Chapitre 4
Protocoles de sécurisation du paiement en ligne

1. Introduction

L'enjeu du commerce électronique est celui d'acquérir la confiance des consommateurs pour développer ce marché. En revanche, la confiance en matière de transactions électroniques transite principalement par la sécurité du mécanisme de paiement. Deux vulnérabilités méritent en particulier d'être soulignées :

- La vérification de l'identité des parties impliquées dans les transactions car l'absence d'identification forte et mutuelle crée des risques de fraudes,
- La protection de l'ordinateur personnel des clients : celui-ci est généralement peu protégé contre les tentatives externes de piratage.

Le manque de sécurité des instruments de paiement constitue un frein à la décision d'achat sur Internet. C'est la raison pour laquelle des protocoles de paiement sécurisé sont mis en place.

2. Les protocoles du paiement sécurisé

Les protocoles de sécurité établissent des mécanismes de communication qui garantissent la confidentialité des données. Il existe plusieurs protocoles mais nous allons nous intéresser ici à trois protocoles particulièrement reconnus.

- **Le protocole SSL (Secure Sockets Layers)** : consiste au cryptage des informations sensibles pour les rendre incompréhensibles de ceux qui ne disposent pas des éléments nécessaires pour les décrypter. Dans ce cas, lors d'un paiement sécurisé les informations bancaires du client parviennent directement au marchand sous forme cryptées.
- **Le protocole SET (Secure Electronic Transactions)** : utilise le protocole SSL avec en plus la particularité d'identifier de manière précise le détenteur de la carte de crédit. De plus, ce protocole confie la gestion de la transaction entre le vendeur et l'acheteur à un intermédiaire (comme une banque par exemple). Ceci a l'avantage d'éviter au consommateur de communiquer au site marchand, son numéro de carte bancaire. Un mécanisme de paiement sécurisé confié à un tiers est apprécié également par le vendeur car ce procédé le dégage de toute responsabilité en cas de piratage de ces bases de données puisqu'il n'a accès à aucun moment aux données bancaires du client.
- **Le protocole SSL via un organisme bancaire** est un compromis entre les deux protocoles précédents : la gestion des paiements se fait via l'Extranet proposé par la banque et l'acheteur envoie ainsi directement ses informations bancaires sur le site de la banque du marchand. Le marchand ne voit jamais transiter les numéros de carte bancaire et informations associées. Ce en quoi il ressemble au protocole SET. Mais il lui reste toujours une faille par apport à ce dernier, c'est que le marchand n'a aucune garantie concernant l'identité du client car l'utilisation de certificats électroniques permettant d'identifier aussi le client et pas seulement le marchand n'est pas pris en compte par SSL.

3. Les procédés du paiement sécurisé

Nous décrivons dans cette section les procédés techniques utilisés par ces protocoles, pour garantir et assurer la fiabilité des transactions.

Les procédés permettant de garantir la sécurité transactionnelle lors des paiements électroniques doivent apporter quatre garanties principales aux utilisateurs (marchands comme clients) :

- L'authentification,
- L'intégrité des données,
- La non-répudiation, et
- La confidentialité.

Toutes ces garanties ne peuvent être apportées que par la combinaison de plusieurs procédés.

Concrètement, la **confidentialité** consiste en un **cryptage/décryptage** des données échangées par le navigateur de l'internaute et le serveur du marchand. Lorsque cette sécurité existe, le navigateur impliqué dans cette opération peut en informer l'internaute en affichant, le plus souvent, l'icône d'un cadenas fermé qui indique également la taille de la clé de cryptage utilisée. Cette icône étant produite par le navigateur, il n'existe pas de faille connue permettant de la falsifier : elle est le reflet exact de la sécurité transactionnelle utilisée pendant l'échange des données de la page en cours. Il est donc possible à tout internaute de vérifier le niveau de sécurité d'un site simplement avec son navigateur.

Mais à la cryptographie, se joignent d'autres procédés permettant d'identifier avec plus de précision et de fiabilité les interlocuteurs c'est **la signature numérique** et **la certification**.

Nous étudierons donc dans cette partie la cryptographie qui est le socle de tous procédés de sécurité car elle est garante de la confidentialité mais aussi, la signature numérique et la certification qui la complète pour garantir les 3 autres critères d'une transaction sécurisée.

3.1. La cryptographie (rappels de la matière cryptologie-I)

Crypter une information revient à la rendre incompréhensible par ceux qui ne possèdent pas le procédé de décodage. C'est un procédé mathématique à la base mais qui est utilisé en informatique sur les réseaux non sécurisés comme Internet, pour crypter les messages, afin qu'aucune personne autre que le destinataire ne puisse les lire. Le dialogue se passe alors ici entre les machines. Le décryptage qui est l'opération inverse permet au destinataire du message de déchiffrer le message qui lui est destiné. Le schéma de la figure 1 illustre ce mécanisme:

Fig. 1 : Mécanisme de cryptage et décryptage

Le processus de cryptage et de décryptage nécessite l'utilisation de deux outils :

- Un algorithme de cryptographie ou un chiffrement qui est une fonction mathématique.
- Une clé (un mot, un nombre ou une phrase) qui associé à cet algorithme va crypter le texte ou le décrypter.

La notion de clé

Une clé est une valeur utilisée dans un algorithme de cryptographie, afin de générer un texte chiffré. Les clés sont en réalité des nombres extrêmement importants, concrètement c'est une suite de bits qui forme un nombre. La taille d'une clé se mesure en bits et plus la taille des clés est importante plus elle est sécurisée. Actuellement, la réglementation fixe la taille maximale des clés à 128 bits. Il faut noter qu'en deçà de ce nombre une clé est considérée comme vulnérable car plus il y a de bits, plus le nombre est grand, plus la tâche du pirate sera longue : il devra tester, un par un, toutes les combinaisons possibles jusqu'à trouver le nombre qui décrypte le message protégé.

L'opération n'est donc pas complexe : elle demande seulement du temps et de la puissance informatique. En effet, si pour casser une clé de 40 bits, il faut tester 240 combinaisons, soit quelques 1 099 milliards de possibilités, pour casser une clé de 128 bits, c'est 2128 combinaisons qu'il s'agit de tester : Aucun cas de cassage d'une clé de 128 bits n'a été révélé et le défi reste les clés de 64 bits pour les pirates.

→La sécurité des données cryptées repose donc entièrement sur deux éléments :

1) L'invulnérabilité de l'algorithme de cryptographie (algorithme difficile à retrouver)
2) La confidentialité de la clé

Une seule clé peut être utilisée pour crypter et décrypter. Dans ce cas le destinataire communique la clé aux destinataires pour qu'il puisse décrypter son message. C'est la cryptographe à clé privée ou à clé symétrique.

3.1.1. La cryptographie à clé privée ou symétrique

Dans ce cas, la clé doit être gardée secrète car elle permet de crypter et décrypter le message. Si elle est interceptée, le système s'écroule. Voici une illustration de son mécanisme en figure2 :

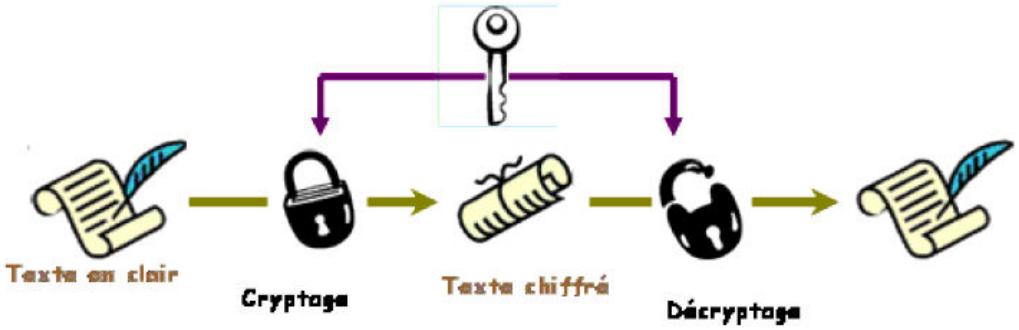

Fig. 2 : Mécanisme de la cryptographie à clé privée

Utilité et limites

Le cryptage conventionnel à clé privée comporte des avantages car il est très rapide. De plus, il s'avère particulièrement utile pour les données véhiculées par des moyens de transmission sécurisés. En effet comme on le voit dans le paragraphe suivant, il peut entraîner des coûts importants en raison de la difficulté à garantir la confidentialité d'une clé de cryptage lors de la distribution notamment sur les réseaux insécurisés comme Internet.

La clé privée doit être distribuée de façon confidentielle à tous les destinataires des messages pour qu'il puisse les décrypter. Cette contrainte soulève plusieurs problèmes :

● Les risques de détournement de cette clé lors de sa distribution au destinataire notamment dans le cas de milliers de navigateurs et d'un serveur qui échange leurs clés sur le réseau Internet pour crypter et décrypter leurs dialogues.

● Pour assurer la confidentialité, chaque expéditeur devrait fournir une clé différente, à chaque destinataire avec lequel il entend communiquer. Autrement chaque destinataire potentiel serait capable de lire tous les messages, qu'ils lui soient destinés ou non.

● Une autre limite du chiffrement avec une clé secrète est l'incapacité de cette méthode d'assurer la non-répudiation. Étant donné que les deux parties ont la même clé, l'une d'entre elles peut créer un message avec la clé secrète partagée et soutenir que le message a été émis par l'autre partie.

S'il est utilisé seul, le chiffrement avec une clé secrète ne convient donc pas au commerce électronique c'est la raison pour laquelle la cryptographie à clé publique, utilisée dans les protocoles de paiement électronique a vu le jour.

3.1.2. Cryptographie à clé publique ou asymétrique

La cryptographie à clé publique utilisée par les protocoles SSL et SET est un procédé asymétrique utilisant une paire de clés pour le système de cryptage, dont l'une sert à chiffrer les messages et l'autre à déchiffrer les messages ou vice-versa. Voici une illustration de ce mécanisme :

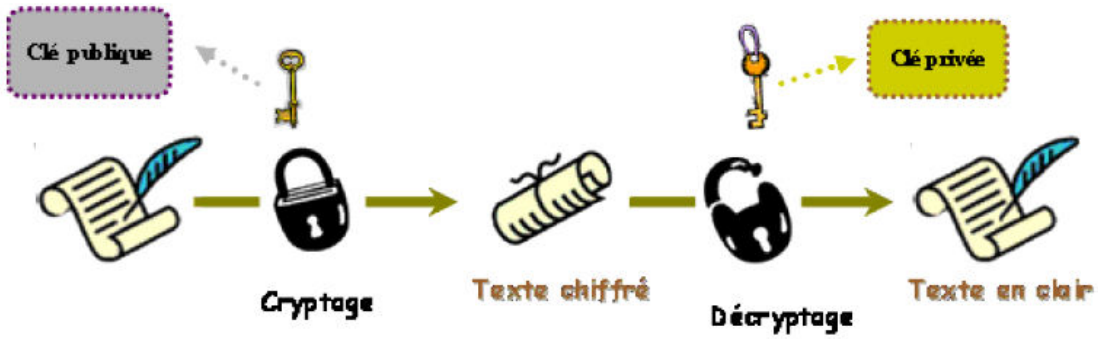

Fig. 3 : Mécanisme de la cryptographie à clé publique

Règles de sécurité

- Les deux clés sont reliées par une fonction mathématique
- Lorsqu'un message est chiffré par une clé il ne peut être déchiffré que par l'autre clé
- Il est impossible de déduire la clé privée à partir de la clé publique
- Le Récepteur communique sa clé publique à l'émetteur
- L'émetteur chiffre le message avec la clé publique puis l'envoi
- Le récepteur déchiffre le message avec sa clé privée

Utilités et limites

La cryptographie de clé publique présente un avantage majeur car l'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. Les communications impliquent uniquement l'utilisation de clés publiques et plus aucune clé privée n'est transmise ou partagée. L'utilisation de clés permet de sécuriser le

dialogue et donc de garantir la confidentialité des données. Mais ceci ne suffit pas à rassurer les internautes, car l'identité de ceux avec qui le dialogue est établi et l'intégrité du message qui leur parvient sont des points tout aussi importants à protéger. Un prétendu récepteur peut par exemple détourner une clé privée et récupérer les informations d'un message alors qu'il n'est pas le récepteur attendu par l'émetteur. Il peut disposer du message comme il veut et porter atteinte à l'intégrité du message, puis le renvoyer aux émetteurs qui possèdent les clés publiques. La confidentialité du message est bien garantie ici, mais l'intégrité ne l'est pas, ni l'authentification.
Deux procédés de sécurité supplémentaires sont donc mis en place afin de garantir l'intégrité des données ainsi que l'**identification** et l'**authentification** des émetteurs et récepteurs : c'est la signature numérique et la certification.

3.2. La signature numérique

Une signature numérique a la même utilité qu'une signature manuscrite. Cependant, une signature manuscrite peut être facilement imitée, alors qu'une signature numérique est pratiquement infalsifiable.

Utilité et principe

La signature numérique confère trois des quatre fonctionnalités d'un mécanisme de sécurité :
- L'intégrité des informations c'est à dire qu'elle permet de s'assurer que le message n'a pas été modifié.
- L'identification du signataire car elle permet de faire le lien avec l'auteur.
- La non répudiation, car l'expéditeur ne peut prétendre qu'il n'a pas envoyé les informations.

La signature numérique à elle seule ne garantit en aucun cas la confidentialité des données. C'est la raison pour laquelle elle est combinée avec les systèmes de cryptographie lorsque les quatre fonctionnalités d'un mécanisme de sécurité sont recherchées.
Dans le cas de figure où la confidentialité n'est pas un critère prépondérant elle peut être utilisée avec du texte en clair. Elle atteste juste que l'entité avec qui on dialogue est bien celle à qui on s'attend et que le message n'a pas été récupéré et modifié.

Principe de la signature numérique

La signature numérique s'obtient en 2 étapes :
(1) Lorsqu'on applique au message en clair une fonction de hachage, on obtient un élément de longueur définie à l'avance appelé résumé de message. En outre, toute modification apportée aux informations entraîne un résumé complètement différent.
(2) Ensuite le résumé et la clé privée sont associés pour créer la 'signature'. Le message et la signature sont transmis au récepteur. Le message peut-être crypté ou pas.

Pour vérifier la signature, c'est-à-dire que le contenu du message est conforme au message attendu et que l'émetteur du message est bien celui qui nous a donné une clé publique, il suffit de réaliser l'opération inverse. C'est-à-dire d'appliquer d'une part la fonction de hachage au texte en clair lui-même pour obtenir le « résumé du message » et d'autre part d'appliquer à la signature la clé publique correspondante pour obtenir également le « résumé du message ». Si les deux condensés sont les mêmes, alors la signature correspond bien au message reçu.

Les figures 4 et 5 représentent une illustration du mécanisme de signature numérique et du procédé de vérification, respectivement.

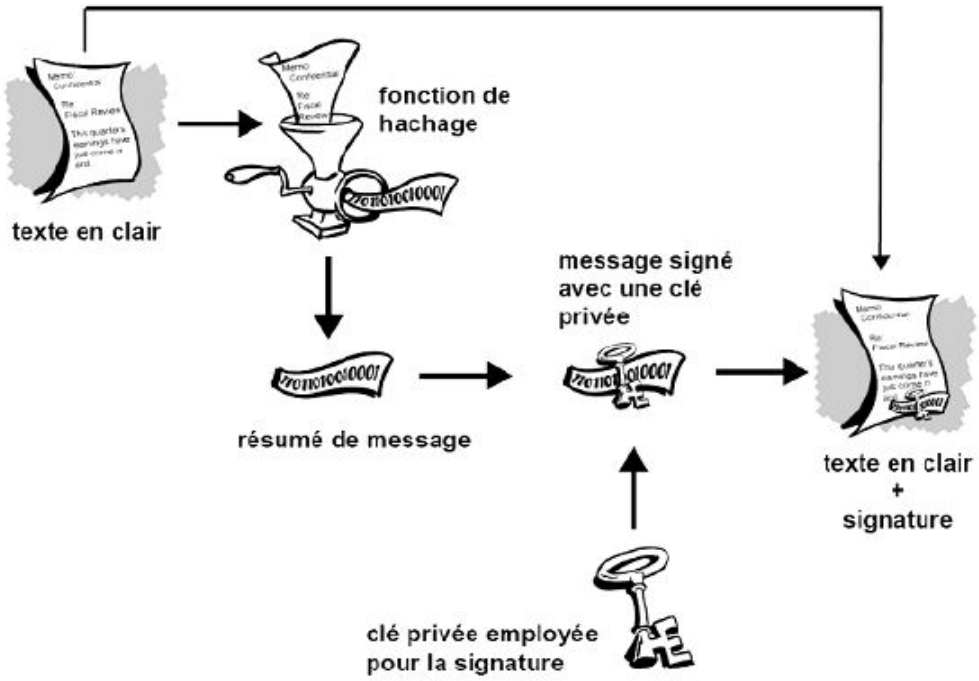

Fig. 4 : Génération d'une signature numérique (côté émetteur)

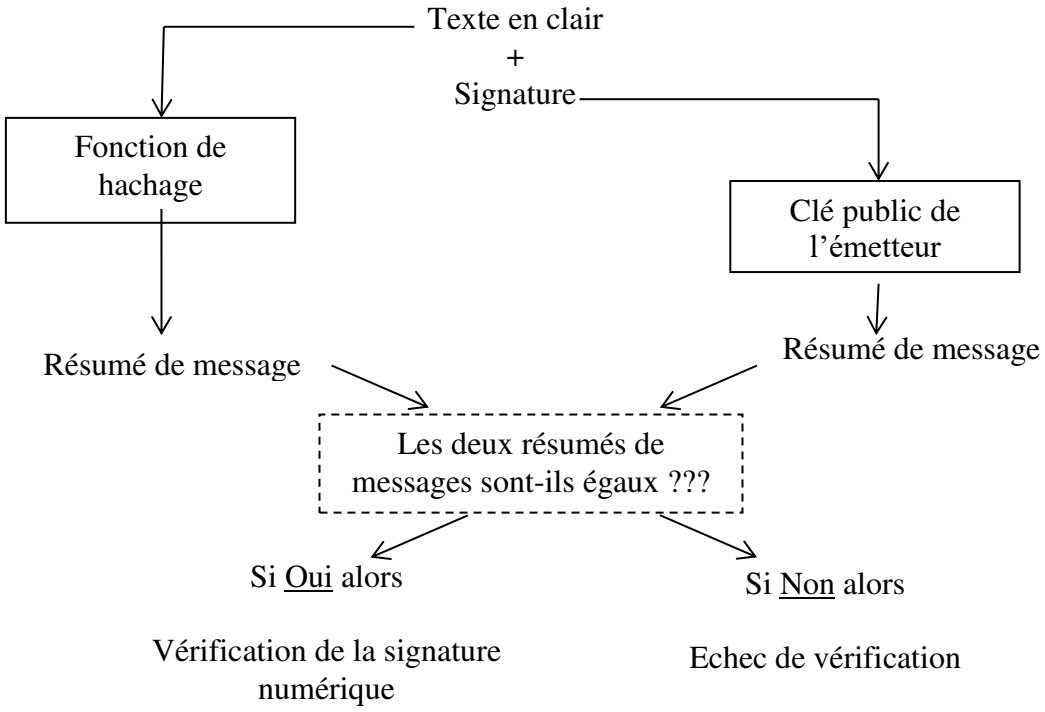

Fig. 5 : Vérification d'une signature numérique (côté récepteur)

Si une fonction de hachage sécurisé est utilisée, il est impossible de récupérer la signature d'un document pour la joindre à un autre document ou d'altérer un message signé. La moindre modification apportée à un document signé entraîne l'échec du processus de vérification de la signature numérique.
La signature numérique est souvent utilisée pour valider des documents tels que les certificats dont on parlera en détail plus loin. Dans ce cas le document est en clair et la signature numérique est opposée au bas du document avec une fonction de hachage permettant de retrouver le résumé du message fourni. En appliquant la clé publique à la signature d'une part et la fonction de hachage au message en clair d'autre part. On retrouve alors un résumé du message comparable à celui qui est fourni au bas du document. Si les deux résultats sont similaires (« résumé du message ») en tout point, on en conclut que le document provient bien de l'émetteur dont on a la clé publique.
Cependant la signature numérique a ses limites car rien n'atteste que celui qui nous donne la clé publique n'a pas détourné la clé privé correspondante et se fait passer pour quelqu'un qu'il n'est pas afin de soutirer des informations. En réalité, la seule façon de garantir que la clé publique obtenue est celle du destinataire qu'on attend c'est d'accepter uniquement les clés distribuées physiquement, car l'identité de l'émetteur serait vérifiée.
Mais dans la réalité d'Internet où le dialogue se fait avec des milliers de serveurs, ce procédé est inapplicable mais un autre mécanisme similaire allant dans le même sens est utilisé : c'est la certification qui va permettre de confirmer qu'une clé appartient réellement à l'interlocuteur qui la distribue.

3.3. La certification

Utilité et principe

Le certificat à la fonction qu'un passeport aurait dans le monde matériel car il comporte des informations qui identifie l'auteur d'une clé et déclare qu'une autre personne a confirmé cette identité.

- Il a une valeur juridique même s'il se sert de la cryptographie (signature numérique).
- Il contient des informations (associées à la clé publique d'une personne), aidant d'autres personnes à vérifier qu'une clé est authentique ou valide.
- Il permet de contrecarrer les tentatives de substitution de la clé d'une personne par une autre.

→ Renforcer l'authentification en utilisant des certificats numériques, entraîne d'avoir recours à un tiers de confiance ou à une société d'authentification (SA).

3.3.1 Principe de la certification par un tiers

Ce mécanisme nécessite d'avoir recours à un tiers de confiance ou à une société d'authentification (SA).
Les détenteurs de clés publiques les soumettent à une SA accompagné d'une preuve d'identité, et la SA appose sa signature numérique certifiant ainsi que la clé publique jointe au certificat appartient à la partie stipulée. Les certificats numériques constituent un des fondements des opérations électroniques protégées puisqu'ils permettent à toutes les parties d'une transaction de vérifier facilement et rapidement l'identité des autres participants.
Il faut savoir que les sociétés de certification sont une entité humaine (une personne, un groupe, un service, une entreprise ou une autre association) autorisée par une société à émettre

des certificats à l'attention de ses utilisateurs informatiques. Une SA fonctionne comme un service de contrôle des passeports du gouvernement d'un pays. Elle crée des certificats et les signe de façon numérique à l'aide d'une clé privée de SA.
A l'aide de la clé publique de la SA, quiconque souhaite vérifier l'authenticité d'un certificat doit vérifier la signature numérique de la SA émettrice et, par conséquent, l'intégrité du contenu du certificat (essentiellement, la clé publique et l'identité du détenteur du Certificat)
→ Un certificat numérique peut se présenter sous différents formats et contenir plusieurs informations.

3.3.2 Les informations minimales d'un certificat

* La clé publique du détenteur du certificat
* Les informations du détenteur du certificat : il s'agit des informations portant sur l' «identité» de l'utilisateur, telles que son nom, son ID utilisateur, sa photographie, etc.
* La signature numérique, dont on a parlé précédemment du détenteur du certificat, également appelée auto-signature.
* La période de validité du certificat : dates/heures de début et d'expiration du certificat.
* L'algorithme de cryptage symétrique préféré pour la clé : indique le type d'algorithme de cryptage que le détenteur du certificat préfère appliquer au cryptage des informations.

→ Ces informations peuvent varier selon la norme des certificats utilisés, notamment certains certificats autorisent plusieurs personnes à valider le même certificat.

3.3.3 Le concept de signatures multiples

Certains certificats permettent à plusieurs personnes de signer une paire de clés/d'identification pour attester en toute certitude de l'appartenance de la clé publique au détenteur spécifié. Certains certificats sont également composés d'une clé publique avec plusieurs libellés, chacun offrant la possibilité d'identifier le détenteur de la clé différemment (par exemple, le nom et le compte de messagerie d'entreprise du détenteur, l'alias et le compte de messagerie personnel du détenteur, sa photographie, et ce, dans un seul certificat).
La liste des signatures de chacune de ces identités peut varier. Les signatures attestent de l'authenticité de l'appartenance de l'un des libellés à la clé publique et non de l'authenticité de tous les libellés sur la clé. Différentes personnes vérifient à différents niveaux l'authenticité avant de signer une clé.

3.3.4 Le mécanisme de distribution de certificats

Au-delà d'une certaine charge de communication, il est nécessaire de mettre en place des systèmes pouvant fournir des mécanismes de sécurité, de stockage et d'échanges de clés nécessaires pour communiquer. Car il est facile pour un petit groupe de s'échanger des clés par émail, mais lorsqu'il s'agit de milliers de clients et serveurs, la mise en place de systèmes de gestion de certificats est nécessaire. Ces systèmes peuvent se présenter sous la forme de référentiels de **stockage uniquement**, appelés serveurs de certificats ou sous la forme de **systèmes structurés** offrant des fonctions de gestion de clés, appelés infrastructures de clé publique (PKI : public key infrastructure). Le rôle d'une PKI n'est pas simplement le stockage. Elle permet de gérer l'émission, la révocation (annulation avant échéance d'un certificat), le stockage, la récupération et la fiabilité d'un certificat.
Un **serveur de certificats**, également appelé serveur de clés, est une base de données permettant aux utilisateurs de soumettre et de récupérer des certificats numériques. Un serveur de certificats offre généralement des fonctions de gestion permettant à une entreprise de

soutenir sa politique de sécurité (par exemple, autoriser uniquement le stockage des clés répondant à des exigences spécifiques).
Nous verrons dans la section 4 quelques exemples des manières comment les procédés présentés ci-dessus sont combinés pour élaborer des solutions de paiement électronique.

4. Exemples de solutions de paiement sécurisé

Dans le système traditionnel du paiement par carte, chacun des éléments suivant à une fonction spécifique :

● Le numéro facial permet d'identifier la carte et de vérifier son existence. Il n'est pas confidentiel.

● Le code confidentiel permet de garantir que le titulaire a exprimé son adhésion au principe et aux modalités du paiement.

● La puce, par la mise en œuvre d'algorithmes de chiffrement, permet de garantir la sécurité du processus de paiement.

Dans l'hypothèse d'un paiement par Internet fondé sur la seule communication du numéro facial, du nom du titulaire et de la date d'expiration, l'opération de paiement offre un degré de sécurité nettement moindre. Contrairement au paiement par code confidentiel, rien ne permet de considérer que le titulaire a exprimé son adhésion à l'opération de paiement. Pour répondre à ce problème plusieurs solutions ont été mises en œuvre :

● Les protocoles nécessitant une authentification forte par les certificats et les signatures numériques,

● L'intervention d'un tiers (au moins) pour des éléments de preuve, à qui sont transmises les données confidentielles pour qu'ils fassent le paiement, ou

● L'utilisation d'une carte bleue dont le numéro de compte virtuel est utilisable une seule fois avec un plafond défini.

Bibliographie

Gérard-Michel Cochard, 'paiement électronique et sécurisation des échanges', Management et productivité des TIC, cours de l'université Jules Verne.