrité et authentification de l'origine des données)

Lorsque l'on communique avec une autre personne au travers d'un canal peu sûr, on aimerait que le destinataire puisse s'assurer que le message émane bien de l'auteur auquel il est attribué et qu'il n'a pas été altéré pendant le transfert. Les services correspondant sont l'authentification de l'origine des données et l'intégrité.

Les fonctions de hachage à sens unique permettent d'assurer l'intégrité des données : appliquée à un ensemble de données, une telle fonction génère un bloc de taille plus petite appelée empreinte ou condensât. Toute modification des données entraîne une modification du condensât, et il est très difficile (entendre par là : dans le domaine de l'impossible) de générer un message ayant le même condensât que l'original.

Si l'on transfère le condensât sur un canal de communication non sûr, un intercepteur peut modifier les données puis recalculer le condensât. Il convient donc de trouver une

méthode pour s'assurer que seul l'expéditeur est capable de calculer le condensât. Pour cela, on peut utiliser, par exemple, une fonction de hachage à sens unique qui fonctionne de plus avec une clé secrète ou privée. On remarquera que, ce faisant, on fournit également l'authentification de l'origine des données. Inversement, si on désire fournir l'authentification de l'origine des données et que l'on utilise pour cela un moyen qui ne garantit pas l'intégrité des données authentifiées, un intrus peut modifier le message et donc faire accepter comme authentifiées les données qu'il a choisies. C'est pourquoi intégrité et authentification de l'origine des données sont généralement fournies conjointement par un même mécanisme. Le terme « authenticité » désigne l'intégrité jointe à l'authentification des données. Par abus de langage, le terme « authentification » est également couramment utilisé pour désigner en fait authentification et intégrité.

Les deux mécanismes permettant d'assurer l'authenticité des données transmises sont le scellement et la signature.

Le *scellement* consiste à adjoindre au message code d'authentification de message *(Message Authentication Code, MAC)*[1], qui est le résultat d'une fonction de hachage à sens unique à clé secrète. Le paraphe dépend à la fois des données et de la clé; il n'est donc calculable que par les personnes connaissant la clé.

La *signature numérique* ou le sceau[2] assure également l'authenticité des données et fournit en plus la non-répudiation : l'émetteur ne peut pas nier avoir émis un message qu'il a signé. Ce dernier point différencie la signature des codes d'authentification de message, et a pour conséquence que la plupart des algorithmes de signature utilisent la cryptographie à clé publique. Dans le cadre de la protection d'échanges réseau, on utilise, pour des raisons de performance, un mécanisme de scellement (cryptographie symétrique).

---

[1] Dans le présent mémoire, nous trouverons plusieurs définitions de MAC. Dans le présent contexte, MAC est un *Message Authentication Code* ou paraphe.

[2] La signature numérique d'un texte obtenue en chiffrant le condensât du texte en question à l'aide de la clé privée du signataire [Sherif00].

De plus amples informations sur les détails des mécanismes associés aux services de sécurité seront disponibles dans [Mel01], [Sherif00] et [Pfleeger02].

2.4.3 Certificats numériques

Il est essentiel que l'échange des clés publiques initial se déroule dans un contexte de confiance, d'où l'existence de certificats numériques. Un certificat numérique (*digital certificate*) est un message signé numériquement avec la clé privée d'une partie tierce de confiance, autorité de certification ou CA (*Cerificate Authority*)[3] qui confirme l'appartenance d'une clé publique spécifique à une personne ou entité donnée dotée d'un nom et d'un ensemble d'attributs tels que l'identité du propriétaire de la clé, la clé publique et l'usage de la clé ainsi que la période de la validité du certificat, l'algorithme de cryptage utilisé, le numéro de série et autres. Si cet échange a lieu dans un environnement non sécurisé, un individu malveillant pourrait facilement usurper l'identité d'une des parties communicantes.

En transposant la notion de signature et de notaire dans le monde électronique, une garantie supplémentaire peut être apportée par la notarisation: les entités font confiance à un tiers qui assure l'intégrité, l'origine, la date et la destination des données. Le processus sous-entend que ce tiers doit acquérir les informations par des voies de communications très protégées. Ainsi, chaque message émis est envoyé au notaire *N* qui effectuera un certain nombre d'authentifications afin de s'assurer de l'origine et du contenu; le message sera alors daté et enregistré par *N* puis envoyé avec un certificat au récepteur.

2.4.3.1 PKI (*Public Key Infrastructure*)

PKI (*Public Key Infrastructure*) ou IGC (Infrastructure de gestion de clés) est un ensemble d'outils (logiciels et matériels) qui gèrent les clés cryptographiques et les certificats. L'IGC permet les transactions sécurisées et les échanges d'informations entre deux parties en garantissant la confidentialité, l'intégrité et l'authentification.

---

[3] Un organisme qui génère les certificats des différents utilisateurs. C'est un passage obligé pour la mise en place d'un système sécurisé en commerce électronique

On y retrouve :

- la gestion des clés (création, distribution, entreposage, etc.);
- association de la clé publique et de l'entité (certificat);
- recouvrement de clé.

2.4.4 Exemples d'algorithmes de chiffrement

2.4.4.1 Chiffrement symétrique

DES (*Data Encryption Standard*), mis au point dans les laboratoires d'IBM en 1977 [Mel], a été normalisé au sein de l'ISO et proposé sous le nom de *Data Encipherment Algorithm*. Il a été retenu par le gouvernement américain pour le cryptage des informations non secrètes. C'est un algorithme très répandu dans le monde industriel et bancaire. Il est notamment implémenté pour le contrôle des codes liés aux cartes bancaires (cartes à pistes et cartes à microcircuits).

Cet algorithme repose sur l'utilisation d'une clé unique de longueur relativement petite. En effet, elle possède 64 bits dont 56 bits sont utilisés pour tous les blocs de données de 64 bits. Les 8 bits restants sont des bits de parité. Par conséquent, le nombre de clés possibles est d'environ 72 millions de milliards (2^{56}). Le standard DES possède donc un haut niveau de sécurité. De plus, cet algorithme est très rapide, mais sa difficulté réside dans la communication des clés de cryptage et de décryptage.

Longtemps réputé incassable, Le DES a finalement perdu ce titre en raison de la puissance des ordinateurs actuels. Le standard 3DES ou (*Triple DES*) a donc été désigné pour lui succéder. Avec cet algorithme, les données sont cryptées trois fois à l'aide de différentes clés ce qui permet d'augmenter le temps nécessaire pour briser l'algorithme. Néanmoins, le 3DES sera bientôt obsolète également en raison de l'augmentation rapide de la puissance des ordinateurs. C'est pourquoi il est maintenant combiné au standard AES (*Advanced Encryption Standard*). Ce standard utilise l'algorithme de Rijendal et est aussi fort que le 3DES, mais beaucoup plus rapide. L'AES est un algorithme relativement nouveau.

2.4.4.2 Chiffrement asymétrique

2.4.4.2.1 L'algorithme RSA

L'algorithme RSA, du nom de ses trois concepteurs américains R. Rivest, A. Shamir et L. Adleman, a été proposé en 1978 [Mel01]. RSA est un exemple type d'algorithme asymétrique. C'est une méthode fondée sur la théorie des nombres et permettant d'utiliser deux paires de clés : publiques et privées.

La sécurité de cette technique réside dans le choix de très grands nombres dont la décomposition en facteurs premiers est difficile.

Soient deux grands nombres premiers p et q et soit leur produit $n = pq$, choisissons un nombre e inférieur à n, à partir de là, on obtient:

- la clé publique, donnée par le couple (e, n), tel que e soit premier avec $(p-1)(q-1)$
- la clé secrète (d, n), obtenue en cherchant le nombre d tel que $ed = 1 \bmod (p-1)(q-1)$
- pour chiffrer un bloc P en clair, on génère : $P^e \pmod n = C$ codée
- pour déchiffrer C codée, on récupère: $C^d \pmod n = P$ en clair, car $C^d \pmod n = (P^e)^d \pmod n = P^{ed} \pmod n = P \pmod n$

En fait, RSA est basé sur la difficulté de factoriser n. En effet, celui qui arrive à factoriser n (retrouver p et q à partir de n) peut retrouver facilement la clé secrète e connaissant seulement la clé publique d. La factorisation est un problème très difficile si p et q sont très grand. Dans la pratique on utilisera n et e ayant au moins 1000 bits.

RSA est le seul système cryptographique généralisé qui permette à ses clés publiques et privées de chiffrer des messages. Les calculs qui sous-tendent le système RSA sécurisent le chiffrement de la clé publique et privée. Le système RSA apporte donc la confidentialité (chiffrement à l'aide d'une clé publique et déchiffrement à l'aide d'une clé privée) et la signature numérique (chiffrement à l'aide d'une clé privée et déchiffrement à l'aide d'une clé publique). Presque toutes les autres méthodes cryptographiques gèrent l'une ou l'autre, mais pas les deux.

2.5 Modèle OSI de sécurisation cryptographique

2.5.1 Le Modèle de Référence OSI

En 1983 [Tanenbaum96], l'organisme de normalisation ISO (*International Organization for Standardization*), basé en Suisse, a développé un modèle de référence pour permettre de normaliser les méthodes d'échange entre deux systèmes et pour que les réseaux puissent se développer à l'échelle mondiale en dehors du cercle fermé de certaines entreprises et institutions. Ce modèle est dénommé le modèle OSI (*Open Systems Interconnection*) et comporte sept couches superposées de protocoles [ISOOSI94].

Cette décomposition en couches a été créée pour simplifier considérablement la compréhension globale du système et pour faciliter sa mise en œuvre. On doit pouvoir remplacer une couche par une autre couche de même niveau, sans avoir à changer les autres niveaux. Les interfaces entre couches doivent être respectées pour sauvegarder la simplicité de l'édifice.

Les quatre premières couches sont les couches réseaux. Elles transportent physiquement les données d'une application vers une autre, sans erreur. Les trois autres couches sont chargées de formater les informations et de fournir des voies d'accès multiples à la même application.

Chaque couche a un rôle bien particulier et communique sur requête (sur demande) de la couche supérieure en utilisant des services de la couche inférieure (sauf pour la couche physique 1).

Les données transférées par les services sont des SDU (*Service Data Unit*). L'échange d'information suit un protocole avec des couches distantes de mêmes niveaux. Les données transférées par ce protocole sont des PDU (*Protocole Data Unit*).

Notez que le modèle OSI n'est pas en soi une architecture de réseau parce qu'il ne spécifie pas réellement les protocoles utilisés dans chaque couche. Il décrit simplement ce que chaque couche doit faire. Cependant, l'ISO a également produit des normes pour toutes les couches, quoiqu'elles ne fassent pas strictement partie du modèle.

Voici les différentes couches (tableau 2.1):

Hôte A		**Hôte B**
Application	7	Application
Présentation	6	Présentation
Session	5	Session
Transport	4	Transport
Network (Réseau)	3	Network (Réseau)
Data Link (liaison de données)	2	Data Link (liaison de données)
Physical (Physique)	1	Physical (Physique)
Support de communication entre Hôte A et Hôte B		

Tableau 2.1. Les sept couches OSI

Nous décrirons brièvement chaque couche en partant de la couche 1, en donnant des exemples de protocoles sur chacune des sept couches.

2.5.1.1 La couche Physique (C1)

La couche physique est la couche au niveau de laquelle sont définies les propriétés électriques, mécaniques et fonctionnelles des interfaces (niveaux des signaux, débits, structures, etc.). La couche physique spécifie les éléments suivants :

- La vitesse de transfert des données ;
- Le type de câble utilisé (coaxial, UTP (*Unshield Twisted Pair*), fibre optique, etc.) ;
- Le niveau du signal électronique ou lumineux, permettant de représenter par un 1 ou un 0.

Les protocoles qui interviennent à ce niveau sont par exemple DWDM (*Dense Wavelength Division Multiplexing*) pour la fibre optique ou les normes RS- ou 10baseT en entrée/sortie d'équipements comme les cartes réseaux.

2.5.1.2 La couche Liaison (C2)

La couche liaison définit les moyens d'assurer une transmission ordonnée et sans erreur entre deux nœuds du réseau. Les protocoles qui fonctionnent à ce niveau délivrent des données de carte à carte.

Des exemples WAN (*Wide Area Network*) de ces types de protocoles incluent :

- HDLC (*High Level Datalink Control*), utilisé par des réseaux X.25 ;
- ATM (*Asynchronous Transfer Mode*);
- *Frame Relay* ou X.25.

Dans les réseaux LAN (*Local Area Network*), il existe plusieurs protocoles. Les plus importants sont ceux qui décrivent les méthodes d'accès aux câbles, les formats de trame et l'adressage physique. Ces protocoles sont les suivants :

- *Ethernet;*
- *Token Bus;*
- *Token Ring*.

2.5.1.3 La couche Réseau (C3)

La couche réseau définit les fonctions de routage, de multiplexage des paquets, de contrôle du flux et de supervision du réseau. Les protocoles suivants sont actuellement utilisés pour cette couche :

- IPX (*Internetwork Packet Exchange*) de Novell;
- IP (*Internet Protocol*).

À ce niveau interviennent aussi les protocoles de routage tels :

- RIP (*Routing Information protocol*);
- BGP (*Border Gateway Protocol*).

2.5.1.4 La couche Transport (C4)

La couche transport est responsable du transport fiable du trafic sur le circuit reliant les deux extrémités du réseau ainsi que de l'assemblage et du désassemblage des messages. La communication est de bout en bout (application). Les protocoles suivants sont actuellement utilisés pour cette couche :

- TCP (*Transport Control Protocol*);
- UDP (*User Datagram Protocol*);

- SPX (*Sequenced Packet Exchange*);
- NCP (*Netware Core Protocol*) chez Novell.

2.5.1.5 La couche Session (C5)

La couche session est responsable du dialogue entre les processus des deux extrémités du réseau.

2.5.1.6 La couche Présentation (C6)

La couche présentation se charge de régler la différence de syntaxe entre les multiples représentations des données à l'aide d'un format normalisé.

Il existe de multiples manières de coder les informations en informatique suivant le matériel et les logiciels utilisés. Par exemple:

- Plusieurs codes existent pour coder les caractères (ASCII, EBCDIC, etc.) ;
- Les nombres peuvent être codés sur un nombre d'octets différent ;
- Les octets de poids fort et de poids faible peuvent être répartis différemment, autrement dit, un nombre peut être lu de gauche à droite ou de droite à gauche ;
- Etc.

2.5.1.7 La couche Application (C7)

La couche application a le rôle d'assurer la coopération des processus applicatifs des deux extrémités du réseau afin de traiter l'information de la manière désirée. Les protocoles suivants sont quelques exemples des protocoles de la couche application:

- HTTP (*HiperText Transfer Protocol*);
- MIME (*Multi-Purpose Internet Mail Extensions*);
- TELNET;
- FTP (*File Transfer Protocol*);
- SMTP (*Simple Mail Transfer Protocol*).

2.5.2 Répartition des services de sécurité

Les services de sécurité peuvent se faire sur une ou plusieurs couches du modèle OSI [Rolin95]. Le tableau 2.2 illustre leur emplacement au niveau de chaque couche.

					Application
				Présentation	
				Session	
			Transport		Non-répudiation de remise
		Réseau			Non-répudiation de l'origine
	Liaison				Confidentialité sélective des champs
Physique					Intégrité sélective des champs (mode connexion)
					Intégrité sélective des champs (mode non-connexion)
			Intégrité de la connexion avec restauration		Intégrité de la connexion avec restauration
		Authentification des entités paires	Authentification des entités paires		Authentification des entités paires
		Authentification de l'origine	Authentification de l'origine		Authentification de l'origine
		Contrôle d'accès	Contrôle d'accès		Contrôle d'accès
		Intégrité de la connexion sans restauration	Intégrité de la connexion sans restauration		Intégrité de la connexion sans restauration
		Intégrité sans connexion	Intégrité sans connexion		Intégrité sans connexion
	Confidentialité sans connexion	Confidentialité sans connexion	Confidentialité sans connexion		Confidentialité sans connexion
Confidentialité avec connexion	Confidentialité avec connexion	Confidentialité avec connexion	Confidentialité avec connexion		Confidentialité avec connexion
Confidentialité du flux de données		Confidentialité du flux de données			Confidentialité du flux de données

Tableau 2.2. Placement des services de sécurité dans le modèle de référence OSI [Hassler01]

Le choix de la couche dépend des critères suivants :

1. Si la protection de tous les flux doit être assurée de la même manière, l'intervention a lieu au niveau de la couche physique ou de la couche liaison. La protection à ces niveaux est particulièrement importante dans le cas de la transmission sans fil telle que les cellulaires IEEE 802.11, etc.). La confidentialité est le seul service de sécurité cryptographique prévu au niveau de ces deux couches. La protection sur la couche physique concerne tout le flux, non seulement les données de l'utilisateur, mais aussi les informations relatives à l'administration du réseau : alarmes, synchronisation, actualisation des tables de routage, etc. La protection se fait par le chiffrement des données ou par tout autre moyen (évasion de fréquence, étalement de spectre ou autres). L'inconvénient de la protection à ce niveau est qu'une attaque réussie déstabilise tout l'édifice de sécurité, car la même clé est utilisée pour sécuriser toutes les transmissions. Le *Link Encryption protocol* et le *MAC* (*Message Access Control*) sont deux protocoles de sécurité pour la couche liaison.
2. Pour une protection sélective mais globale de toutes les communications associées à un sous-réseau particulier d'un système à un autre, le chiffrement sera effectué au niveau de la couche réseau. IPSEC (*Internet Protocol Security*) est un protocole de sécurité de cette couche [Doraswamy99].
3. Pour assurer une protection avec restauration en cas de panne ou si la couche réseau n'est pas suffisamment fiable, c'est la couche transport qui fournit de bout en bout les services de sécurité suivants : l'authentification par mot de passe ou authentification simple, l'authentification par signatures ou certificats, dite authentification poussée, le contrôle d'accès, la confidentialité et l'intégrité. TLS (*Transport Layer Security*) est un protocole de la couche transport.
4. Si un niveau plus fin de protection est recherché ou si le service de non-répudiation doit être assuré, le chiffrement se fait au niveau de l'application, C'est à ce niveau qu'agissent la majorité des protocoles de sécurisation du commerce électronique. Notons qu'aucun service n'est prévu au niveau de la couche session et présentation. En revanche, les services offerts dans la couche application assurent principalement la confidentialité, l'intégrité et la non-répudiation avec preuve de l'origine ou de la remise. Cette confidentialité et cette

intégrité peuvent être sélectives par champ de données, mais elles peuvent s'appliquer aussi à tout le flux de données.

2.6 Conclusion

En fonction des services de sécurité et des mécanismes de sécurité, nous pouvons en déduire les points suivants :

- Une des solutions pour résoudre le problème lié à l'authentification des parties d'un échange est l'utilisation des algorithmes de chiffrement à clé publique qui permettent de garantir l'identité et l'authenticité des deux interlocuteurs d'un échange. Un message chiffré par la clé privée de l'émetteur ne peut être déchiffré qu'avec la clé publique de cet émetteur, dont dispose le récepteur; un message chiffré avec la clé publique du destinataire ne peut être déchiffré que par celui-ci, à l'aide de sa clé privée.
- Une des solutions pour assurer l'authenticité des messages d'une transaction de commerce électronique peut être l'utilisation des mêmes algorithmes à clé publique qui permettent, d'une part, de signer un acte de manière irréfutable, et d'autre part (grâce à un résumé numérique du message, lui-même signé) de contrôler l'intégrité du fichier.

Ces deux solutions mentionnées ne sont possibles que si les deux interlocuteurs font parties de la même infrastructure de gestion de clé (IGC ou *PKI Public Key Infrastructure*). Les deux partenaires devraient faire confiance à la même partie tierce pour pouvoir effectuer une transaction utilisant un algorithme à clé publique. Ce qui limite la sélection des mécanismes de sécurité à un espace auquel les deux partenaires font confiance.

De plus, les services de sécurité peuvent se faire sur une ou plusieurs couches du modèle OSI, le choix de la couche et l'emplacement des services dépendent des critères que nous étudierons dans les chapitres qui suivent.

Le chapitre suivant nous présente quelques systèmes de sécurité, SET et SSL, en identifiant les services de sécurité qu'ils offrent et les participants aux transactions de ces systèmes.

Chapitre 3. Paiements électroniques sur Internet

3.1 Introduction

Nous constatons que les solutions technologiques se multiplient pour proposer des échanges sécurisés sur Internet. Il existe des groupements industriels qui travaillent pour concevoir un standard pour les paiements en ligne. Certaines sociétés offrent déjà des services proposant des transactions sécurisées.

Le but de ce chapitre est de présenter plusieurs modèles de systèmes de paiements sécurisés, les différentes solutions proposées par ces systèmes pour payer un produit ou un service sur Internet, ainsi que les acteurs participant au développement du paiement électronique et les services de sécurité offerts par ces systèmes.

3.2 Modèles de paiements en commerce électronique

Un critère de distinction entre les différents systèmes de paiements serait de déterminer si la communication entre l'initiateur et le receveur du paiement est *directe* ou *indirecte*. Dans le dernier cas, le paiement est initié par un participant et n'implique que l'initiateur et la ou les banques. L'autre participant se voit notifier par sa banque que la transaction a été complétée.

Il existe un grand nombre de systèmes de paiements: Ecash, Netcash, CAFE, et Mondex sont des exemples orientés espèces (*Cash-like*) tels que les cartes à puce préchargées de monnaie légale, les systèmes de porte-monnaie électronique, etc. [Sherif00]. SET, iKP et CyberCash sont des exemples orientés comptes (*account-based*) tels que les chèques virtuels, les avis de prélèvement et les virements (transferts électroniques de fonds) [SET02].

Parfois les transactions de commerce électronique se contentent des mécanismes de sécurité offerts au nivaux de communication, c'est-à-dire au niveau réseautique. SSL et TLS sont deux exemples de ces mécanismes de sécurité.

Nous étudierons par la suite deux systèmes, SSL et SET, afin de mieux comprendre les interactions dans une transaction entre les différents participants.

3.3 Sécurisation des paiements avec SSL

Le protocole SSL (*Secure Socket Layer*) est un protocole généraliste de sécurisation des échanges, actuellement très utilisé dans les applications du commerce électronique. SSL est intégré dans les navigateurs pour assurer la sécurité des échanges entre un client et un serveur sur les réseaux ouverts.

Dans cette section, nous décrirons l'architecture ainsi que les services offerts par SSL.

3.2.1 Architecture

SSL est employé pour sécuriser tous les échanges entre un client et un serveur d'une manière transparente. Aussi a-t-il dépassé le protocole S-HTTP (*Secure HTTP*) qui considère seulement les échanges régis par le protocole HTTP (*Hyper Text Transfer Protocol*). En revanche, le protocole SET (*Secure Electronic Transaction*), développé par VISA et Mastercard et décrit par la suite, concerne exclusivement les transactions par carte bancaire.

SSL se situe entre les couches d'application et de transport. Par rapport au modèle de référence OSI, SSL est en quelque sorte un protocole de session.

La figure 3.1 montre la relation entre SSL et les différents protocoles d'application de l'Internet. SSL opère au-dessus du protocole de transport TCP et non pas au-dessus du protocole UDP (*User Datagram ptotocol*), car ce dernier n'offre pas un moyen de transport fiable. Les interruptions de flux que causent les pertes de paquets IP seraient interprétées comme des brèches dans le système de sécurité, forçant la coupure de la communication.

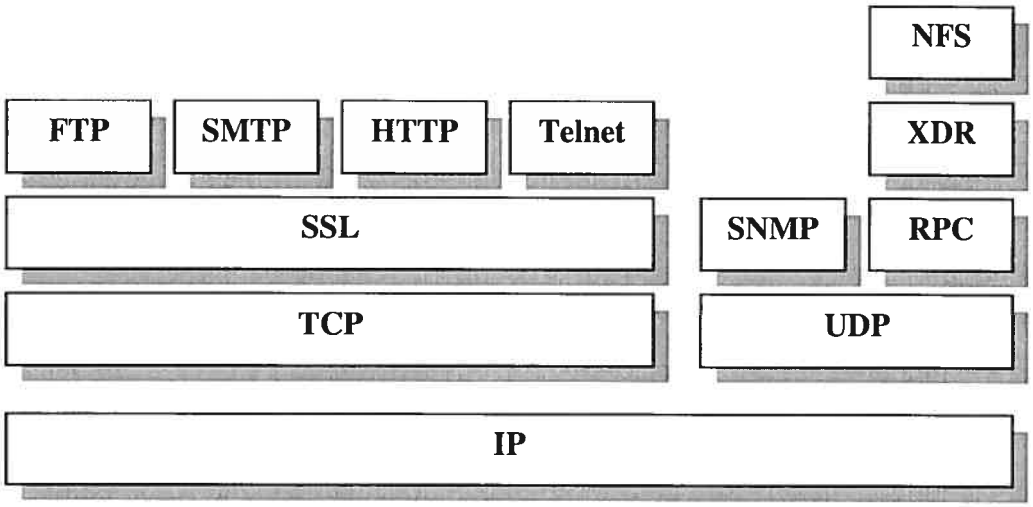

Figure 3.1. Position du protocole SSL au sein de la pile TCP/IP

3.3.1 Les services de sécurité de SSL

SSL fournit trois services de sécurité : l'authentification, l'intégrité et la confidentialité. À l'aide d'une signature numérique, il est possible de présenter les éléments nécessaires pour assurer un service de non-répudiation.

SSL définit le cadre dans lequel sont utilisés les algorithmes de chiffrement et de hachage entre les deux parties. Cette structure flexible permet d'intégrer de nouveaux algorithmes au fur et à mesure de leur adoption par les usagers.

3.3.1.1 L'authentification

L'authentification a lieu à l'établissement de la session et avant la première transmission de données. Ce service, qui était facultatif dans la version 2.0, est à présent obligatoire pour le serveur dans la version 3.0 [Freier96]. Ce choix encourage l'usage de SSL tout en faisant l'économie d'une infrastructure complexe de gestion de clés pour les applications orientées vers le grand public. Cependant, le serveur peut exiger du client qu'il s'authentifie et peut même lui refuser l'établissement de la session en l'absence de certificat.

L'échange de clés durant la phase d'authentification peut se faire avec un des algorithmes suivants [Freier96]: RSA (Rivest Shamir Adelman), Diffie-Hellman et l'algorithme confidentiel que la NSA (*National Security Agency*) des États-Unis a développé pour les applications sur carte PCNCIA dite «Fortezza» [NSA94].

3.3.1.2 La confidentialité

La confidentialité des messages s'appuie sur des algorithmes de chiffrement symétrique avec une clé de longueur 128 bits ou de 40 bits. Le même algorithme de cryptographie est utilisé par les deux parties, mais chacune se sert de sa propre clé secrète, qu'elle a partagée avec l'autre partie.

On nomme ces clés *client_write_key* (côté client) et *server_write_key* (côté serveur). Les algorithmes que l'on peut exploiter sont : DES, DES40 (le même algorithme que DES mais avec une clé limitée à 40 bits), triple DES, RC2, RC4 avec une clé de 128 bits ou de 40 bits, IDEA et l'algorithme SKIPJACK de Fortezza.

3.3.1.3 L'intégrité

L'intégrité des données est assurée par l'application de fonctions de hachage selon la procédure HMAC, ce qui confère une meilleure protection contre les attaques [Bellare96].

Les fonctions de hachage utilisées peuvent être soit SHA, soit MD5. Le condensât est traité par une série d'opérations qui font appel à une clé secrète pour donner ce que SSL nomme un code d'authentification de message MAC (*Message Authentication Code*). Cette opération sert également à l'authentification, dans la mesure où les secrets utilisés pour le chiffrement du condensât sont uniquement des deux parties.

3.3.2 Les sous-protocoles de SSL

Le protocole SSL se compose de quatre sous-protocoles :

1. *Handshake,* qui est chargé de l'authentification des parties en communication, de la négociation des algorithmes de chiffrement et de hachage, ainsi que de l'échange d'un secret, le *PreMasterSecret* ;

2. *Record,* qui met en œuvre les paramètres de sécurité négociés pour protéger les données d'application ainsi que les messages en provenance des protocoles *Handshake*, *ChangeCipherSpec* (CCS) et *Alert* ;
3. *ChangeCipherSpec,* qui a pour fonction de signaler à la couche *Record* toute modification des paramètres de sécurité ;
4. *Alert,* qui est chargé de signaler les erreurs rencontrées pendant la vérification des messages ainsi que toute incompatibilité qui pourrait survenir pendant le *Handshake*.

La figure 3.2 illustre l'agencement de ces différents éléments. On voit que le protocole *Record* se place au-dessus de la couche transport, tandis que les trois autres protocoles se situent entre l'application et la couche *Record*.

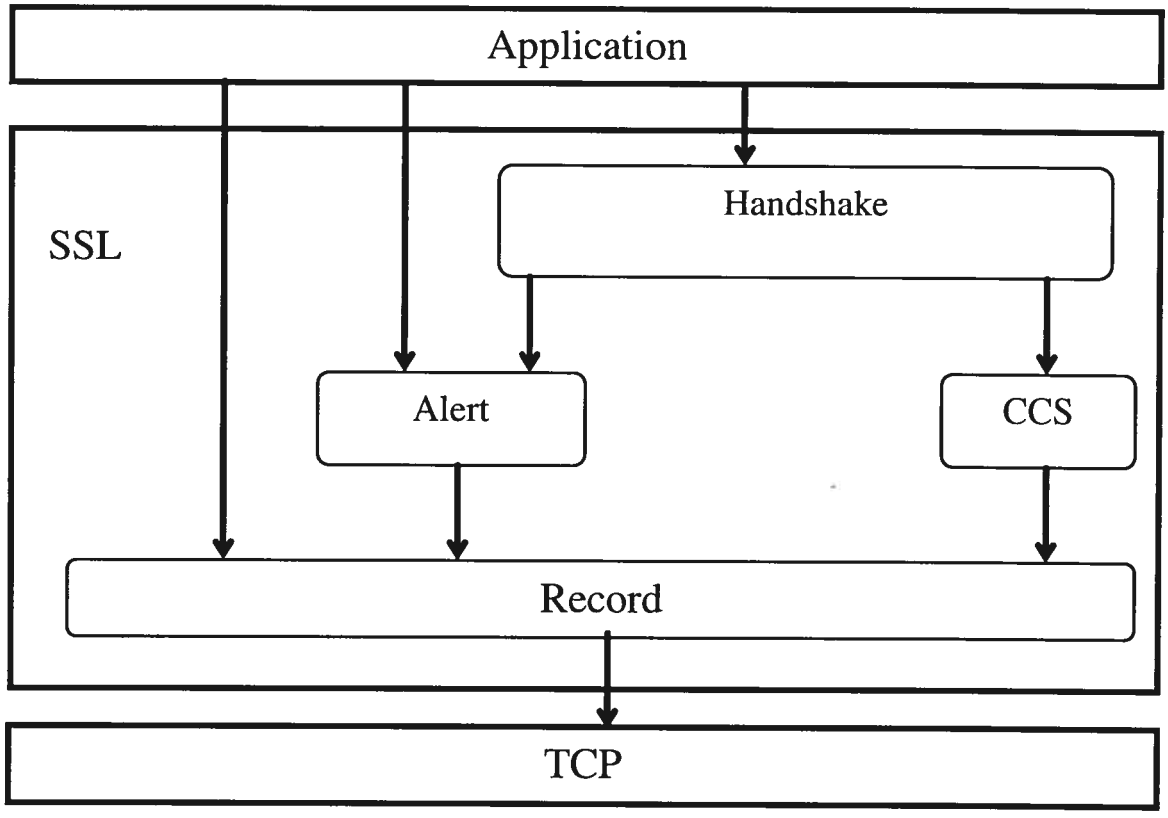

Figure 3.2. Empilement des sous-couches protocolaires de SSL

3.3.3 Déroulement des échanges SSL

Les échanges définis par le protocole SSL se déroulent en deux temps :

1. durant la phase préliminaire ont lieu l'identification des parties, la négociation des attributs cryptographiques, la génération et le partage des clés ;

2. durant les échanges de données, la sécurisation s'opère à partir des algorithmes et des paramètres secrets négociés durant la phase préliminaire.

À tout moment, il est possible de signaler une intrusion ou une erreur d'opération.

SSL reprend, en l'adaptant au nouveau contexte de sécurité, la notion de session des applications TCP/IP. Chaque fois qu'un client se connecte à un serveur, il déclenche une nouvelle session SSL. Si le client se connecte à un autre serveur, il engage une nouvelle session, sans interrompre la session en cours. S'il revient par la suite au premier serveur et souhaite conserver les précédents choix cryptographiques, il demeurera au premier serveur afin de reprendre une ancienne session plutôt que d'en commencer une nouvelle. Ainsi, selon SSL, une session est une association entre deux entités ayant en commun un certain nombre de paramètres et attributs cryptographiques. Pour limiter le risque d'attaque par interception de messages, SSL suggère de limiter la durée d'une session à 24 heures au maximum, mais la durée exacte reste à la discrétion du serveur. La reprise d'une session interrompue est seulement possible si la procédure de suspension a été suivie scrupuleusement.

Une session peut contenir plusieurs connexions contrôlées par l'application. Grâce à la notion de connexion SSL, une application est en mesure de « rafraîchir » (modifier) certains attributs de sécurité (tels que les clés de chiffrement) sans remettre en cause tous les attributs déjà négociés en début de session.

De plus amples informations sur les détails des échanges SSL seront disponibles dans [Sherif00].

3.4 Sécurisation des télépaiements avec SET

SET (*Secure Electronic Transaction*) est un protocole de sécurisation des transactions par carte bancaire effectuées sur les réseaux ouverts, comme l'Internet. Il a été parrainé par VISA et Mastercard avec la collaboration des principaux acteurs du monde informatique tels IBM, GTE, Microsoft, Terisa systems et Verisign [SET02]. Le but est de développer l'usage des cartes bancaires pour les paiements en ligne.

SET opère au niveau de l'application indépendamment de la couche de transport, ce qui le distingue de SSL. En pratique, il est envisagé d'utiliser SET pour sécuriser les

transports conformes au protocole TCP. SET porte uniquement sur l'acte de paiement, excluant ainsi la recherche et la sélection des produits.

Dans une transaction SET, le porteur de la carte effectue son paiement sans insérer la carte dans un quelconque lecteur, mais en présentant un certificat que lui a déjà délivré une autorité certifiante. Ce certificat est enregistré sur le disque dur d'un micro-ordinateur ou sur une disquette et permet d'authentifier le porteur à l'aide de la cryptographie à clé publique.

3.4.1 Architecture

Les architectes de SET ont eu pour principe fondamental de sécuriser les transactions par carte bancaire sur l'Internet sans modifier les circuits bancaires d'autorisation et de télé-collecte existants.

Les réseaux de cartes bancaires font intervenir des serveurs d'autorisation afin de filtrer les transactions abusives selon des critères précis, par exemple un plafond de dépenses, le nombre excessif de transactions conduites pendant un intervalle donné, etc. Ainsi, avant d'autoriser une transaction par carte bancaire, le marchand doit interroger le serveur correspondant de son banquier. Dans un second temps, le marchand doit interroger le serveur correspondant à la vente d'un bien ou d'un service, dans l'étape dite de compensation. Mais les règles des différents systèmes de cartes bancaires exigent que la compensation du marchand ne se fasse qu'après l'expédition des biens acquis ou la réalisation du service. Pour recouvrer ses créances, le marchand envoie à son banquier une requête de compensation, qui sera acheminée vers la banque émettrice à travers les réseaux bancaires. Dans certains systèmes de cartes bancaires, les demandes d'autorisation et de compensation peuvent être combinées en une seule et même opération lors de chaque transaction. D'autres systèmes permettent le regroupement des requêtes d'autorisation ou de compensation, par exemple à la fin de chaque journée de travail.

Si le marchand doit rembourser l'acheteur, soit que le produit lui ait été retourné, soit qu'il se soit avéré défectueux, le marchand devra donner à son banquier des instructions pour créditer le compte du client.

Afin de ne pas perturber cet édifice qui fonctionne déjà au niveau planétaire, SET fait appel à deux nouveaux acteurs : l'autorité certifiante chargée de certifier les acteurs et la passerelle de paiement. Cette dernière gère la frontière entre l'Internet et le réseau de carte bancaire.

Les principaux acteurs de SET sont donc au nombre de six :

- le détenteur de la carte bancaire (le porteur) ; il possède une carte, conforme aux spécifications SET, émise par une institution émettrice, typiquement une banque affiliée à VISA ou MasterCard ;
- le serveur du marchand ;
- l'autorité de certification ;
- la passerelle de paiement ;
- l'institution émettrice de la carte bancaire du porteur ;
- l'institution d'acquisition, qui est souvent la banque du marchand.

La figure 3.3 illustre le schéma fonctionnel de SET. Le porteur, le marchand, l'autorité certifiante et la passerelle de paiement sont reliés par le réseau Internet. Le client n'établit pas de connexion directe avec la passerelle de paiement, mais utilise un tunnel (*tunneling*[4]) passant par le serveur du marchand. Chaque participant doit d'abord obtenir un certificat auprès d'une autorité certifiante agréée selon les spécifications de SET. Ces certificats sont ensuite inclus dans les messages échangés entre le détenteur de la carte, le marchand et la passerelle de paiement.
Les institutions émettrices et d'acquisition sont reliées par un réseau bancaire fermé et sécurisé. La passerelle de paiement fait le pont entre les deux réseaux ouvert et fermé, ce qui permet de protéger l'accès au réseau bancaire. Elle doit donc posséder deux interfaces, l'une pour le protocole SET (côté Internet), l'autre pour un protocole propriétaire (côté réseau bancaire).

---

[4] Le fait pour un réseau d'utiliser les connexions d'un autre réseau, en encapsulant ses données dans des paquets conformes au protocole utilisé sur le second réseau

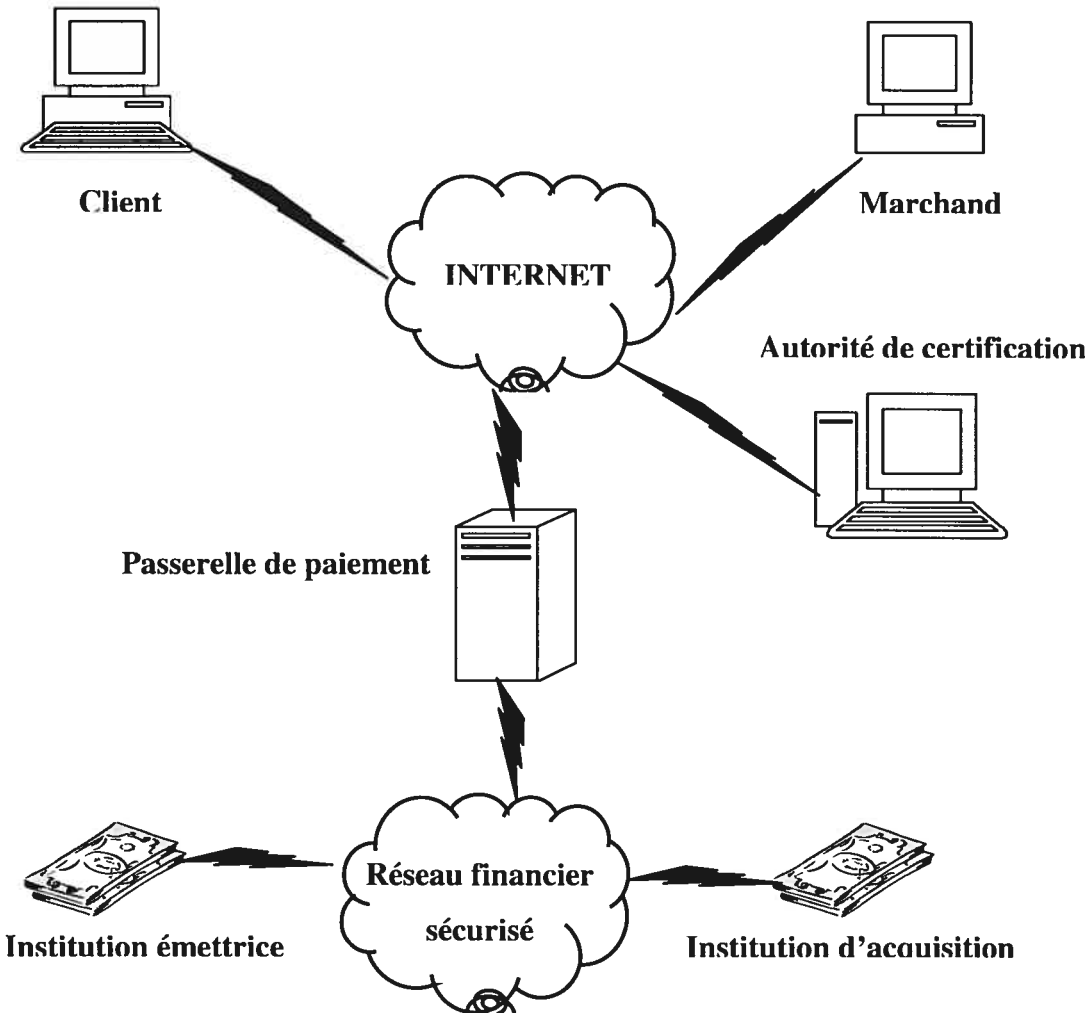

Figure 3.3. Les acteurs d'une transaction SET

SET sécurise les échanges entre le client et le marchand ainsi qu'entre le marchand et la passerelle de paiement. La passerelle de paiement administre les paiements pour le compte des banques émettrices de cartes bancaires et des banques d'acquisition. En toute logique, elle doit aussi être entérinée par les autorités bancaires, sinon être sous la responsabilité d'une institution financière pour s'acquitter de ces fonctions.

La figure 3.4 présente la position de SET dans la pile protocolaire TCP/IP.

Le protocole SET est un protocole orienté transaction et fonctionne selon le mode requête/réponse ; en d'autres termes, les messages constituent des paires. La structure des messages suit les règles DER (*Distinguished Encoding Rules*, règles de codage

distinctives) de la notation ASN.1 (*Abstract Syntax Notation 1*, notation de syntaxe abstraite 1) [Steedman93].

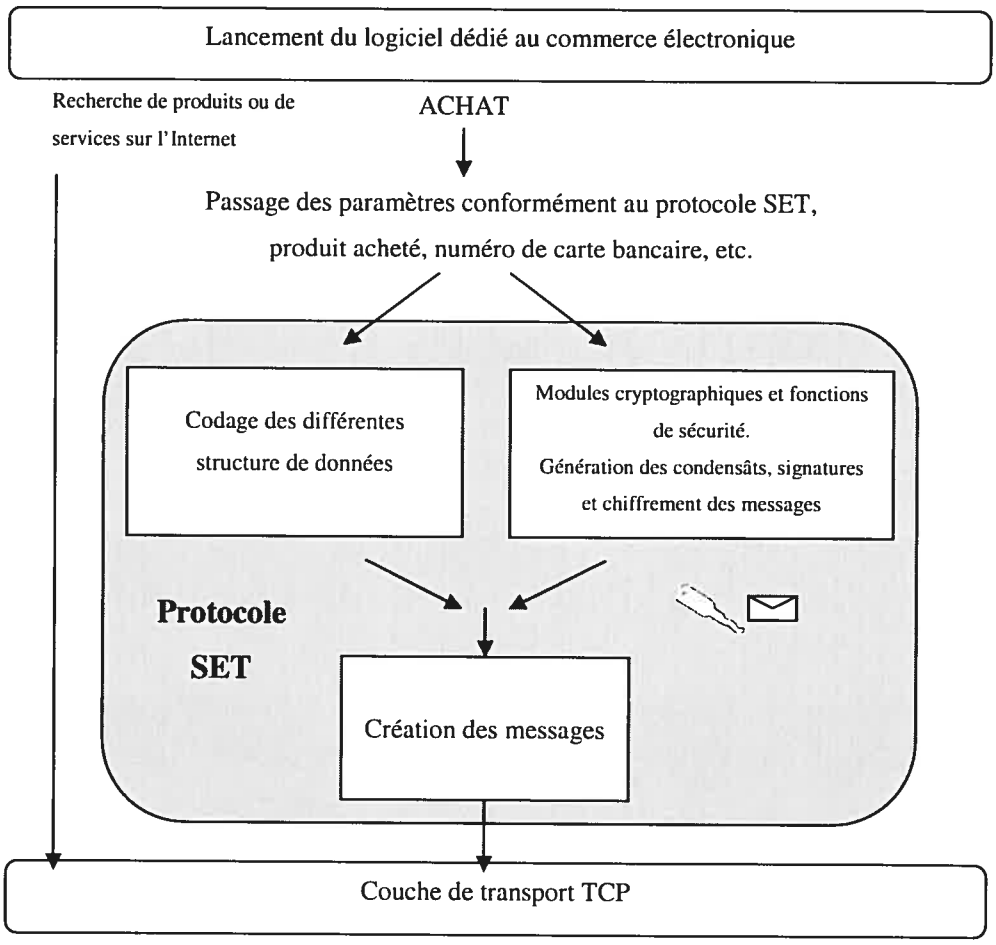

Figure 3.4. Positionnement de SET au-dessus de la pile TCP/IP

3.4.2 Sécurisation

Les transactions de SET fournissent les services suivants :

- inscription des porteurs et des marchands auprès de l'autorité certifiante ;
- octroi de certificats aux porteurs et aux marchands ;
- authentification, confidentialité, intégrité des transactions d'achats ;
- autorisation de paiement ;
- capture (collecte) du paiement pour initier la demande de compensation financière au profit du marchand.

SET utilise les techniques de cryptographie à clé publique afin de garantir à la fois :

- la confidentialité des échanges pour qu'ils ne puissent pas être lus en ligne par une entité extérieure à la transaction ;
- l'intégrité des données échangées entre le client, le marchand et la banque acquéreur ;
- l'identification des intervenants ;
- l'authentification des intervenants.

Pour assurer le service de non-répudiation des transactions, une condition nécessaire mais non suffisante est que le porteur de la carte soit certifié. Les autres conditions portent sur la réalisation d'un mécanisme d'horodatage et sur le caractère irréfutable des autorités certifiantes et des passerelles de paiement.

La *confidentialité* des messages est assurée à l'aide d'algorithmes de chiffrement symétriques. Cependant, la clé secrète est elle-même distribuée à l'aide d'algorithmes de cryptographie à clé publique. Ainsi, lorsque la passerelle de paiement désire envoyer des données de façon confidentielle au marchand, elle génère une clé de chiffrement symétrique avec laquelle elle les chiffre. Cette même clé est chiffrée avec la clé publique du destinataire qui, étant l'unique détenteur de la clé privée correspondante, sera le seul capable de récupérer la clé symétrique et de déchiffrer les données.

L'*intégrité* des messages a pour but de garantir que les données reçues sont bien celles que l'émetteur avait envoyées et qu'elles n'ont pas été modifiées par malveillance ou par erreur pendant leur transit sur le réseau. SET utilise le sceau de l'expéditeur pour assurer l'intégrité du message. Quiconque dispose de la clé publique de l'émetteur pourra vérifier l'intégrité du message en comparant le condensât obtenu et en déchiffrant le sceau au condensât recalculé. Le sceau garantit à la fois l'identité de l'émetteur et l'intégrité des données, si le couple clé publique et clé privée est unique et en l'absence de toute tentative d'usurpation d'identité.

L'*identification* des participants dans une transaction SET correspond à une relation préétablie entre une clé de chiffrement et une entité. Ainsi, chaque entité joint à son message, chiffré ou non, une signature numérique qu'elle seule peut générer, mais qui peut être vérifiée par les entités paires.

Dans le protocole SET, c'est le crédit accordé au certificat scellé par l'autorité certifiante de SET qui sanctionne, d'une manière sûre, l'association d'une clé publique à son propriétaire et donc *l'authentification* de ce dernier.

Les procédures d'authentification du protocole SET sont fondées sur la version 3 de la recommandation X.509 de l'UIT-T. Chaque certificat comporte l'identité de son propriétaire, une clé publique relative à l'algorithme de chiffrement à clé publique employé et le sceau de l'autorité ayant délivré ce certificat. Pour s'authentifier mutuellement, deux parties doivent remonter l'arborescence de certification jusqu'à un nœud commun.

3.5 Conclusion

Le protocole SSL est actuellement le seul protocole de sécurisation déployé à grande échelle. Il se trouve déjà sur la plupart des plates-formes sécurisées de la Toile aussi bien du côté serveur que du côté client. Son grand avantage est sa transparence par rapport aux applications sur TCP.

SSL semble inadapté aux applications du commerce électronique qui mettent en relation plusieurs acteurs, notamment le client, le marchand et une passerelle avec les réseaux bancaires. Pour tenir compte des différentes relations d'intermédiation commerciale, il faut associer d'autres protocoles à SSL, ce qui risque d'alourdir l'architecture des systèmes de communication.

En outre, dans SET, les moyens de sécurisation sont assez compliqués, pour que les participants puissent conserver les renseignements nécessaires durant chaque transaction, ainsi que sécuriser les informations non autorisées aux autres participants, ce qui se traduit par une surcharge en calcul et des temps de réponse assez longs.

SET a donc été sévèrement critiqué et la lourdeur de son fonctionnement exclut son utilisation pour les paiements de faibles montants.

D'où la nécessité de développer *SecAdvise* qui assistera à la sélection optimale d'un ou de plusieurs combinaisons de mécanismes de sécurité pour un scénario de sécurité donné. Nous identifions un scénario comme étant l'ensemble des menaces et vulnérabilités qui menacent le système ou l'infrastructure effectuant une transaction sur le réseau ouvert.

Chapitre 4. Inventaire des architectures existantes

4.1 Introduction

Les chapitres précédents ont décrit quelques mécanismes de sécurité spécifiques à différents systèmes de paiements sécurisés. Chaque système de paiement définit ses propres messages et a ses propres conditions de sécurité. Ainsi plusieurs initiatives ont cherché à faire converger les diverses approches en vue d'élaborer une plate-forme de services commune.

Nous décrirons dans ce chapitre le programme européen SEMPER (*Secure Electronic Marketplace for Europe*) [Lacoste00] ainsi que la plate-forme IOTP (*Internet Open Trading Protocol*) [Hassler01]. Nous terminerons par la description d'un modèle de confiance [Robles01] sur lequel nous nous baserons pour créer notre aviseur de sécurité.

4.2 *Secure Electronic Marketplace for Europe* (SEMPER)

SEMPER était un projet parrainé par la direction générale XIII de la commission européenne de 1995 à 1998 dans le programme de recherche ACTS 026 (*Advanced Communication Technologies and Services*) [Lacoste00].

Le but de SEMPER était d'examiner le commerce électronique sur des réseaux ouverts et non sécurisés de tous les points de vue, qu'ils soient légaux, commerciaux, sociaux ou techniques. Du point de vue technique, cela signifie que l'accès ouvert et sécurisé sur la Toile (Web) doit être indépendant de l'architecture du réseau, du système d'exploitation, des équipements périphériques (carte à puce ou ordinateur) ou des logiciels employés. Dans ce contexte, une architecture ouverte est non-propriétaire et aussi évolutive, permettant l'ajout de nouveaux composants sous forme de *plug-in*. En d'autres termes, le principe opératoire est de masquer les particularités des différentes

méthodes de paiements électroniques au moyen d'API spécifiques, afin de permettre l'emploi de tout moyen de paiement que l'usager a choisi.

4.2.1 Architecture de SEMPER

Les concepteurs de SEMPER ont choisi une architecture en quatre couches illustrée à la figure 4.1

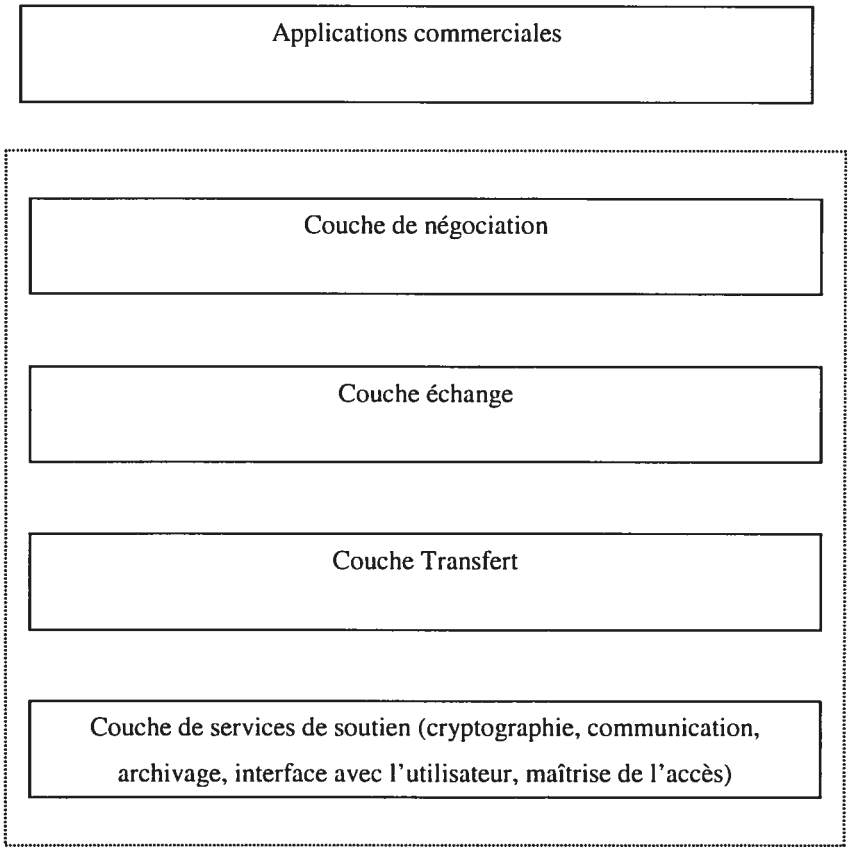

Figure 4.1. Architecture de SEMPER

1. La couche de négociation (*commerce layer*) se rapporte aux détails de la session commerciale tels que la commande d'articles, les instructions de paiement, la signature, etc.
2. La couche échange (*exchange layer*) se charge d'établir les dialogues entre les diverses entités participant à une transaction : le débiteur, le créditeur, les institutions émettrices et d'acquisition et, selon les cas, l'arbitre, le notaire ou le tiers de confiance. Le principe de l'équité des échanges (*fair exchange*) sous-tend

toute l'architecture de SEMPER. Ainsi, chaque partie doit être assurée de la réciprocité de la transaction, c'est-à-dire qu'elle reçoit toujours la contrepartie d'un bien envoyé conformément à l'accord commercial établi entre les partenaires.

3. La couche transfert (*transfer layer*) utilise des « conteneurs » (*containers*) pour l'envoi d'informations (documents signés ou paiement) destinées aux couches supérieures et pour la réception de données originaires de ces mêmes couches, conformément aux protocoles de sécurité. Cette couche se compose de trois blocs distincts pour les fonctions de certification, de vérification des déclarations (par exemple des signatures) ou de paiement. Ces blocs sont respectivement nommés « bloc de certification » (*certification block*), « bloc des déclarations » (*statement block*) pour les documents électroniques ou « bloc des paiements » (*payment block*) (figure 4.2). Grâce à ce cloisonnement des rôles, il est possible d'adapter l'architecture au mode de paiement sélectionné sans perturber l'édifice qui fonctionne déjà au niveau planétaire.

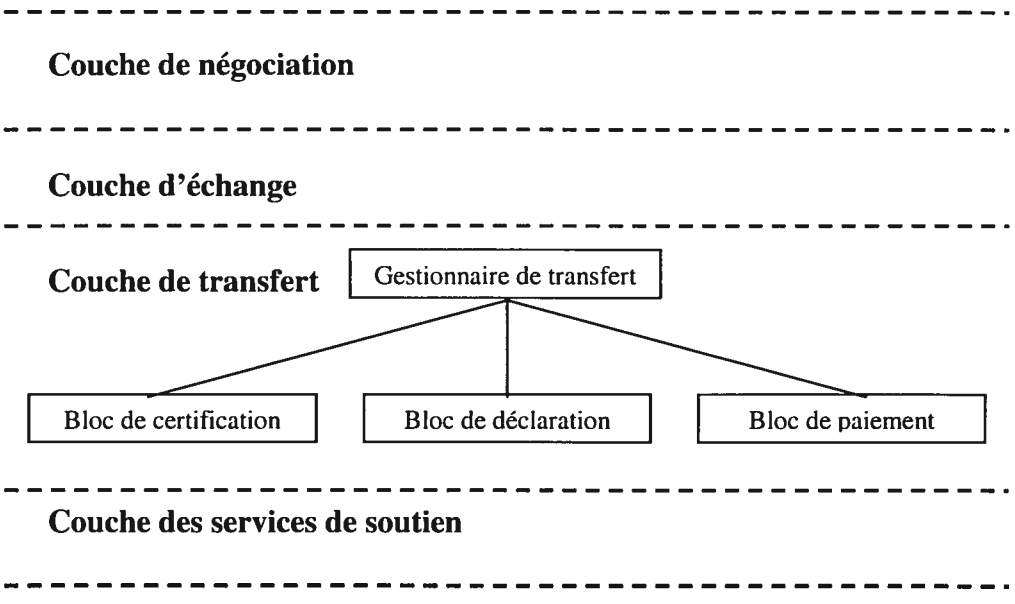

Figure 4.2. La couche de transfert de SEMPER

4. Enfin la couche des services de soutien (*supporting services layer*) effectue les fonctions de sécurisation par chiffrement, de communication avec les différents réseaux, d'archivage et de maîtrise de l'accès. L'offre d'archivage se rapporte aux messages échangés, mais peut aussi inclure l'archivage des certificats et des paires de clés de chiffrement pour les algorithmes de chiffrement asymétrique.

Le gestionnaire de transfert (*transfer manager*) se charge de l'analyse syntactique du message reçu de la couche échange avant de l'aiguiller vers le bloc assorti. Dans le sens inverse, il compose les en-têtes des messages avant de les envoyer sur le réseau approprié (l'Internet ou le réseau bancaire).
Le bloc de certification vérifie et authentifie les paramètres du client ou de l'institution financière.

4.2.2 Terminologie de SEMPER

SEMPER répartit les instruments de paiements en deux catégories [Abad96b, Abad98] :

- Les instruments orientés espèces (*cash-like*), tels que les cartes à puce préchargées de monnaie légale, les systèmes de porte-monnaie électronique comme *Chipper* ou le paiement par monnaie numérique de *DigiCash*;
- Les instruments orientés comptes (*account-based*) tels que les chèques virtuels, les avis de prélèvement et les virements (transferts électroniques de fonds). Selon l'écart entre le moment où le débiteur effectue le paiement et celui où le créditeur reçoit la valeur correspondante, SEMPER distingue les instruments de paiement instantané (*pay now*), lorsque le compte du payeur est débité instantanément, et les instruments de paiement en différé (*pay later*), lorsque le compte bancaire du commerçant est crédité du montant de la vente avant que le compte du payeur ne soit débité.

Certaines cartes de débit relèvent de la catégorie des instruments de paiement instantané tandis que les systèmes de crédit ou de débit différé font partie des instruments de paiement différé. Les architectes de SEMPER ont rebaptisé les avis de prélèvement (*indirect pull)* et les virements (*indirect push*).

La passerelle de paiement de SEMPER effectue la jonction entre les systèmes bancaires existants et les nouveaux instruments utilisés sur l'Internet, par exemple SET, *Chipper* ou le système de monnaie numérique de *DigiCash*. La fonction de la passerelle de SEMPER est de masquer les détails du système de paiement par rapport aux circuits bancaires. Par conséquent, pour les paiements orientés crédit, l'interface entre la passerelle et la banque émettrice et une banque acquéreur. De même, la passerelle doit utiliser les messages EDIFACT dictés par la norme ISO 9735 dans le cas de virements.
Dans le cadre de SEMPER, un porte-monnaie (*purse*) se trouve à chaque extrémité du transfert de valeurs effectué à l'aide d'un moyen de paiement. Un porte-monnaie de SEMPER est donc l'instance abstraite d'un système de paiement disponible à l'usager. Selon cette définition, chaque carte bancaire du payeur conforme à l'un des protocoles de paiement en ligne tels que SET ou EMV (*Europay, MasterCard and Visa*) correspond à un porte-monnaie de SEMPER. SEMPER reconnaît aussi les porte-monnaie électroniques émis selon les spécifications de Chipper, Ecash ou autres. Le même porte-monnaie peut être impliqué dans plusieurs transactions commerciales simultanées sous la vigilance d'un gestionnaire de paiement (*payment manager*).

4.2.3 Le gestionnaire de paiement

Le gestionnaire de paiement a deux fonctions : il administre le choix du porte-monnaie convenable pour une transaction et il recense les porte-monnaie disponibles en tenant l'inventaire des transactions actives ou passées, surtout celui des données qui permettent la récupération en cas de panne.
La figure 4.3 illustre les composantes du gestionnaire de paiement et les différentes interfaces internes et externes. Chaque porte-monnaie communique avec l'instance du système de paiement choisi par le truchement d'adaptateurs spécialisés qui établissent la jonction entre le modèle de paiement et l'instance externe du système de paiement [Abad96a].

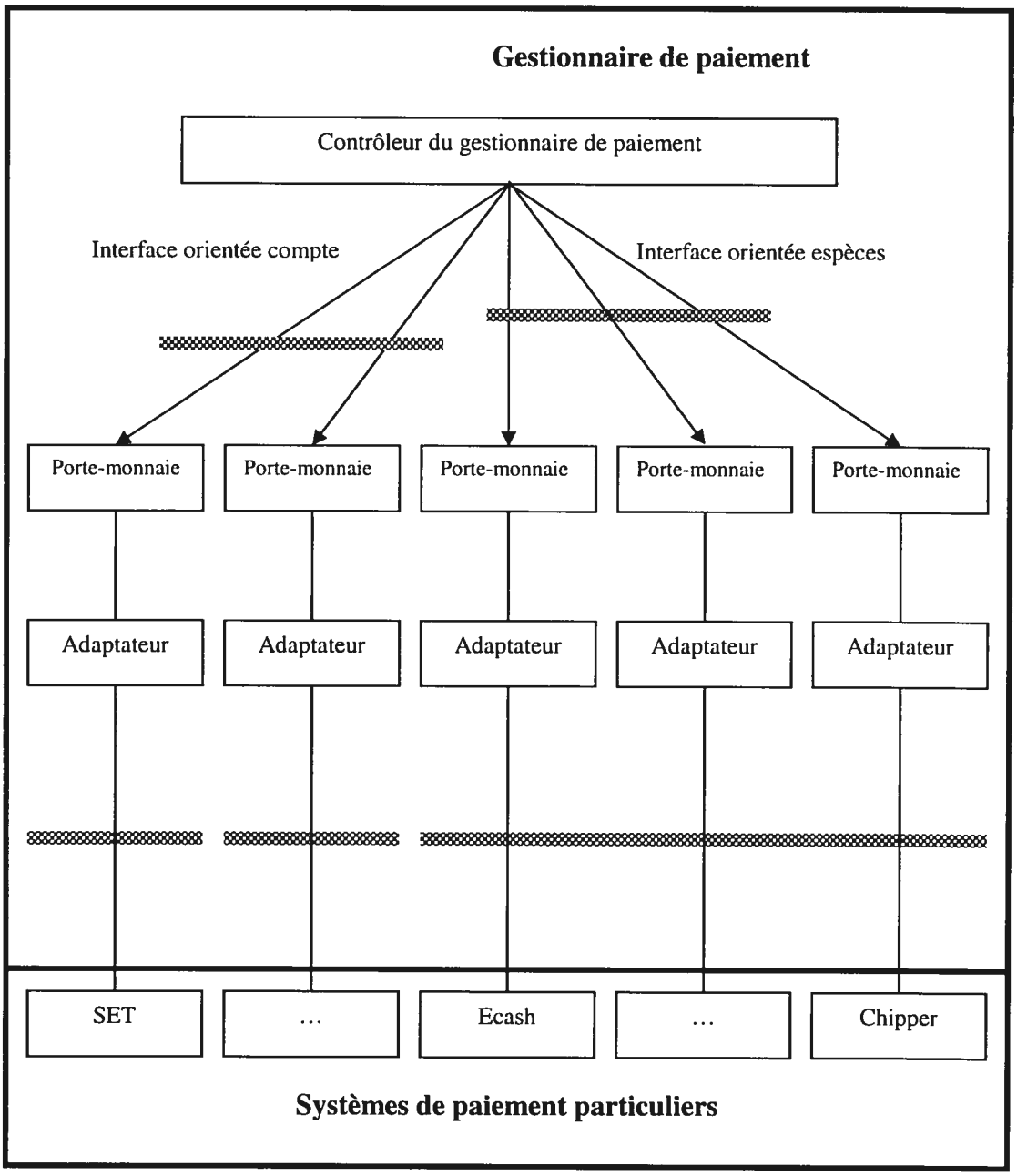

figure 4.3. Organisation du gestionnaire de paiement de SEMPER

4.3 *Internet Open Trading Protocol* (IOTP)

Le IOTP (*Internet Open Trading Protocol*) [Burdett00] est une plate-forme de paiement pour le commerce électronique dont le but est d'assurer l'interopérabilité parmi différents systèmes de paiements. Le groupe de travail d'IETF, le responsable de ce projet, a le même nom (IOTP WG) et appartient au domaine d'applications d'IETF. Un participant à IOTP peut exécuter un ou plusieurs rôles de commerce: le consommateur, le marchand, la banque, l'agent de la livraison et le service à la clientèle. Par exemple, un marchand peut être en même temps le fournisseur du service à la clientèle. Le protocole décrit le contenu, le format et la séquence des messages de commerce électronique qui sont échangés entre les participants.

Les messages IOTP sont des documents XML (*Extensible Markup Language* [W3CXML98]). Un ensemble prédéfini de messages IOTP définit un échange de commerce (par exemple l'offre, le paiement, la livraison, l'authentification). Les transactions peuvent être de différents types, tels que l'achat, le remboursement ou l'authentification.

IOTP est indépendant des systèmes de paiements. Cela signifie que n'importe quel système de paiement électronique (par exemple SET ou *DigiCash*) peut être employé dans la plate-forme. Chaque système de paiement définit certaines séquences spécifiques de message. Les spécifications fondamentales des protocoles de paiements sont contenues dans un ensemble supplémentaire des spécifications d'IOTP.

La figure 4.4 illustre la structure générale des messages IOTP. Elle se compose de plusieurs blocs. Chaque message a un bloc de référence de transaction (*Trans Ref Block*) qui identifie une transaction d'IOTP. Une transaction (par exemple l'achat, l'authentification, le retrait, le dépôt) a un identifiant de transaction globalement unique (*Trans Id*). Elle inclut un ou plusieurs messages d'un ensemble prédéfini et tous les messages appartenant à la même transaction ont le même *Trans Id.* En plus, chaque message a son propre identifiant (*Msg Id*) qui est unique dans la transaction. Un message contient un ou plusieurs *Trading Block*, par exemple, requête et réponse d'authentification ou requête et réponse de paiement. Optionnellement, il peut contenir des *signature blocks* ou des *Trading Components* et une *Certificate Component* pour la

vérification de signatures. Finalement, un *Trading Block* se compose d'un ensemble prédéfini de *Trading Components* (par exemple, requête et réponse d'authentification, arrangement de paiement et reçu de paiement).

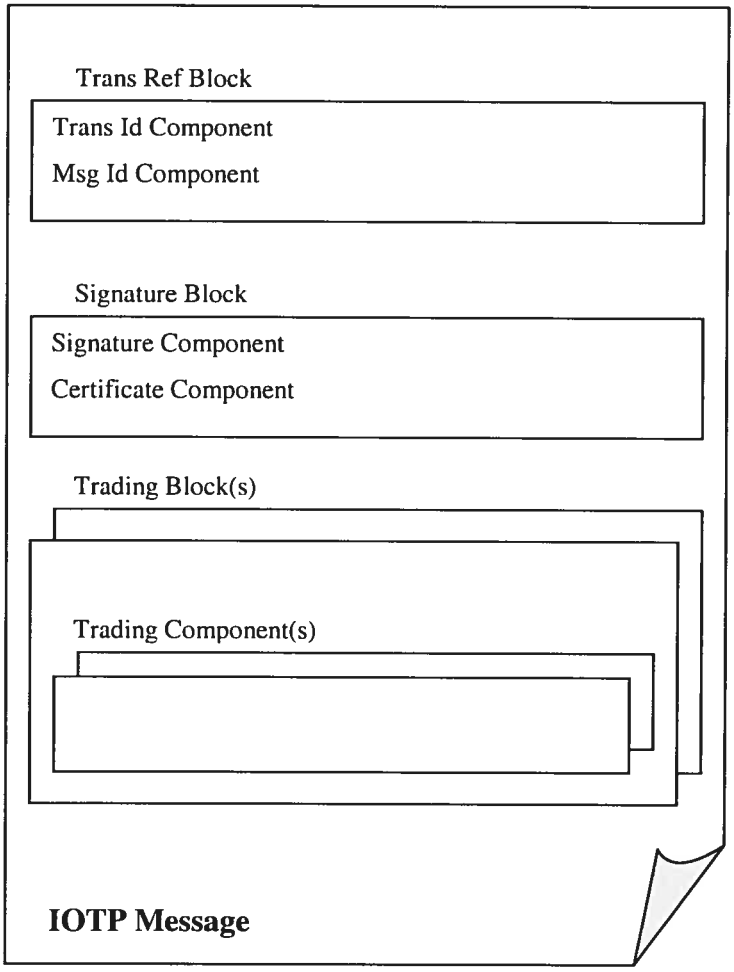

Figure 4.4. Message IOTP

4.3.1 Sécurisation

La plupart des systèmes de paiement qui peuvent être employés dans la plate-forme d'IOTP ont déjà leurs propres concepts de sécurité. Néanmoins, il y a quelques concepts de sécurité qui sont couverts par IOTP pour assurer une protection additionnelle facultative. S'il est nécessaire de considérer la sécurité de paiement dans une perspective IOTP, ceci devrait être inclus dans le supplément de protocole de paiement qui décrit comment IOTP soutient ce protocole de paiement.

Les participants à IOTP peuvent s'authentifier par un échange d'identité. L'authentification peut être effectuée à un point quelconque dans le protocole. Elle suspend simplement la transaction IOTP courante. Par exemple, un consommateur peut vouloir authentifier l'agent de paiement après la réception d'une réponse d'offre du marchand et avant d'envoyer la demande de paiement à cet agent de paiement. Le protocole d'authentification est en dehors de la portée d'IOTP. Si la transaction d'authentification est réussie, la transaction IOTP originale est reprise; autrement elle est annulée. La transaction d'authentification peut être liée à la transaction IOTP originale au moyen du composant *Related To Component* contenant l'identifiant de la transaction IOTP (*Trans Id*).

L'intégrité des données et la non-répudiation d'origine peuvent être réalisées au moyen de signatures numériques [Davidson99]. Par exemple, un agent de paiement peut vouloir fournir une preuve de non-répudiation du statut d'accomplissement d'un paiement. Si une réponse de paiement est signée, alors le consommateur peut plus tard l'utiliser comme preuve de paiement. En outre, il est possible d'employer les signatures numériques pour lier ensemble les enregistrements contenus dans les réponses de chaque échange commercial d'une transaction. Par exemple, IOTP peut lier ensemble une offre et un paiement. Un *Signature Component* comprend les éléments suivants :

- des éléments de sceaux (signatures digitales des condensâts) contenant des sceaux d'un ou de plusieurs blocs de commerce ou des composants de commerce dans un ou plusieurs messages d'IOTP (de la même transaction d'IOTP);
- un élément manifeste (référence vers les éléments signés) comprenant l'émetteur, le destinataire et l'algorithme de signature, le tout enchaîné avec les éléments de sceaux;
- une valeur représentant la signature de l'élément manifeste.

Optionnellement, le certificat d'originaire peut être inclus dans le *Certificate Component* du même bloc de signature.

La confidentialité des données est assurée en envoyant les messages IOTP entre les divers participants à l'aide d'une connexion sécurisée, avec SSL ou TLS, par exemple. L'utilisation d'une connexion sécurisée est facultative dans IOTP.

4.4 Le modèle de confiance de Robles

Nous représentons ici un modèle de confiance proposé dans [Robles01]. Cet article discute des aspects requis dans ce modèle pour des applications de sécurité multi-agents dans le contexte du commerce électronique. Ce modèle décrit une méthodologie pour augmenter la protection et la confiance dans les systèmes de commerce électronique.

4.4.1 Définitions et méthodologie du modèle de confiance

Le modèle de confiance de Robles est un modèle descriptif ou conceptuel qui se concentre sur l'identification des problèmes de confiance et sur le développement d'une méthodologie pour dériver une solution de confiance s'appliquant à ces problèmes. Le but de ce modèle de confiance est de définir un espace de problème de confiance ou *Trust Problem Space* et de relier cet espace à une collection de mécanismes en corrélation pour fournir des sauvegardes afin de protéger des systèmes et des sous-systèmes et d'ainsi augmenter la confiance dans ces systèmes ou ces sous-systèmes. Ce modèle de confiance combine les notions mentionnées dans [Robles01, Abdul96, Marsh94], soit la confiance de contrôle et la confiance sociale.

4.4.1.1 L'espace du problème de confiance TPS (*Trust problem Space*)

Un TPS est défini comme étant l'ensemble de toutes les situations possibles dans le système, dans lequel les agents de commerce électronique peuvent avoir des problèmes de confiance entre eux ou au sujet de l'environnement. Cet espace contient divers types d'attaques et de vulnérabilités causés par la fraude ou l'abus des ressources de système.
Pour définir le TPS, Robles utilise les unités de base appelées sous-espaces de problème de confiance TPSS (*Trust Problem Sub-Spaces*) de telle manière que le TPS se compose d'un ensemble de TPSS indépendants (figure 4.5)

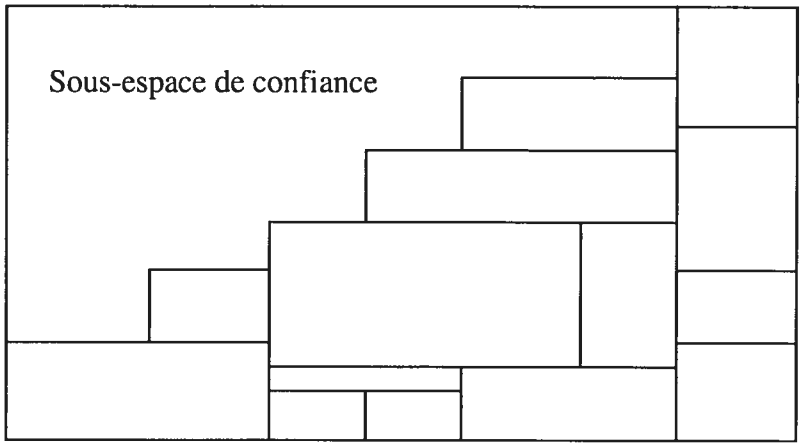

Figure 4.5. L'espace des problèmes de confiance (espace de confiance et sous- espaces de confiance) [Robles01]

4.4.1.2 Unité de confiance TU (Trust Unit)

Une TU est une unité logique de confiance représentant une solution ou des contre-mesures partielles ou complètes à n'importe quel TPSS présenté précédemment (Figure 4.6). Cela peut impliquer des protocoles, des mécanismes de sécurité ou des infrastructures cryptographiques.

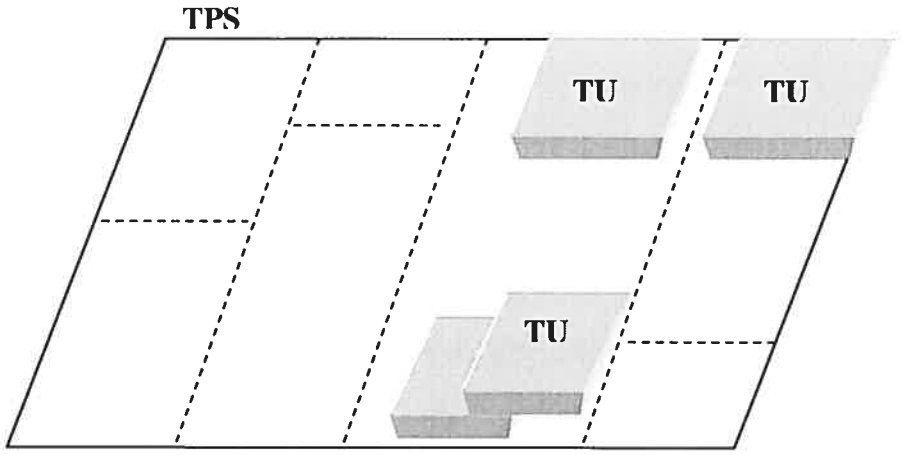

Figure 4.6. Unités de confiance dépendant d'autres unités de confiance et couvrant partiellement l'espace de problème de confiance [Robles01]

4.4.1.3 Solution de confiance TS (*Trust Solution*)

Une TS est un ensemble d'unités de confiance (TU) qui couvre totalement l'espace de problème de confiance, c'est-à-dire tous les TPSS (figure 4.7). Une TU pourrait ne pas être indépendant ou d'un seul bloc et peut aussi employer des mécanismes d'autres TU. Ces relations sont énoncées dans un champ appelé *dependencies* dans la TU, indiquant les conditions et l'utilisation parmi toutes les TU. Ainsi un TS définit un enchaînement complexe de TU. Un TS remplit les conditions de confiance de la description de l'espace du problème de confiance. Puisque plusieurs TU pourraient couvrir le TPS, il se peut donc que plusieurs TS puissent exister. S'il était possible d'évaluer la complexité de chaque TS, il serait alors possible de déterminer quel ensemble de TU est le meilleur TS pour le système.

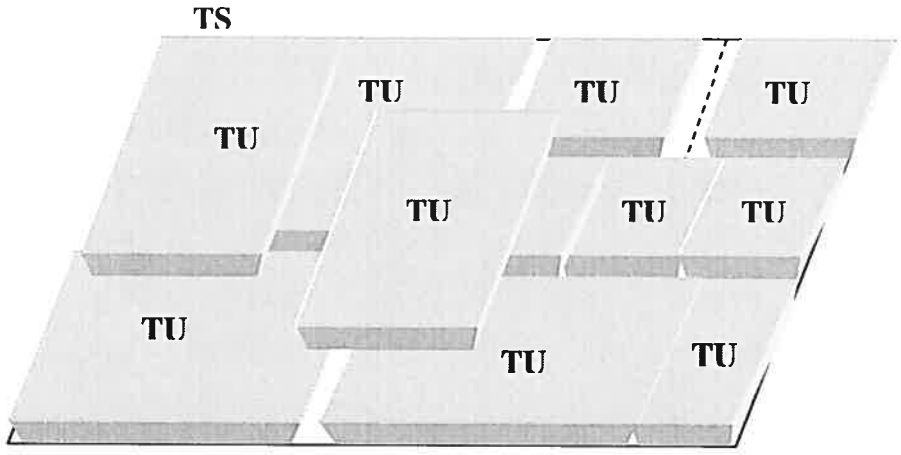

Figure 4.7. Solution de confiance : l'ensemble des TU couvrant totalement le TPS [Robles01]

4.4.1.4 La méthodologie du modèle de confiance

L'idée globale de ce modèle de confiance est de définir un ensemble dominant de contraintes pour la confiance croissante en systèmes. Ceci comprend la sécurité classique avec la confidentialité, l'authentification et la non-répudiation pour les actions et l'information, aussi bien que les mécanismes de sécurité directs (par exemple des mécanismes techniques tels que l'infrastructure de gestion de clés publiques) et indirects (par exemple des mécanismes organisationnels tels que la rédaction des politiques et

procédures de sécurité) pour augmenter la performance et pour améliorer l'utilisation du système.

Dans le modèle de Robles, on définit une méthodologie à trois dimensions. Premièrement, nous devons définir l'espace de problème de confiance (TPS), c'est-à-dire définir les conditions de confiance et les vulnérabilités de confiance. Deuxièmement, nous définissons les unités de confiance (TU) qui représentent les solutions aux TPSS. Et troisièmement, nous choisissons et combinons certaines des unités de confiance (TU) déjà définies pour composer une solution de confiance (TS) qui couvre la totalité du TPS pour le système. Si plusieurs TS existent, seulement l'une d'elles doit être choisie. Ce choix pourrait tenir compte de la complexité telle que le nombre d'agents impliqués ou de participants externes, les infrastructures, etc.

4.5 Comparaison

SEMPER se concentre sur les systèmes de paiements sécurisés et la sélection des instruments de paiement suivant leur type, tels que la monnaie virtuelle, la carte bancaire, la carte à puce, etc. La sécurité des transactions dépend complètement des systèmes de paiement déjà choisis. SEMPER n'offre aucun suppléant de sécurité dans sa propre architecture. De plus, cette architecture ne discute pas la confiance vis-à-vis les solutions de sécurité trouvées. Enfin, SEMPER ne rentre pas dans les détails des transactions ; il s'inclut dans un niveau plus abstrait, les interactions dépendant du système déjà choisi.

IOTP est une architecture orientée transaction. Elle se contente de convertir les messages échangés entre les différents partenaires, utilisant n'importe quel système de sécurité, que ce soit SET, SSL ou *DigiCash*. Cette conversion est faite en langage standardisé XML, qui assure l'interopérabilité des systèmes de paiement. Cette plate-forme assure un minimum de sécurité en utilisant le mécanisme de signature électronique à clé publique. En fait, la vraie sécurité des transactions dépend strictement des systèmes de commerce électronique utilisés. De plus, cette plate-forme ne se charge pas de sélectionner le système de sécurité idéal pour une transaction de commerce électronique.

Enfin, le modèle de confiance de Robles se situe dans un niveau plus abstrait. Il se charge de sélectionner des solutions à n'importe quel problème de sécurité et de confiance. Le problème dans l'utilisation de ce modèle est de bien définir les risques et les attaques qui peuvent s'opposer aux systèmes de commerce électronique, ainsi que de bien associer les solutions (mécanismes de sécurités, protocoles ou infrastructure) aux risques. Dans ce modèle, l'étude des risques doit être bien poussée afin d'aboutir à une solution idéale.

4.6 Conclusion

Les différentes plates-formes communes des systèmes de sécurité de commerce électronique résolvent le problème d'interopérabilité d'un seul point de vue : SEMPER au point de vue porte-monnaie de paiement, IOTP au point de vue messages et le modèle de confiance de Robles au point de vue confiance en général.

Le modèle de confiance de Robles pourrait être une base solide afin de développer notre aviseur de sécurité *SecAdvise* pour sélectionner les mécanismes de sécurité nécessaires dans un scénario de sécurité donné (par exemple, un paiement sécurisé).

Nous avons choisi le modèle de confiance Robles à cause de sa transparence et de son abstraction. Il est indépendant des domaines d'application des systèmes de sécurité : une analyse de risques identifierait les vraies menaces et les exigences de sécurité nécessaires pour n'importe quelle transaction de commerce électronique. De plus, la sélection des mécanismes de sécurité est un résultat de cette analyse de risques, ce qui ajoute une transparence à notre aviseur *SecAdvise*.

Chapitre 5. L'aviseur préliminaire *SecAdvise*

5.1 Introduction

Dans ce chapitre, nous introduisons notre aviseur en mettant l'emphase sur les concepts de base utilisés. Notre but est de nous baser sur le modèle de confiance de *Robles* [Robles01] pour créer un aviseur de sécurité *SecAdvise,* interopérable dans les systèmes de commerce électronique. Dans notre recherche, nous limitons l'étude sur les systèmes de paiements sécurisés, sachant qu'il existe d'autres types d'interactions en commerce électronique, par exemple les systèmes électroniques de votes (e-voting) [Riera99].

SecAdvise aura l'habileté d'assister la sélection des mécanismes ou les systèmes de sécurité nécessaires pour exécuter une transaction de commerce électronique entre les différents partenaires impliqués dans cette transaction, ce qui l'identifie comme étant un gestionnaire des risques.

Au début, nous présenterons la méthodologie de *SecAdvise* impliquant l'analyse des risques et nous introduirons les formules et les termes ainsi que les règles de décompositions des TU de *SecAdvise,* en tenant compte des dénominations utilisées par *Robles*. Ensuite, nous introduirons la base de données de *SecAdvise.* Et enfin, nous testerons notre modèle sur une transaction de paiement, en utilisant le protocole de sécurité de paiement SET.

5.2 Discussion sur la décomposition suivant le modèle OSI

Dans la plupart des applications de commerce électronique, la sécurisation sur une seule couche est amplement suffisante. En effet, le but explicite de nombreux systèmes de paiement électronique est d'éviter que les informations concernant les comptes du client, comme les numéros de carte bancaire, circulent sur l'Internet en clair ou qu'elles soient accessibles au commerçant. C'est le cas par exemple dans SET; les informations de la transaction sont toutes cryptées, soit par des mécanismes de signature numérique, soit par des mécanismes de la signature duale qui sert à signer deux genres d'information

pour deux participants différents. La raison est que les deux sources les plus importantes de fraude par carte bancaire sont le vol de numéros de carte et leur utilisation fallacieuse par des commerçants peu scrupuleux. Par conséquent, les systèmes de paiement électronique se concentrent principalement sur la sécurisation des échanges associés à une transaction et non sur les négociations qui précèdent le placement de l'ordre d'achat. Or, il est parfois suffisant de détecter la présence d'une communication entre les partenaires, pour essayer par exemple de deviner :

- les caractéristiques des biens ou des services échangés;
- les conditions de leur acquisition : délais de livraison, conditions et mode de règlements;
- le règlement financier proprement dit.

L'établissement d'un canal chiffré ou «tunnel» entre les deux points au niveau de la couche réseau peut contrer ce type d'agression en masquant les échanges dès le début. Néanmoins, d'autres indices, tels que le temps relatif pris par les opérations cryptographiques, les variations dans la consommation électrique ou du rayonnement électromagnétique, pourraient permettre d'entrevoir les tendances du trafic chiffré et de finalement casser les algorithmes de chiffrement.

Nous pouvons déduire que la sécurité des données au niveau application est particulièrement nécessaire, vis-à-vis des données critiques. Par exemple, les informations d'une carte de crédit ne doivent pas être révélées au marchand. Ainsi, si on se contente de seulement sécuriser les données au niveau de la couche réseau, une fois arrivé à la couche application chez le marchand, le numéro sera en clair, ce qui est inacceptable au niveau de la confidentialité des données. Quant à l'authentification des partenaires, elle doit être faite aussi au niveau de la couche application. L'authentification des entités paires ne suffit pas pour donner la confiance au partenaire à l'autre bout. Une authentification serait faite en envoyant le certificat des partenaires avec les messages échangés dès le début des transactions, c'est-à-dire à la couche application.

5.3 La méthodologie de *SecAdvise*

En partant du principe que *SecAdvise* est un aviseur qui aide à la sélection de mécanismes de sécurité afin d'assurer un niveau de sécurité optimal dans une transaction de commerce électronique, *SecAdvise* devrait être un gestionnaire des risques.

La gestion des risques est le procédé qui consiste à évaluer les risques, à prendre des mesures pour les réduire à un niveau acceptable, à accepter les risques résiduels et à maintenir ce niveau de risque [Peletier01]. Un risque n'est pas une certitude, mais tout simplement la possibilité d'une occurrence défavorable dans le monde des TI et des réseaux ouverts; l'objectif consiste à diminuer le niveau de risque à l'aide de mesures de protection (mécanismes de sécurité). Le processus de gestion des risques inclut trois composantes : actif, menace et vulnérabilité [Pipkin00]. La réduction du risque s'effectue en réduisant soit l'incidence de l'une ou de l'autre des composantes de l'équation de risque (menace, vulnérabilité), soit les contrôles ou encore les mécanismes de sécurité, qui permettent d'éliminer une vulnérabilité de système ou d'empêcher une menace.

Globalement, nous divisons la méthodologie de *SecAdvise* en sept étapes:

1. identifier le domaine d'application de *SecAdvise* ;
2. identifier les ressources ou actifs à protéger ainsi que leur valeur;
3. identifier les menaces et les vulnérabilités sur les ressources et actifs ;
4. déterminer la probabilité d'occurrence des menaces ;
5. analyser les pertes potentielles dans le cas d'occurrence des menaces ;
6. identifier les mécanismes de sécurisations les plus efficaces dans un contexte donné (une menace exploitant une vulnérabilité dans un actif résultant un risque) ;
7. traiter le risque, c'est-à-dire sélectionner les mécanismes de sécurité déjà identifiés afin de réduire le risque.

En fait, le modèle de Robles à trois dimensions pourrait être associé aux étapes de SecAdvise :

- La définition de l'espace de problème de confiance (TPS) est effectuée par l'identification du domaine d'application, des actifs, des menaces et des vulnérabilités qui résultent de l'identification du risque (la perte qui résulte d'un risque sur un actif est un problème de confiance);
- Les unités de confiances (TU) qui représentent les solutions aux TPSS sont associées à l'étape 6, identification des mécanismes de sécurisations les plus efficaces ;
- Enfin, le TS, qui est la solution de confiance, est associé à la dernière étape de SecAdvise, sélection des mécanismes de sécurisation les plus optimaux. Cette sélection pourrait tenir compte de la complexité, telle que le nombre d'agents impliqués ou de participants externes, les infrastructures, etc.

5.3.1 Domaine d'application de *SecAdvise*

Les systèmes de communication mis en jeu s'appuient en général sur un réseau privé assez facile à isoler et à sécuriser ainsi que sur l'Internet pour accéder à des partenaires d'autres entreprises ou utiliser des ressources disponibles via ce réseau, voire à n'utiliser que le réseau Internet pour les besoins internes de l'entreprise.

Ainsi, nous distribuons les services de sécurité identifiés dans le chapitre 2, l'authentification (de l'entité homologue ou de l'origine des données), le contrôle d'accès, la confidentialité des données (selon différents modes de transfert), l'intégrité des données (selon les modes de transfert ou les parties protégées) et la non-répudiation (avec preuve d'origine ou de remise) entre trois aspects techniques : sécurité individuelle, sécurité collective et sécurité des échanges [Peltier01]. Ses trois aspects seront les domaines d'application de *SecAdvise*.

La sécurité individuelle implémente essentiellement les services d'authentification et de contrôle d'accès. Une première approche de cette solution a été définie par le ministère de la Défense des États-Unis DoD (*Department of Defense*) dans le cadre du projet

Kerberos. Elle repose sur un ensemble de serveurs (implantables sur un seul système) qui permettent de distribuer à des utilisateurs authentifiés des droits d'accès à des ressources pour une période donnée.

La sécurité collective met en jeu des sous-réseaux protégés par des coupe-feu (*firewalls*). Ceux-ci peuvent avoir des configurations très différentes selon le niveau de sécurité recherché et le niveau de contraintes acceptable. Ils peuvent être réalisés à partir d'un simple routeur muni d'un logiciel adéquat ou par un ensemble de deux routeurs et de serveurs *Proxy* placés dans une zone démilitarisée DMZ (*Demilitarized Zone*) ou par tout ensemble intermédiaire. Les sous-réseaux sécurisés peuvent être reliés entre eux dans un réseau virtuel privé VPN (*Virtual Private Network*) par des canaux de communication sûrs (tunnels).

La sécurisation des échanges entre partenaires distants ne peut mettre en œuvre que des services d'intégrité, d'authentification de la source des données, de non-répudiation et, éventuellement, de confidentialité.

5.3.2 Identification des ressources et actifs

Une ressource, c'est quelque chose qui a de la valeur pour une organisation et dont la perte ou l'altération est susceptible de causer des dommages à l'organisation tout entière. Les biens sont plus que de simples biens : ils comprennent le personnel, l'infrastructure, les relations avec les clients ou les partenaires et l'image de marque.

Toutes ces ressources ont des besoins de sécurisation qui dépendent de leur importance. Un inventaire complet des ressources est nécessaire pour savoir ce qui doit être protégé. Toutes les ressources concernant les informations capitales doivent être prises en compte et se voir attribuer un propriétaire, une classification de sécurité et une valeur [Pipkin00].

Un exemple de liste des actifs est présenté dans l'annexe B.

5.3.3 Estimation de la menace

Toute menace est une cause potentielle de perte. Vous n'avez aucun contrôle direct sur les menaces et il y a peu de choses à faire contre les menaces elles-mêmes, sinon essayer

de les comprendre. Vous ne pouvez que mettre en œuvre des sauvegardes pour vous protéger de leurs atteintes. L'étendue des menaces auxquelles doit faire face une entreprise peut être établie d'après sa localisation géographique, l'état d'esprit de son personnel, l'image de marque de l'entreprise, son organisation interne, ses partenariats et ses relations avec le public. Les menaces peuvent être internes ou externes. Les menaces internes viennent d'entités qui ont un accès légitime à l'objectif alors que les menaces externes ont pour source des entités qui n'y ont pas accès.

Le but d'une évaluation des menaces est de comprendre le type de menace et la probabilité qu'a cette menace d'entraîner une perte.

5.3.3.1 Identification de la menace

C'est le processus d'identification de l'utilisateur ou de l'évènement potentiellement menaçant. Les menaces courantes sont les erreurs, la fraude, le personnel mécontent, l'incendie, les pirates informatiques et les virus. Il est important d'identifier parmi ces causes celles qui ont le plus de chance de survenir et de provoquer des dommages.

5.3.3.2 Évaluation de la probabilité d'occurrence

C'est le processus d'évaluation du risque qu'une menace puisse causer une perte. Une estimation de probabilité prend en compte la présence, la ténacité et la force des menaces aussi bien que l'efficacité des moyens de prévention et l'existence de vulnérabilités. Nous pourrions organiser les menaces selon la probabilité de leur occurrence. Cette valeur peut servir de multiplicateur du dommage que pourrait causer la menace. Pour qualifier les catégories les plus courantes, nous parlons de « fréquent », « probable », « occasionnel », « éloigné » et « improbable ». En général, nous disposons d'informations statistiques sur les menaces physiques dans des domaines de comportement humain.

5.3.3.3 Analyse des pertes

L'analyse des pertes permet de définir l'impact de ces pertes. Celles-ci peuvent toucher l'entreprise sur le plan financier et sur le plan opérationnel. Bien comprendre ces impacts peut permettre à l'entreprise de définir les moyens d'assurer la continuité de ses opérations et d'établir des programmes de gestion des risques. Sans ces informations, il

n'est pas possible de définir correctement le coût de la remise en état consécutive à des attaques.

On peut établir un classement des pertes en neuf catégories [Pepkin00]:

- absence de service ;
- vol de ressources ;
- altération des informations ;
- destruction d'informations ;
- vol des informations ;
- divulgation des informations ;
- vol de logiciel ;
- vol de matériels ;
- dysfonctionnement des systèmes de contrôle.

Les TPS sont identifiés après l'évaluation les risques résultant d'une menace qui exploite la vulnérabilité d'un actif.

5.3.3.4 Identification des mécanismes de sécurité

La protection consiste à réduire les vulnérabilités par l'application des mesures préventives appropriées. Ayant identifié les risques qui menacent un actif ou une ressource ainsi que les mécanismes de sécurité existants en place, *SecAdvise* sélectionnera l'ensemble des mesures associées à un tuple (actif, vulnérabilité, menace).

L'annexe C représente un exemple d'un document de calcul des risques. Dans cet exemple, l'analyse est qualitative (valeur estimée suivant l'importance de l'actif ou la menace : basse - moyenne - élevée) et non quantitative (valeur monétaire de l'actif ou de la perte) [Peltier01].

Dans cet exemple, la valeur du risque est calculée en multipliant la valeur de l'impact de perte d'un actif résultant de la probabilité d'occurrence d'une menace :

Risque = Impact x probabilité

Ainsi, la sélection est basée sur la valeur et l'importance du risque identifié et calculé. Par la suite, nous définissons dans la table des risques une ligne de tolérance. Si le risque dépasse cette ligne, la sélection du contrôle identifié sera indispensable.

5.4 Définitions et formules

Afin de bien formaliser la méthodologie de *SecAdvise,* nous introduisons les définitions et les termes suivants :

c Le contexte/transaction à exécuter et qui a besoin d'être sécurisé.
Ce contexte ou transaction pourrait être un paiement par carte de crédit à un marchand.

$\mathbf{U}$ L'ensemble de toutes les unités de confiance TU (*Trust Unit*). Une TU peut être un mécanisme de sécurité, un protocole de sécurité ou une infrastructure de sécurité (algorithmes de cryptages, procédures de sauvegarde de l'information, mécanisme d'authentification, etc.). Dans notre exemple, **U** est l'ensemble de tous les mécanismes de sécurité contenant par exemple SET, SSL ou un autre mécanisme de sécurité.

u Une unité de confiance TU ($u \in \mathbf{U}$), par exemple SSL .

$\mathbf{R}$ L'ensemble de tous les risques de sécurité non décomposables, tels que $\forall r \in \mathbf{R}$, $\forall u \in \mathbf{U}$, u couvre r entièrement ou bien u ne couvre pas r. En d'autres termes, Nous décomposons les risques r de façon à ne pas avoir un mécanisme de sécurité qui couvre entièrement un risque r et à moitié un autre risque r'.

r Un risque de sécurité non décomposable ($r \in \mathbf{R}$) .

$\mathbf{P}$ L'ensemble de tous les participants potentiels dans une transaction sécurisée, par exemple un client, un marchand, une banque, une autorité certifiante, etc.

p Un participant $p \in \mathbf{P}$.

R_u L'ensemble des risques de sécurité couverts entièrement par l'unité de confiance u ($R_u \in P(\mathbf{R})$)

R_c L'ensemble des risques de sécurité à couvrir dans le contexte/transaction c ($R_c \in P(\mathbf{R})$). Ce sont les TPS définis au-dessus.

P_c L'ensemble de tous les participants qui sont impliqués directement dans le contexte/transaction c ($P_c \in P(\mathbf{P})$). Par exemple, un client veut payer un marchand, donc les participants directs sont le marchand, le client, la banque émettrice de la carte de paiement et la banque du marchand.

$A_{u,p}$ 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 une TU u ($u \in \mathbf{U}$, $p \in \mathbf{P}$, $A_{u,p} \in P(\mathbf{P})$). Si la TU n'a pas besoin d'une troisième partie de confiance, $A_{u,p} = \mathbf{P}$, pour simplifier le processus d'association entre les unités de confiance TU.

U_p L'ensemble des unités de confiance disponibles à un participant, par exemple PGP, SET, etc. Ces unités de confiance seront disponibles dans la base de données des mécanismes de sécurité. $p \in \mathbf{P}$ ($U_p \in P(\mathbf{U})$).

$\overline{U}_P$ L'ensemble des unités de confiance disponibles à tous les participants $\forall p \in \mathbf{P}(\overline{U}_P \in P(\mathbf{U}))$

$$\overline{U}_P = \{\ u \in \bigcap_{p \in P} U_p \mid \bigcap_{p \in P} A_{u,p} \neq \phi\ \}$$

Les unités de confiances u de cet ensemble utilisent la même infrastructure à clé publique, ou le même espace de confiance; en d'autres termes, les participants font confiance à une ou plusieurs autorités certifiantes communes.

$\tilde{U}_c$ L'ensemble minimal des unités de confiance pour couvrir les risques de sécurité d'une transaction/contexte c ($\tilde{U}_c \in P(\mathbf{U})$)

$$\tilde{U}_c = U \in P(\overline{U}_P) \mid R_c \subseteq \bigcup_{u \in U} R_u \wedge \|U\| = \min_{U' \in P(\overline{U}_{P_c})} \|U'\|$$

$\tilde{U}_c$ appartient à l'ensemble des unités de confiances disponibles à tous les participants tel que les risques associés au contexte sont couverts entièrement par l'ensemble minimal des unités de confiance disponibles pour tous les participants.

L'ensemble **R** est défini comme étant l'ensemble des risques non décomposables. Définir cet ensemble n'est pas une tâche simple. Afin de bien définir cet ensemble, la

gestion de risque au début de l'exécution de *SecAdvise* sera nécessaire. Par conséquent, nous pourrions construire **R** à partir de l'analyse de risque établie, en prenant en considération que si nous trouvons une unité de confiance u et que le risque r est couvert en partie par u, nous pouvons toujours définir des risques r' et r'', comme étant $r' \bigcup r'' = r$ et $r' \bigcap r'' = \phi$ et que r' est couvert entièrement par u et r'' n'est nullement couvert par u.

Ces règles seront les conditions de sélection des TU pour un ensemble de risques donné.

5.5 Structure de la base de donnée de *SecAdvise*

La base de données de *SecAdvise* se constitue de plusieurs tables associées aux mécanismes de sécurité et à leurs domaines d'application, aux services de sécurité ainsi qu'aux risques de sécurité.

5.5.1 Table du domaine d'application des mécanismes de sécurité

La table de domaine d'application contient l'information touchant le domaine d'application du contexte c (sécurité individuelle, sécurité collective ou sécurité des échanges).

5.5.2 Table des actifs et ressources

La table des actifs contient l'inventaire de tous les actifs et ressources dans l'organisation. Pour chaque actif, nous assignons le possesseur, la valeur (qualitative ou quantitative) et la classification.

5.5.3 Table des types de mécanismes de sécurité

Les types de mécanismes de sécurité ou mesures de sécurité sont catégorisés en plusieurs classes (par exemple : mesure technique, mesure organisationnelle, mesure préventive, mesure corrective, etc.)

5.5.4 Table des services de sécurité

La table de services de sécurité contient l'information concernant les services ainsi que leur emplacement dans les couches du modèle OSI, que ce soit l'authentification, la confidentialité des données, l'intégrité, etc.

5.5.5 Table des menaces et des vulnérabilités

La table des menaces et vulnérabilités contient les différents types de risques (erreurs humaines, désastres naturels et pannes de systèmes informatiques).

5.5.6 Table des risques associés aux mécanismes de sécurité

À chaque tuple (actif, menace, vulnérabilité) un risque est associé, qui est remédié par une ou plusieurs mesure de sécurité (mécanismes de sécurité). La valeur de probabilité d'occurrence sur un actif est enregistrée dans cette table.

5.5.7 Table des couches OSI

Les mécanismes ou mesures de sécurité techniques sont reliés aux différentes couches OSI à l'aide de cette table.

5.5.8 Table de mécanismes de sécurité

La table de mécanismes de sécurité contient les caractéristiques des mécanismes de sécurités, telles que :

- le domaine d'application : chaque mécanisme de sécurité fait partie d'un domaine d'application;
- le type : deux mécanismes du même type peuvent interagir entre eux;
- la description : la description en texte du mécanisme;
- les mécanismes prédécesseurs (optionnels) : ce sont des mécanismes du même type que le mécanisme courant ;
- les mécanismes successeurs (optionnels) : comme les mécanismes prédécesseurs, ils sont du même type que le mécanisme courant;
- les options;

- les services de sécurités offerts par le mécanisme de sécurité;
- les risques de sécurité résolus par ce mécanisme;
- la couche associée à ce mécanisme de sécurité : couche application, réseau, etc.;
- les participants impliqués : le marchand, le client, la passerelle de paiement, etc.

La figure 5.1 illustre le diagramme de modèle de données de *SecAdvise*.

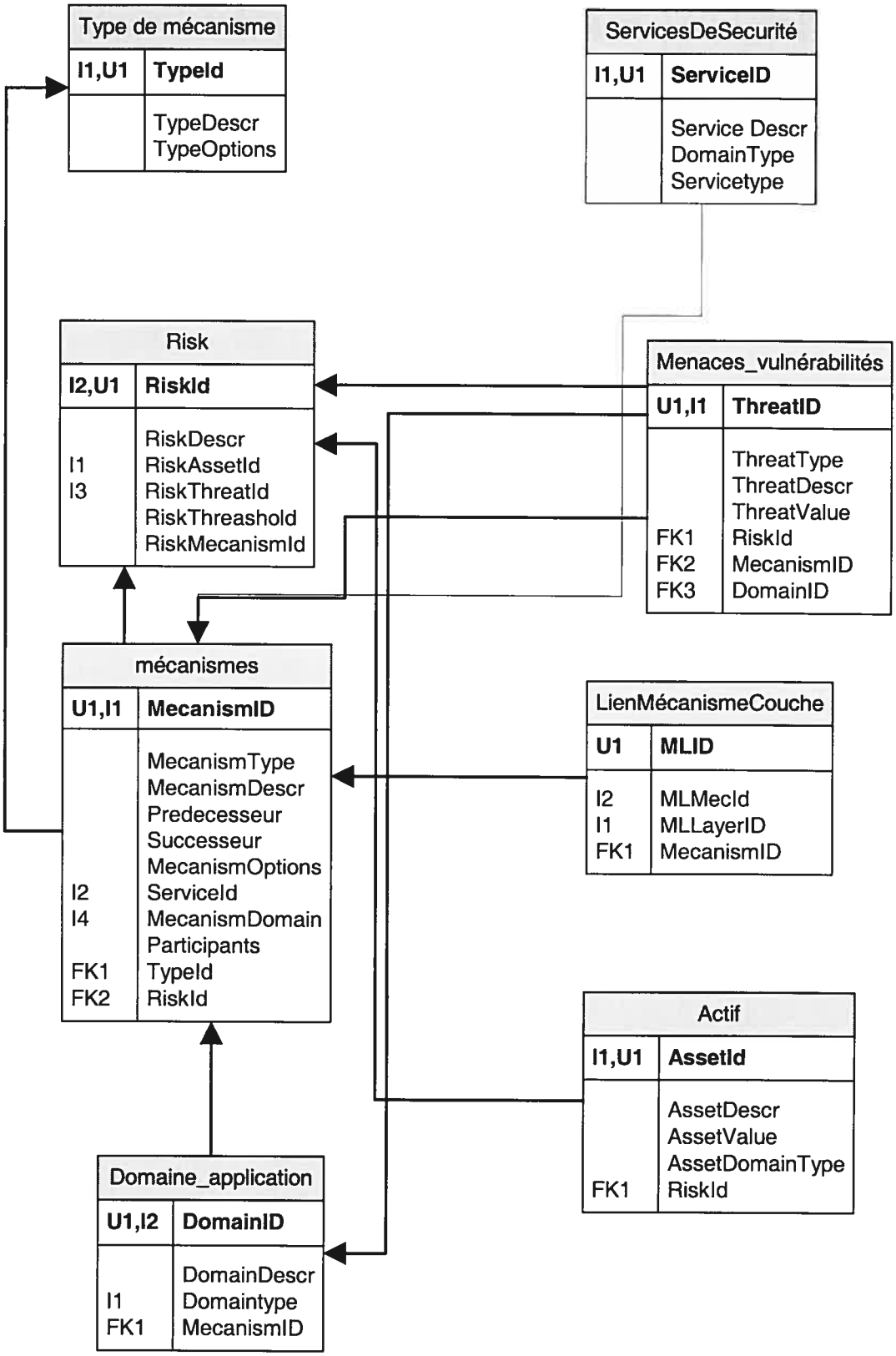

Figure 5.1. MDD Modèle de données de *SecAdvise*

5.6 L'utilisation de *SecAdvise*

Dans cette section, nous testons l'applicabilité de *SecAdvise* sur le protocole de sécurité des paiements SET. Comme décrit dans l'annexe A, la transaction de paiement se décompose en six étapes :

1. PinitReq (*Initiate Request*) du client au marchand ;
2. Pinitres (*Initiate Response*) du marchand au client;
3. PReq (*Purchase Request*) du client au marchand;
4. AuthReq (*Authorization Request*) du marchand à la passerelle de paiement;
5. AuthRes (*Authorizations Response*) de la passerelle de paiement au marchand;
6. PRes (*Payment Response*) du marchand au client.

Ainsi, dans cet exemple nous définissons chaque itération comme étant un mécanisme de sécurité (TU) et les risques *r* associés à chaque itération (TPS), ainsi que les services de sécurité fournis durant chaque itération.

5.6.1 PinitReq (TU1)

TPS1 associé : interception de l'identification de la carte de crédit

Service associé : intégrité des données

5.6.2 PinitRes (TU2)

TPS3 associés : interception de l'information TransId, et les certificats du marchand et du paiement Gatway

Services associés :

- authentification du marchand;
- authentification de la passerelle du paiement;
- intégrité de la TransId.

Mécanisme prédécesseur : PinitReq

Emplacement : couche application

5.6.3 PReq (TU3)

TPS3 associés :

- interception de l'information : paiement et commande;
- vol du numéro de la carte de crédit par le marchand;
- altération des données durant la communication entre le client et le marchand;
- reniement de la commande.

Services associés :

- authentification du client pour la passerelle de paiement;
- intégrité et confidentialité du paiement;
- intégrité et confidentialité de la commande;
- non-répudiation de la commande;
- authenticité des données.

Mécanisme prédécesseur : PinitRes

Emplacement : couche application

5.6.4 AuthReq (TU4)

TPS4 associés :

- divulgation de la description et des prix à la passerelle de paiement;
- interception de l'information : paiement et commande;
- altération des données durant la communication entre le marchand et la passerelle de paiement;
- reniement du paiement (de la part du marchand).

Services associés :

- authentification du client pour la passerelle de paiement;
- authentification du marchand pour la passerelle du paiement;
- intégrité du paiement;
- intégrité et confidentialité de la commande;
- non-répudiation de la demande de paiement (de la part du marchand) ;
- non-répudiation du paiement (de la part du client);
- authenticité des données.

Mécanisme prédécesseur : PReq

Emplacement : couche application

5.6.5 AuthRes (TU5)

TPS5 associés :

- interception de l'information : confirmation sur le paiement;
- altération des données durant la communication entre le marchand et la passerelle de paiement;
- reniement de la confirmation de paiement (de la part de la passerelle).

Services associés :

- intégrité de la confirmation;
- non-répudiation de la confirmation.

Mécanisme prédécesseur : AuthReq

Emplacement : couche application

5.6.6 PRes (TU6)

TPS5 associés :

- interception de l'information : confirmation sur le paiement (de la part du marchand) ;
- reniement de la confirmation de paiement (de la part du marchand).

Services associés :

- non-répudiation de la confirmation.

Mécanisme prédécesseur : AuthRes

Emplacement : couche application

5.7 Conclusion

L'aviseur *SecAdvise* proposé dans ce chapitre est une version préliminaire d'un gestionnaire de risques. En consultant la base de données et en se basant sur l'analyse du risque, le type de mécanisme, le domaine d'application, les participants et les mécanismes disponibles, *SecAdvise* peut sélectionner les mécanismes de sécurité appropriés pour une transaction de commerce électronique. Aussi, les mécanismes prédécesseurs et successeurs sont des critères indispensables pour sélectionner des mécanismes compatibles existants chez les différents participants.

SecAdvise emploie le principe « diviser pour conquérir »; en fait, c'est ce qu'on a essayé de prouver avec SET. Nous supposons que pour chaque risque *r* ou TPS, il existe un ou plusieurs TU qui englobent totalement cet espace de problèmes (TPS). Cependant, cette hypothèse s'est avérée fausse puisqu'il y a corrélation entre plusieurs infrastructures ou mécanismes (par exemple, l'infrastructure PKI et le mécanisme de signature numérique) afin de réduire le risque *r'*, et parce que la même infrastructure est utilisée dans d'autres mécanismes cryptographiques.

Chapitre 6. Conclusion

6.1 En résumé

Le commerce électronique met l'emphase sur la force de la sécurité informatique et le marché des moyens de systèmes de sécurité demeure très fragmenté entre plusieurs solutions incompatibles. Cette situation est intenable à long terme à cause de la difficulté de gestion et des coûts qu'elle impose. Plusieurs approches ont tenté d'unifier les systèmes de sécurité en une seule solution, mais elles sont toujours limitées par le domaine d'application.

Ainsi, dans notre mémoire nous avons présenté une nouvelle approche d'un aviseur de sécurité *(SecAdvise)*, qui fera le travail d'un gestionnaire des risques pour les transactions de commerce électronique dans les différents domaines d'application. *SecAdvise* sélectionne les meilleurs mécanismes ou systèmes de sécurité, quels que soient les risques qui s'imposent sur le système entre les différents partenaires impliqués dans une transaction de commerce électronique. Il fournit une procédure de gestion et de sélection des mécanismes de sécurité associés aux risques qui menacent les systèmes de commerce électronique dans les différents domaines d'application. Pour y parvenir, il s'appuie sur la base de données des différents partenaires et sur la négociation de leurs paramètres de sélection (entre les bases de données locales de chacun des partenaires).

6.2 Discussion et conclusion

Discutons de quelques points que nous n'avons pas pris en considération dans le développement de *SecAdvise* :

- Les fonctions de sécurité s'appuient sur des mécanismes généralement mis en jeu par plusieurs d'entre elles, par exemple la signature numérique, le scellement, les certificats, etc. Ces mécanismes utilisent souvent des fonctions cryptographiques qui sont soumises à des restrictions légales d'usages; celles-ci varient d'un pays à l'autre et posent des problèmes pour les communications internationales. Par conséquent, le but de l'interopérabilité entre différents systèmes n'est atteint que si ce côté législatif est pris en considération.
- L'élaboration d'une infrastructure de sécurité requiert la conception et la mise en œuvre de contrôles administratifs, procéduraux et techniques permettant d'atténuer les risques de sécurité. La mise en oeuvre de *politiques* [Barman 01], *normes et meilleures pratiques saines en matière de sécurité permettra une réduction importante de l'exposition globale aux risques,* tout en témoignant d'un niveau de prudence approprié. Dans [BS779993] et [GMITS97], vous trouverez les codes des meilleures pratiques de la gestion de l'information.
- Malheureusement, *SecAdvise* est de nature statique, ce qui ne suffit pas dans le monde dynamique d'Internet. La technologie évolue rapidement et l'on assiste au déploiement continu de nouveaux systèmes, de connexions et d'applications de réseaux. De plus, on découvre continuellement de nouvelles menaces et vulnérabilités et de nouveaux scripts d'exploitation. Si une organisation n'est pas en mesure de réagir rapidement lorsque se présentent de nouvelles possibilités d'exploitation d'une vulnérabilité, l'exposition aux risques s'accroît de manière significative. Par conséquent, le processus de gestion des risques *SecAdvise* doit inclure un processus permettant de surveiller en permanence la « santé » du réseau et de prendre des mesures appropriées lorsque les risques pour la sécurité changent.

Pour les travaux futurs, il est intéressant d'aborder ces sujets en détail afin de bien englober la sécurité de l'information sous tous ses angles.

En conclusion, le présent mémoire est une tentative de modéliser tous les mécanismes, infrastructures, protocoles et architectures de sécurité dans un même modèle. Ce projet est réalisable à condition de prendre en considération tous les points de vue techniques,

administratifs, législatifs et juridiques influençant les aspects de la sécurité des organisations et d'entreprendre une analyse de risques dynamique comme celle proposée dans OCTAVE (une approche dynamique pour l'évaluation du risque) [Dorofee02].

Il importe de souligner qu'une approche équilibrée est essentielle. Il est difficile de s'assurer que les mécanismes de protection fonctionnent de manière efficace sans la mise en place d'une forme quelconque de protection active de l'information. De plus, la protection efficace de l'information exige la coordination et le partage de l'information en raison de la nature complexe des menaces. À cette fin, on doit pouvoir compter sur une fonction interjuridictionnelle tel un centre de coordination national de protection de l'information.

Bibliographie

[Abad96a] J. Abad Peiro, N. Asokan and M. Waidner, *Payment Manager – Overview*, SEMPER Activity Paper 212ZR054, MARCH 1996, disponible sur *http://www.semper.org/info.*

[Abad96b] J. Abad Peiro, N. Asokan, M. Steiner and M. Waidner, *Designing a generic payment system service*, IBM Research Report RZ 2891, SEPTEMBER 1996, disponible sur *http://www.research.ibm.com/journal/sj/371/abadpeiro.html*,

[Abad98] J. Abad Peiro, N. Asokan, M. Steiner, and M. Waidner, *Designing a generic payment system service*, *IBM Systems Journal*, 37 (1), 72-88, 1998.

[Abdul96] A. AbdulRahman, *The PGP Trust Model*, EDI-Forum, AUGUST 1996, disponible sur *http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/docs/pgptrust.html.*

[Barman01] S. Barman, *Writing Information Security Policies*, New Riders, 1st edition, NOVEMBER 2001.

[Bellare96] M. Bellare, R. Canetti, and H. Lkrawczyk *Keying hash functions for message authentification*, number 1109 in Lecture Notes in Computer Science, pages 1-15, Springer-Verlag, Berlin, 1996.

[BS779993] *British Standard 7799 - A Code of Practice for Information Security Management, and Specification for Information Security Management Systems*, By the British Department of Trade and Industry Commercial IT Security Group with the British Standards Institution, London: BSI-DISK, 1993.

[Burdett00] D. Burdett, *Internet Open Trading Protocol – IOTP Version 1.0*, The Internet Engineering Task Force, APRIL 2000, disponible sur *http://www.ietf.org/internet-drafts/draft-ietf-trade-iotp-v1.0.*

[Davidson99] K. Davidson, and Y. Kawastsura, *Digital Signatures for the v1.0 Internet Open Trading Protocol (IOTP)*, The Internet Engineering Task Force, Internet Draft, NOVEMBER 1999, disponible sur http://www.watersprings.org/pub/id/draft-ietf-trade-iotp-v1.0-dsig-05.txt.

[Doraswamy99] N. Doraswamy, *IPSEC: The New Security Standard for Internet, Intranet and VPN*, Prentice Hall, 1999.

[Dorofee02] A. Dorofee and R. Higuera, *Managing Information Security Risks, the OCTAVE Approach*, Addison Wesley, JUNE 2002.

[Freier96] A. Freier and P. Karlton, *The SSL Protocol version 3.0*, Internet Draft, MARCH 1996, disponible sur http://wp.netscape.com/eng/ssl3/ssl-toc.html.

[GMITS97] *Guidelines for the Management of IT Security*, ISO/IEC TR 13335, (Part 1- *Concepts and Models for IT Security*, Part 2 – *Management and Planning IT Security*, Part 3 – *Techniques for the Management of IT Security*, Part 4 – *Selection of Safeguards*), 1997

[Hassler01] V. Hassler, *Security Fondamentals for E-commerce*, Computer Security Series, Artech House, 2001.

[IOTP00] IOTP – *Internet Open Trading Protocol,* APRIL 2000, disponible sur *http://www.ietf.org/rfc/rfc2801.txt.*

[ISOOSI94] Information technology-open system interconnection – basic Reference model: *The basic model. ISO/IEC Standard 7498-1*, International Organisation for Standardization, 1994.

[Lacoste00] G. Lacoste, B. Pfitzmann, Michael Steiner and Michael Waidner, *SEMPER – Secure Electronic Marketplace for Europe*, number 1854 in Lecture Notes in Computer Science, Springer- Verlag, 2000.

[Marsh94] S. Marsh, *Formalising Trust as a Computational Concept*, PhD. Thesis, university of Stirling, 1994, disponible sur *http://ii35.ai.iit.nrc.ca/~smarsh/Publications.html.*

[Mel01] H. Mel and D. Baker, *La cryptographie décryptée*, Campus Press, France, JULY 2001.

[NSA94] NSA- National Security Agency, The Mosaic Program Office, *Key management concepts* V. 2.52, FEBRUARY 1994, disponible sur *http:www.rbo.com/PROD/rmadillo/f.*

[OBI99] *OBI Technical Specifications Open Buying On The Internet*, V. 2.1, 1999, disponible sur *http://www.openbuy.org/specs/OBIv210.pdf.*

[Peltier01] T. Peltier, *Information Security Risk Analysis*, Auerbach, 1st edition, JANUARY 2001.

[Pfleeger02] C. Pfleeger and S. Pfleeger, *Security In Computing,* Prentice Hall, 3rd edition, DECEMBER 2002.

[Pipkin00] D. Pipkin, *Sécurité des systèmes d'information*, CampusPress, Paris, OCTOBER 2000.

[Rennhard01] M. Rennhard and S. Mathy, *From SET to PSET- The pseudonymous secure electronic transaction protocol*, Technical report number 117, Swiss Federal Institute of Technology, Computer Engineering and Networks Laboratory, AUGUST 2001, disponible sur *http://www.tik.ee.ethz.ch/~rennhard/publications/PSET.pdf* .

[Robles01] S. Robles, S. Poslad, J. Borell and J. 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, Texas, USA, NOVEMBER 2001.

[Rolin95] P. Rolin, *Réseaux de communication et conception de protocoles*, Hermès, Paris, 1995.

[Saliba02] R. Saliba, G. Babin and P. Kropf. Secadvise : *A Security Mechanisme Advisor.* Distributed Communities on the Web (DCW 2002), Sydney, Australia, LNCS 2468, Springer, Berlin, pages 35–40, APRIL 2002.

[SANS03] SANS, *Acceptable Encryption Policy*. Internet Draft, 2003, disponible sur *http://www.sans.org/resources/policies/Acceptable_Encryption_Policy.doc*.

[SET02] *SET - Secure Electronic Transaction Specification, Book1: Business Description, Book 2: Programmer's Guide, Book 3: Format Protocol Definition*, disponible sur *http://www.setco.org/set_specifications.html*, 2003.

[Sherif00] M. Sherif and A. Serhrouchni, *La Monnaie Électronique- Systèmes de paiement sécurisé*, Eyrolles, 2000.

[Steedman93] D. Steedman, *Abstract Syntax Notation One ASN.1: The Tutorial and reference*, Technology Appraisals, Twickenham, UK, 1993.

[Tanenbaum96] A. Tanenbaum, *Computer Networks*, 3rd edition, Prentice Hall, (traduction française 1998), APRIL 1996

[W3Csecurity] *World Wide Web Consortium Security,* disponible sur *http://www.w3.org/Security*, JUNE 1999.

[W3CXML98] World Wide Web Consortium XML, Working Group, *Extensible Markuo Language (XML) 1.0*, W3C Recommendation, disponible sur *http://www.w3.org/TR/REC-xml*, FEBRUARY 1998.

Annexe A. Scénarios des transactions de SET

Cette annexe donne les scénarios des transactions de SET [Rennhard01].

SET utilise la cryptographie à clé publique pour assurer la sécurité des transactions. Le détenteur de la carte, le marchand et la passerelle de paiement sont impliqués dans le protocole SET. Chacun d'eux possède un ou plusieurs certificats ou paires de clés.
La figure 1 illustre l'infrastructure des clés publiques de SET.

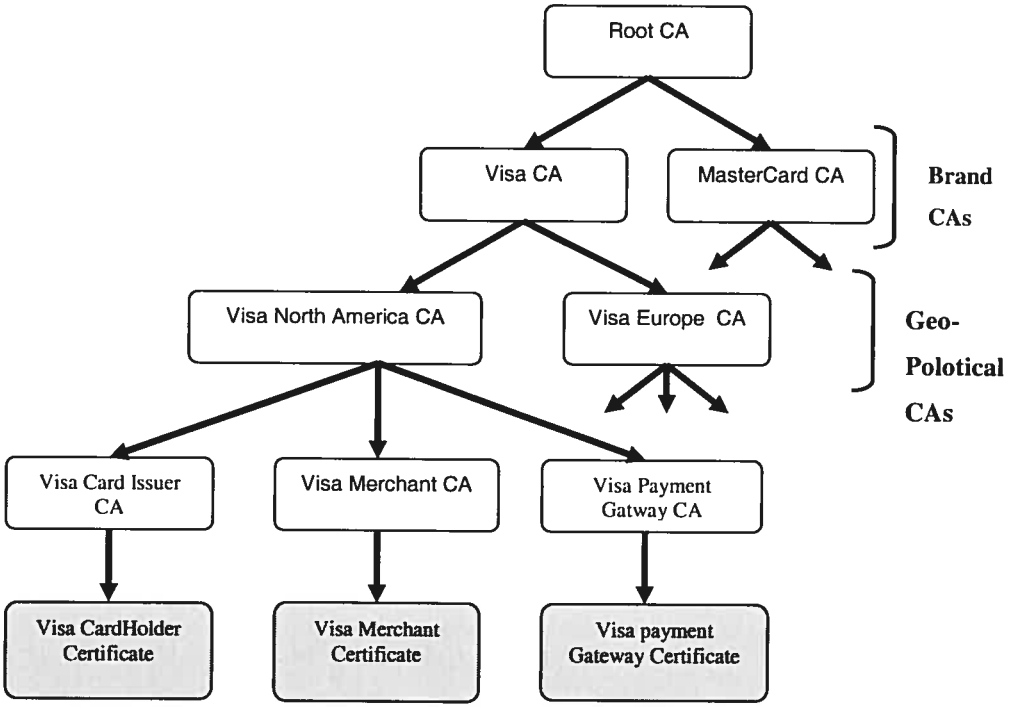

Figure 1. Hiérarchie de la gestion des certificats

L'autorité de certification maîtresse CA (Certification Authority) est une entité qui trône sur tout l'édifice de certification de SET. Elle est chargée d'émettre des certificats pour les autorités de certification de la marque, telles que Visa, MasterCard et American Express. Chaque autorité de certification (CA) de la marque peut émettre des certificats pour les autorités de certification régionales.

La figure 1. contient deux AC régionales de Visa, une pour l'Europe et l'autre pour l'Amérique du Nord. À leurs tours, les autorités de certification régionales émettent des certificats pour l'AC des détenteurs de la carte. L'AC des détenteurs de la carte est associée à une compagnie qui émet des cartes de crédits. Ces AC des détenteurs de la carte émettent à leur tour des certificats pour les détenteurs de la carte. Les AC régionales certifient aussi les marchands et les passerelles de paiement. Ce qui signifie qu'il n'y a pas uniquement les certificats des détenteurs de la carte qui sont liés à une marque de carte spécifiée, ceux des marchands et des passerelles de paiement le sont aussi. Par conséquent, les marchands et les passerelles de paiement possèdent une paire de certificats (l'un pour la signature et l'autre pour l'échange des clés) pour chaque marque de carte de crédit acceptée.

Le tableau 1 liste les certificats qui sont utilisés dans le protocole SET. $Cert_{S,X}$ identifie le certificat de signature de la partie X, tandis que $PrK_{S,X}$ et $PuK_{S,X}$ identifient les clés privé et publique correspondantes. De même, $Cert_{KE,X}$ identifie le certificat d'échange des clés de la partie X, tandis que $PrK_{KE,X}$ et $PuK_{KE,X}$ identifient les clés privé et publique correspondantes.

Notons que le détenteur de la carte possède une seule paire de clés, avec le certificat correspondant à la carte. Le marchand et la passerelle de paiement possèdent deux paires de clés avec les certificats correspondants pour chaque marque de carte de crédit qu'ils emploient.

Tableau 1: Certificats et clés

Participants	Certificats ou clés pour la signature	Certificats ou clés pour l'échange des clés
Détenteur de la carte (par carte de crédit)	$Cert_{S,C}$; $PrK_{S,C}$,$PuK_{S,C}$	
Marchand (par la marque de la carte de crédit)	$Cert_{S,M}$; $PrK_{S,M}$,$PuK_{S,M}$	$Cert_{KE,M}$; $PrK_{KE,M}$,$PuK_{KE,M}$
Passerelle de paiement PG (Payment gateway) (par la marque de la carte de crédit)	$Cert_{S,PG}$; $PrK_{S,PG}$,$PuK_{S,PG}$	$Cert_{KEPG}$; $PrK_{KE,PG}$,$PuK_{KE,PG}$

Les phases du protocole dans SET

Le Protocole SET est compose de plusieurs phases illustrées dans la figure 2.

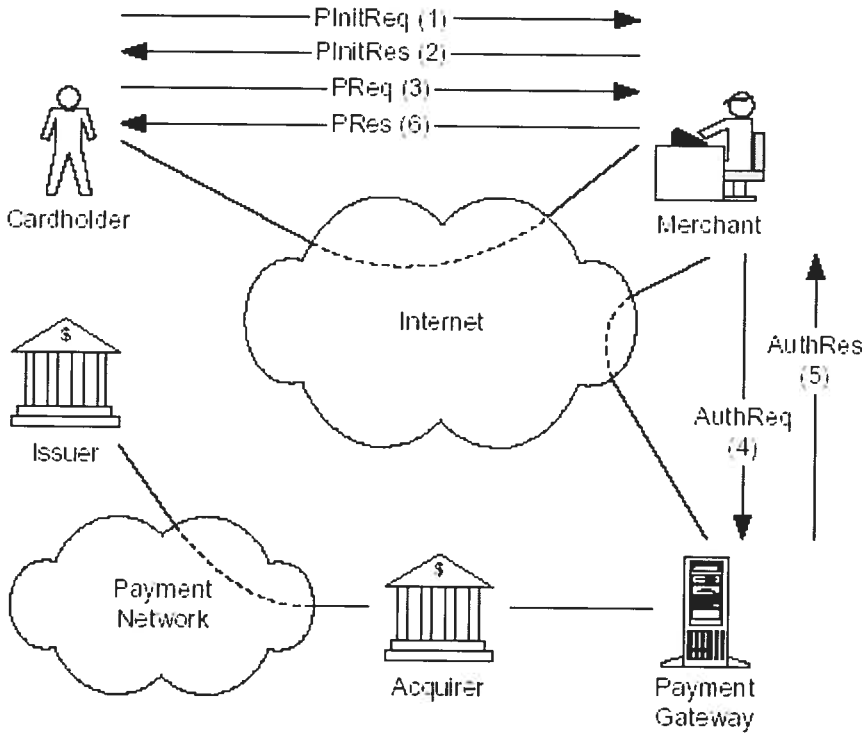

Figure 2. Participants dans SET

1. Quand le détenteur de la carte (cardholder) a terminé son magasinage et désire initier un paiement avec SET, il envoie un message **Initiate Request (PInitReq)** au marchand.
2. Le marchand répond avec un message **Initiate Response (PInitRes).**
3. Le processus de paiement actuel commence quand le détenteur de la carte envoie un message **Purchase Request (PReq)** au marchand.
4. Le marchand initie l'autorisation de paiement en envoyant un message **Authorization Request (AuthReq)** à la passerelle de paiement.

5. Quand la passerelle de paiement complète l'autorisation du paiement via l'institut d'acquisition, elle répond par un message **Authorization Response (AuthRes)** au marchand.

6. Le marchand envoie un message **Purchase Response (PRes)** message au détenteur de la carte.

Puisque nous sommes concernés essentiellement par le processus de paiement et son autorisation, nous regarderons les phases 1 à 4 en détail.

Initiate Request (PInitReq)

Avant que cette phase commence, le détenteur de la carte a complété la sélection des produits et reçoit une description de la commande *Order Description (OD)* présentés par le marchand. Cette description est une liste des produits choisis avec leurs prix, mais le format de ce OD n'est pas standardisé par SET. Notons aussi que la présentation de OD n'est pas une partie du protocole SET. Le tableau 2 spécifie la description de la commande (OD).

Tableau 2: *Order Description (OD)*

OD	La description de la commande, générée par le marchand et envoyée au client.

Éventuellement, le détenteur de la carte informe le marchand qu'il veut initier le paiement, en envoyant un message PInitReq au marchand. Le message contient un BrandID spécifiant la marque de la carte de crédit. Le tableau 3 décrit le message PInitReq.

Ce message est envoyé au marchand. Quand le marchand reçoit le message, il :

- Examine le BrandID et vérifie s'il accepte cette marque de carte de crédit.

Tableau 3: *The Initiate Request message (PInitReq)*

PinitReq	**BrandID**
BrandID	Un identificateur ID spécifiant la marque de la carte de crédit

Initiate Response (PInitRes)

Dans cette phase, le marchand répond à la demande du détenteur de la carte. Le marchand choisit un unique identificateur de transaction *Transaction ID (TransID)* qui sera utilisé durant toute la transaction pour des buts d'identification. Le marchand envoie aussi son certificat pour la signature et le certificat d'échange des clés de la passerelle de paiement. Le message est signé par le marchand. Les deux certificats doivent correspondre à la marque de la carte de crédit spécifiée par l'utilisateur dans son message PInitReq (tableau 3). Le tableau 4 spécifie le message PInitRes.

Tableau 4: *The Initiate Response message (PInitRes)*

PinitRes	**Sign**$_{PrKS.M}$ (Trans Id), Cert$_{S,M}$, Cert$_{KE,PG}$;
TransID	Un ID spécifiant toute la transaction
Cert$_{S,M}$	Le certificat de signature du marchand (tableau 1) correspondant à la marque de la carte de crédit spécifié par le détenteur de la carte (tableau 3)
Cert$_{KE,PG}$	Le certificat d'échange des clés de la passerelle de paiement (tableau 1) correspondant à la marque de la carte de crédit spécifiée par le détenteur de la carte (tableau 3)

Quand le détenteur de la carte reçoit ce message, il :

1. vérifie si le certificat de signature de marchand (Cert$_{S,M}$) est valide, si c'est vraiment le certificat du marchand, et si c'est le bon certificat pour la bonne marque de carte de crédit.
2. vérifie si le certificat de l'échange de clés de la passerelle de paiement (Cert$_{KE,PG}$) est valide, et si c'est le bon certificat pour la bonne marque de carte de crédit.
3. vérifie la signature du marchand. Si la signature a été vérifiée correctement, le détenteur de la carte de crédit pourra s'assurer que le message est généré par le marchand.

Quand cette phase est complétée, le détenteur de la carte commence le processus du paiement.

Purchase Request (PReq)

Pendant cette phase, le détenteur de carte génère l'information nécessaire pour le marchand et la passerelle de paiement. L'information se compose de deux parties, l'une est pour le marchand et l'autre est pour la passerelle passage de paiement. Dans la première étape, les données de l'information de la commande *Order Information Data (OIData)* (le tableau 6) sont créées, qui contiennent l'information pour le marchand. OIData ne contient pas un lien direct à l'OD (tableau 2), mais contient une valeur hachée. La description de la commande hachée *the Hashed Order Description (HOD)*, comme une référence au HOD, OD est décrite dans le tableau 5.

Tableau 5: *The Hashed Order Description (HOD)*

HOD	**Hash(OD, PurchAmt, ODSalt)**
OD	Les informations de la commande (tableau 2)
PurchAmt	Le montant de la transaction
ODSalt	Un *nonce* pour empêcher les attaques du type dictionnaire sur HOD

Tableau 6: *The Order Information Data (OIData)*

OIData	**TransID, HOD, ODSalt, BrandID**
TransID	L'ID identifiant la transaction entière
HOD	Le *hash* appliqué sur OD (tableau 5)
ODSalt	Le *sel utilize* dans HOD (tableau 5)
BrandID	Un ID spécifiant la marque de la carte de crédit à utiliser

Le HOD est maintenant utilisé dans OIData. Le tableau 6 décrit l'information incluse dans OIData. Le client calcule également d'information hachée (Hashed) d'OIData, *Hashed Order Information Data (HOIData)*, qui est utilisée plus tard. Le tableau 7 décrit HOIData.

Tableau 7: *The Hashed Order Information Data (HOIData)*

HOIData	Hash(OIData)
OIData	Les données de l'information de la commande (tableau 6)

De même, le détenteur de carte génère des données de l'information de paiement *Payment Information Data* (PIData) pour la passerelle de paiement.
Le tableau 8 définit PIData.

Tableau 8: *The Payment Information Data (PIData)*

PIData	TransID, HOD, PurchAmt, MerchantID, CC
TransID	Le ID identifiant la transaction entière
HOD	Le parasite sur OD (tableau 5)
PurchAmt	Le montant de la transaction
MerchantID	Un ID identifiant le marchand (extrait de $Cert_{S,M}$)
CC	Données identifiant la carte de crédit du détenteur (tel que le numéro de la carte de crédit)

Le client calcule également l'information hachée sur PIData, le hachage des données de l'information de paiement, *Hashed Payment Information Data* (HPIData). Ceci est utilisé plus tard. Le tableau 9 décrit HPIData.

Tableau 9: *The Hashed Payment Information Data (HPIData)*

HPIData	Hash(PIData)
PIData	Les données de l'information de paiement (tableau 8)

Pour lier l'OIData et le PIData, le détenteur de carte calcule une signature duelle sur OIData et PIData. La signature duelle est fondamentalement une signature au-dessus des informations parasites de la concaténation de HOIData (tableau 7) et HPIData (tableau 9).
Le tableau 10 décrit comment la signature duelle est définie.

Tableau 10: *The Dual Signature (DS)*

DS	$Sign_{PrKS,M}$ (Hash(HOIData, HPIData))
HOIData	Les données de l'information de la commande hachées (tableau 7)
HPIData	Les données de l'information de paiement hachées (tableau 9)

Il est pratique de récapituler toute l'information que le marchand expédiera à la passerelle de paiement plus tard comme information de paiement *Payment Information (PI)*. Ceci est décrit dans le tableau 11.

Notez que *PI* contient PIData, mais PIData est chiffré pour la passerelle de paiement. Ceci signifie que le marchand ne voit pas la carte de crédit du détenteur (incluse dans OIData). C'est un grand avantage pour les paiements par carte de crédit sur Internet.

Tableau 11: *The Payment Information (PI)*

PI	$E_{KC,PG}$ (PIData, HOIData), $E_{PuKKE,PG}(K_{C,PG})$, DS
$E_{KC,PG}$ (PIData, HOIData)	Le PIData (tableau 8) plus HOIData (tableau 7), encryptés avec la clé symétrique jetable $K_{C,PG}$
$E_{PuKKE,PG}(K_{C,PG})$	La clé symétrique jetable $K_{C,PG}$,encryptée avec la clé publique des clés d'échange de la passerelle de paiement $PuK_{KE,PG}$
DS	La signature duelle (tableau 10)

Le client est maintenant prêt à produire la totalité du message de demande d'achat. Le tableau 12 définit comment PReq est construit.

Tableau 12: *The Purchase Request message (PReq)*

Preq	OIData, HPIData, PI, $Cert_{S,C}$
OIData	Les données de l'information de la commande (tableau 6)
HPIData	Les données de l'information de paiement hachées (tableau 9)
PI	L'information de paiement pour la passerelle de paiement (tableau 11)
$Cert_{S,C}$	Le certificat du client pour la signature

Ce message est envoyé au marchand. Quand le marchand reçoit PReq, il exécute les étapes suivantes:

1. Examine si le certificat de la signature pour le détenteur ($Cert_{S,C}$) est valide.
2. Applique la clé publique du détenteur sur la signature duelle DS (contenu dans PI), et compare le résultat à la valeur hachée (Hash(OIData), HPIData) (en utilisant OIData et HPIData de PReq). Si les deux valeurs sont égales, alors la signature a été faite par le client et OIData n'a pas été changé en transfert.
3. Vérifie si TransID dans OIData correspond à une identification de transaction déjà demandée. Si cet essai est correct, alors le marchand sait que ce paiement correspond à un paiement précédemment lancé.
4. Vérifie si BrandID dans le certificat du détenteur de carte correspond à BrandID indiqué dans PInitReq (tableau 3) et OIData.
5. Compare le HOD à une version générée individuellement basée sur l'OD stockée localement, sur PurchAmt, et l'ODSalt d'OIData. Si cet essai est correct, alors le marchand sait que le détenteur de carte paye en effet l'ordre convenu plus tôt (indiqué dans l'OD) et qu'il paye le montant correct.

Notons que le marchand saura maintenant que le détenteur de carte a en effet généré un authentique et valide OIData qui appartient à un OD précédemment indiqué. Le marchand n'a aucune idée si l'information chiffrée de paiement pour la passerelle de paiement contient des données valides. Au moment où nous discuterons de la validation à la passerelle de paiement, nous verrons que la signature duelle lie en effet le paiement à l'ordre, mais ceci peut seulement être vérifié par la passerelle de paiement. Pour le marchand, c'est une authentification pure (et un contrôle d'intégrité) de la commande du détenteur de carte.

Authentication Request (AuthReq)

Dans cette étape, le marchand demande à la passerelle de paiement de valider le paiement. Fondamentalement, le marchand expédie l'information de paiement (PI) reçue du détenteur de carte dans le message de PReq, mais le marchand inclut également une

charge utile de demande d'autorisation *Authorization Request Payload (AuthReqPayload)*, comme décrit dans le tableau 13.

Tableau 13: *The Authorization Request Payload (AuthReqPayload)*

AuthReqPayload	**TransID, AuthReqAmt, HOIData, HOD**
TransID	L'ID identifiant la transaction entière
AuthReqAmt	Le montant que le marchand va charger sur la carte de crédit du détenteur
HOIData	Le hachage sur OIData (tableau 6); calculé indépendamment par le marchand
HOD	Le hachage sur OD (tableau 2); calculé indépendamment par le marchand

Cet AuthReqPayload est envoyé ensuite à la passerelle de paiement dans un message *Authorization Request (AuthReq)* avec d'autres informations. Ceci est décrit dans le tableau 14.

Tableau 14: *The Authorization Request message (AuthReq)*

AuthReq	$\mathbf{E_{K_{M,PG}}}$ **(Sign**$_{PrK_{S,M}}$ **(AuthReqPayload)),** $\mathbf{E_{PuK_{KE,PG}}(K_{M,PG})}$**, PI,** $\mathbf{Cert_{S,C}}$**,** $\mathbf{Cert_{S,M}}$
$\mathbf{E_{K_{M,PG}}}$ **(Sign**$_{PrK_{S,M}}$ **(AuthReqPayload))**	L'AuthReqPayload signé (tableau 13), encrypté par la clé symétrique jetable $K_{M,PG}$
$\mathbf{E_{PuK_{KE,PG}}(K_{M,PG})}$	Clé symétrique jetable $K_{M,PG}$, encryptée par la clé publique des clés d'échange $PuK_{KE,PG}$ de la passerelle de paiement
PI	L'information de paiement du détenteur de la carte (tableau 11)
$\mathbf{Cert_{S,C}}$	Le certificat de signature du détenteur de carte
$\mathbf{Cert_{S,M}}$	Le certificat de signature du marchand

Quand la passerelle de paiement reçoit l'AuthReq, elle exécute les étapes suivantes:

1. Elle examine si le certificat de signature du détenteur de carte ($Cert_{S,C}$) est valide.
2. Elle examine si le certificat de signature du marchand ($Cert_{S,M}$) est valide.

3. Elle extrait la clé symétrique jetable $K_{M,PG}$ et l'utilise pour décrypter le AuthReqPayload.
4. Elle vérifie si la signature du marchand sur AuthReqPayload est authentique.
5. Elle extrait la clé symétrique jetable $K_{C,PG}$ et l'utilise pour extraire PIData et HOIData de PI.
6. Elle vérifie si TransID dans AuthReqPayload correspond à TransID dans PIData. S'ils sont identiques, alors le détenteur de carte paye en effet la transaction que le marchand a demandée. La passerelle de paiement vérifie également que l'AuthReqAmt dans AuthReqPayload est identique à PurchAmt dans PIData, ce qui assure l'exactitude du montant payé.
7. Elle applique la clé publique du détenteur de carte sur la signature duelle DS (contenu dans PI), et compare le résultat à la valeur Hash(HOIData, Hash(PIData)) (en utilisant HOIData et PIData contenus dans PI). Si les deux valeurs sont égales, alors la signature a été faite par le détenteur de carte et PIData n'a pas été changé en transition.
8. Elle compare le HOIData reçu du détenteur de carte (dans PI) et du marchand (dans l'AuthReqPayload), ce qui assure que le paiement appartient en effet à l'information de la commande envoyée du détenteur de carte au marchand.

Notez que si le marchand vérifie la signature duelle et que la signature est authentique, alors il n'est pas possible que le détenteur de carte fournisse une paire différente de PIData/HOIData qui est identique à la signature duelle.

Par conséquent, ce contrôle additionnel par la passerelle de paiement assure que le lien de l'ordre au paiement est garanti même lorsque le marchand ne vérifie pas la signature duelle ou que la signature duelle n'est pas utilisée.

9. Elle compare le HOD reçu du détenteur de carte (dans PI) et du marchand (dans AuthReqPayload). C'est nécessaire si le négociant ne peut pas vérifier le HOD dans OIData (Ceci pourrait se produire dans le cas où les données appropriés envoyées par le marchand ne sont pas reçues).
10. Elle vérifie si le MerchantID dans PIData est identique à MerchantID dans le certificat de signature du marchand. Ceci garantit que les négociants ne peuvent pas employer les informations de paiement prévues pour un autre marchand.

11. La passerelle de paiement utilise le CC et le PurchAmt de PI pour autoriser le paiement par les réseaux financiers existants de la carte de paiement.

Authentication Response (AuthRes)

Ce message est envoyé de la passerelle de paiement au marchand. Il contient le TransID et les informations sur l'autorisation du paiement. Il contient également un jeton de capture qui peut être employée par le marchand pendant la capture de paiement. Le message est signé et chiffré pour le marchand.

Purchase Response (PRes)

Ce message est envoyé du marchand au détenteur de carte pour l'informer que l'achat a été autorisé et s'est donc accompli ou pas. Le message contient le TransID et est signé par le négociant.

Annexe B. Liste des ressources et actifs

Les inventaires des actifs permettent d'assurer une protection efficace des actifs. Le processus de compilation d'un inventaire des actifs constitue un aspect important de la gestion des risques. Une organisation doit être capable d'identifier ses actifs de même que la valeur et l'importance relatives de ces actifs. En se basant sur ces informations, une organisation peut alors fournir des niveaux de protection qui correspondent à la valeur et à l'importance des actifs. Ils convient d'identifier clairement chaque actif et de parvenir à un accord concernant son propriétaire et sa classification de sécurité; il convient d'identifier aussi son emplacement (ce qui est important lorsqu'on essaie de le récupérer en cas de perte ou de dommage).

On peut donner comme exemples des actifs associés à des systèmes d'information les éléments suivants :

1. Actifs information: bases de données et fichiers de données, documentation du système, manuels de l'utilisateur, documents de formation, procédures opérationnelles ou de soutien, plans de continuité, dispositions de substitution, informations archivées;
2. Actifs logiciels : logiciels système, outils de développement et utilitaires;
3. Actifs physiques : matériel informatique (processeurs, moniteurs, ordinateurs portables, modems), matériel de communication (routeurs, PABX, télécopieurs, répondeurs), supports magnétiques (cassettes et disques), autres équipements techniques (dispositifs d'alimentation, unités de climatisation), meubles, espace de travail;
4. Services : services informatiques et de communication, commodités générales (par exemple chauffage, éclairage, alimentation électrique, climatisation)

L'exemple suivant rentre dans plus de détails de chacun des éléments mentionnés auparavant.

Code	Category
I	Information
S	Services
D	Documents
A	Arrangements and procedures
SP	Software and programs
H	Hardware
M	Media
C	Connections and communications
B	Building and equipment
P	Personnel
O	Organisation and reputation

Resource/Asset List	
I	Financial information
I	Sales/marketing information
I	Payment details
S	Information services
S	Communication services
I	Contract details
I	Training material
A	Backup procedures
A	Incident handling procedures
SP	Operating system software
SP	Test programs
SP	Communications software
H	Computing resources
H	Networks
H	Computer
M	CD-ROMS
M	Tapes
C	Cables
C	Switches
C	Firewalls
C	Mobile (cellular) phones
B	Network management centre
B	UPS
P	Managers
P	Temporary personnel

Annexe C. Document d'analyse de risques

Afin de bien déterminer et évaluer les risques auxquels les systèmes pourraient être exposés, les tâches suivantes doivent être exécutées :

1. Définir et évaluer (*impact value*) les actifs (*asset*) et renseignements des systèmes d'information à l'étude
2. Définir les menaces (*threats*) potentielles, qu'elles soient de nature délibérée ou accidentelle, auxquelles ces actifs et renseignements sont exposés
3. Analyser les conséquences ou incidences des menaces potentielles et évaluer la probabilité d'occurrence de ces menaces
4. Déterminer les vulnérabilités (*vulnérabilities*) du système à la lumière d'une analyse des mesures de sécurité existantes ou proposées
5. Évaluer le niveau de risque de chaque actif ou renseignement d'importance critique jugé vulnérable et exposé à des menaces spécifiques.
6. déterminer des mesures de protection proposées (proposed safeguard) et leurs pertinences

Un document de travail contenant toute cette structure pour l'analyse de risque est indispensable. Le document suivant concrétise les concepts de l'analyse de risque en offrant la possibilité de rentrer toutes les données touchant l'analyse de risque.

Risk Analysis Document		
Version 1.0	Date:	Page1 of 1
Prepared By	Confirmed By	
Rima Saliba		

No	Asset name	Impact value	Vulnerabilities	Threats	Prob.	Risk	Proposed safeguard
Informational Assets							
1	User information Database	3	Necessary for Login	Someone will delete it	3	9	Owned by administrator
				Someone will modify it	3	9	
				Someone will learn its content	3	9	One way encryption
				Users will forget their personal information	4	12	Administrator during whole work time
2	Software licences	3	Necessary while system maintenance (online help, upgrades…)	Loosing/ destroyin	2	6	Store in specific place
							Make copies
4	Information Security System documentation	4	Necessary for correct system work	Loosing/ destroyin	3	12	Store in specific place
				Following inappropriate procedures	3	12	Make copies