

Méthodologie

L'Observatoire a étudié en 2003 plusieurs thèmes jugés structurants pour la sécurité des cartes de paiement et a produit pour chacun d'eux une synthèse assortie d'une recommandation. Les thèmes qui ont été traités en 2003 sont les suivants :

- **Usage des protocoles d'identification ou d'authentification biométriques dans l'environnement des cartes de paiement**
Les conclusions auxquelles l'Observatoire est parvenu concernent exclusivement l'utilisation de la biométrie dans le domaine pour lequel il est compétent, c'est-à-dire les cartes de paiement, et ne préjugent pas des apports sécuritaires de la biométrie dans d'autres domaines ;
- **État des lieux cryptographiques**
L'Observatoire a constaté que la plupart des systèmes de paiement par carte utilisent des techniques cryptographiques pour assurer la sécurité des transactions. L'Observatoire s'est interrogé sur l'adéquation des techniques employées au regard des menaces existant dans ce domaine ;
- **Apports sécuritaires des normes EMV**
L'adoption de ces normes internationales permet l'utilisation des cartes à puce à l'échelle mondiale afin de lutter contre la contrefaçon des cartes à piste magnétique. Elles proposent en outre d'autres renforcements sécuritaires – notamment en matière de techniques cryptographiques – qui sont décrits dans la suite du document ;
- **Utilisation des systèmes de détection automatique de la fraude**
De nombreux émetteurs ont recours à ces technologies afin de réduire les conséquences, à la fois financières et en terme d'image, de la fraude. Par exemple, les demandes d'autorisation peuvent être analysées par ces outils, permettant à l'émetteur d'être alerté en temps réel d'éventuelles tentatives de fraude. L'Observatoire a analysé l'intérêt de ces systèmes pour lutter contre la fraude et les conditions qui sont nécessaires au bon fonctionnement de ces outils.

Informations collectées

L'Observatoire a essentiellement recueilli des informations auprès de ses membres et a exploité des travaux universitaires pour mener les analyses dont les résultats sont présentés ci-après.

Biométrie

L'Observatoire s'est attaché à mesurer l'apport éventuel des techniques d'authentification biométrique pour la sécurisation des transactions par carte.

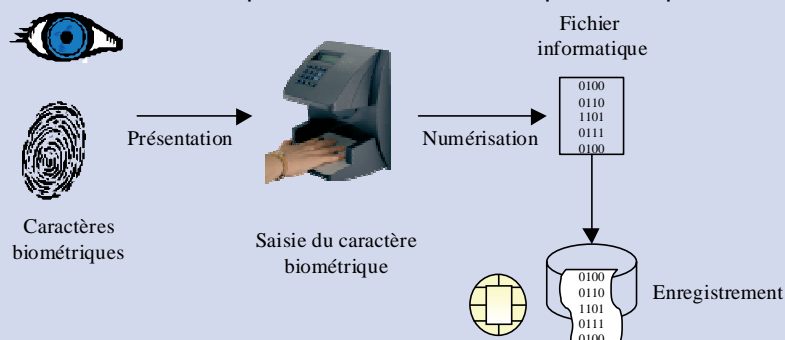
Description générale de la biométrie

La biométrie regroupe l'ensemble des techniques automatisées qui visent à une identification des personnes à partir de caractères physiques propres : empreintes digitales, forme du visage, iris, main, ADN, etc. Elle a comme vocation principale de vérifier la présence physique de la personne. Les gouvernements de plusieurs pays ont lancé des projets d'identification avec biométrie (visa et passeport aux États-Unis, au Japon et en Europe).

Encadré 7 : Principe d'une authentification biométrique

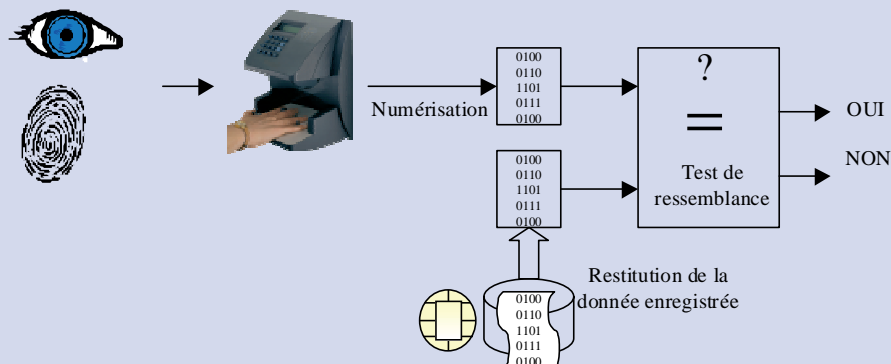
Phase d'enregistrement

La vérification de caractères biométriques tels que la structure de l'iris, une empreinte digitale ou la forme de la main nécessite préalablement une phase d'enrôlement au cours de laquelle une autorité (services de police par exemple) enregistre sous format informatique les données biométriques de la personne.



Authentification biométrique

L'authentification est l'opération par laquelle une entité prouve son identité. Cette vérification peut être assurée de plusieurs manières : un secret (mot de passe, clé de chiffrement...), la possession d'un objet (carte à puce...), un caractère physique (données biométriques...) ou un savoir-faire (signature manuscrite...). Une authentification biométrique consiste à vérifier la ressemblance de la donnée saisie par rapport au caractère préalablement enregistré et stocké soit localement, sur un support matériel (carte ou token), soit à distance sur un serveur.



Utilisation de la biométrie pour les cartes de paiement

Dans l'environnement des cartes de paiement, l'authentification par la biométrie pourrait s'avérer inadaptée pour plusieurs raisons.

Premièrement, il convient de noter que les protocoles d'authentification biométrique sont non-déterministes à l'inverse, par exemple, des fonctions cryptographiques. Les protocoles d'authentification biométrique sont fondés sur une analyse probabiliste impliquant une fiabilité variable de ces protocoles et se traduisant dans la pratique par de possibles rejets et acceptations à tort. Les solutions actuelles d'authentification biométrique peuvent générer des taux de rejet qui ne sont pas compatibles avec le bon fonctionnement des systèmes de paiement par carte. Pour des usages récurrents comme les paiements par carte qui requièrent une certaine fluidité (temps de transaction et fiabilité binaire de l'authentification), le désagrément subi par le porteur et l'accepteur serait difficilement acceptable.

Deuxièmement, le recours à la biométrie pose des problèmes relatifs à l'acceptabilité (confort d'utilisation pour les porteurs, risques d'atteintes physiques pour dérober les éléments d'authentification, acceptation par les porteurs que des données personnelles biométriques soient conservées par les organismes privés) et à l'enregistrement des clients (logistique et fiabilité de l'enregistrement). Ces problèmes sont particulièrement sensibles dans le domaine des cartes de paiement.

Troisièmement, l'usurpation des caractères biométriques est réalisable dans certains cas (par exemple, reproduction d'une empreinte digitale) et une donnée biométrique ne peut pas être changée en cas de compromission. Pour les cartes de paiement, cette menace pourrait être exploitée dans des environnements où le déroulement normal de l'authentification n'est pas toujours contrôlé par une personne physique (par exemple, transactions sur les automates).

Toutefois, l'immaturité actuelle de ces technologies ne signifie pas pour autant que le principe général de l'authentification biométrique soit à rejeter dans le cadre d'une utilisation pour les cartes de paiement. En particulier, le caractère non confidentiel des données biométriques n'est pas en contradiction avec l'objectif de fiabilité des moyens d'authentification, à condition que les dispositifs mis en place pour la vérification des caractères biométriques soient robustes et aptes à résister aux tentatives d'usurpation d'identité. En effet, bien que l'usurpation de données biométriques soit théoriquement réalisable, certains aspects dynamiques liés à la donnée biométrique sont difficilement reproductibles (dynamique des frappes au clavier ou de la signature, capteurs de température, de battements cardiaques ou de conductivité), mais ceci ne semble pas encore avoir été pleinement exploité.

Cryptologie

Étant donné l'importance de la cryptographie pour la sécurisation des systèmes de carte actuels, l'Observatoire a étudié ce thème de façon à identifier les menaces auxquelles est exposé ce type de techniques et qui doivent amener les émetteurs à prendre en compte les évolutions de la cryptologie²⁰.

Besoins de sécurité liés aux cartes de paiement

La carte, comme tout instrument de paiement, doit être protégée contre la contrefaçon et ne doit pouvoir être utilisée que par son porteur légitime. Il est ainsi généralement demandé au porteur de s'authentifier, à l'aide d'un code secret par exemple. Pour éviter qu'il en soit fait un usage frauduleux, il est nécessaire d'assurer la confidentialité des données secrètes et personnelles au sein du système de paiement par carte. De plus, les caractéristiques de la transaction pour laquelle le porteur a donné son accord ne doivent pas pouvoir être modifiées. Enfin, pour éviter l'emploi de cartes contrefaites, l'authenticité des cartes doit être vérifiée à chaque transaction.

Usages possibles de la cryptographie pour les cartes de paiement

Il est apparu que les techniques cryptographiques peuvent être utilisées pour répondre à ces besoins de sécurité. En effet, ces techniques assurent notamment, grâce au chiffrement, la confidentialité des données secrètes (code confidentiel par exemple) et personnelles échangées lors d'une demande d'autorisation ou pour les paiements à distance. De plus, l'origine et l'intégrité des données transactionnelles peuvent être contrôlées grâce à un scellement cryptographique, rendant détectable toute altération accidentelle ou volontaire de la transaction autorisée. Enfin, les techniques cryptographiques peuvent être employées pour vérifier l'authenticité des cartes : les cartes à microprocesseur sont capables de stocker de manière sécurisée des clés secrètes et de répondre aux demandes d'authentification de la carte en réalisant des calculs cryptographiques.

Encadré 8 : Définition de la cryptographie

La cryptographie désigne l'ensemble des techniques qui permettent plusieurs fonctions de sécurité dont la confidentialité et l'intégrité des données échangées. Ces techniques s'appuient sur des algorithmes cryptographiques qui peuvent être classés en deux grandes catégories : les algorithmes symétriques (comme DES²¹, 3DES ou AES²²) et les algorithmes asymétriques (comme RSA²³). Dans le premier cas, chaque partie dispose de la même clé secrète sur la confidentialité de laquelle repose la sécurité. Dans le second, il existe un couple constitué d'une clé privée (secrète) et d'une clé publique (connue de tous) ; ces clés sont distinctes et ne peuvent être déduites facilement l'une de l'autre. Dans l'environnement des cartes de paiement, la cryptographie peut être utilisée pour assurer la confidentialité des données sensibles (fonction de chiffrement), l'authenticité des cartes (fonction d'authentification), l'authenticité et l'intégrité des transactions (fonction de scellement).

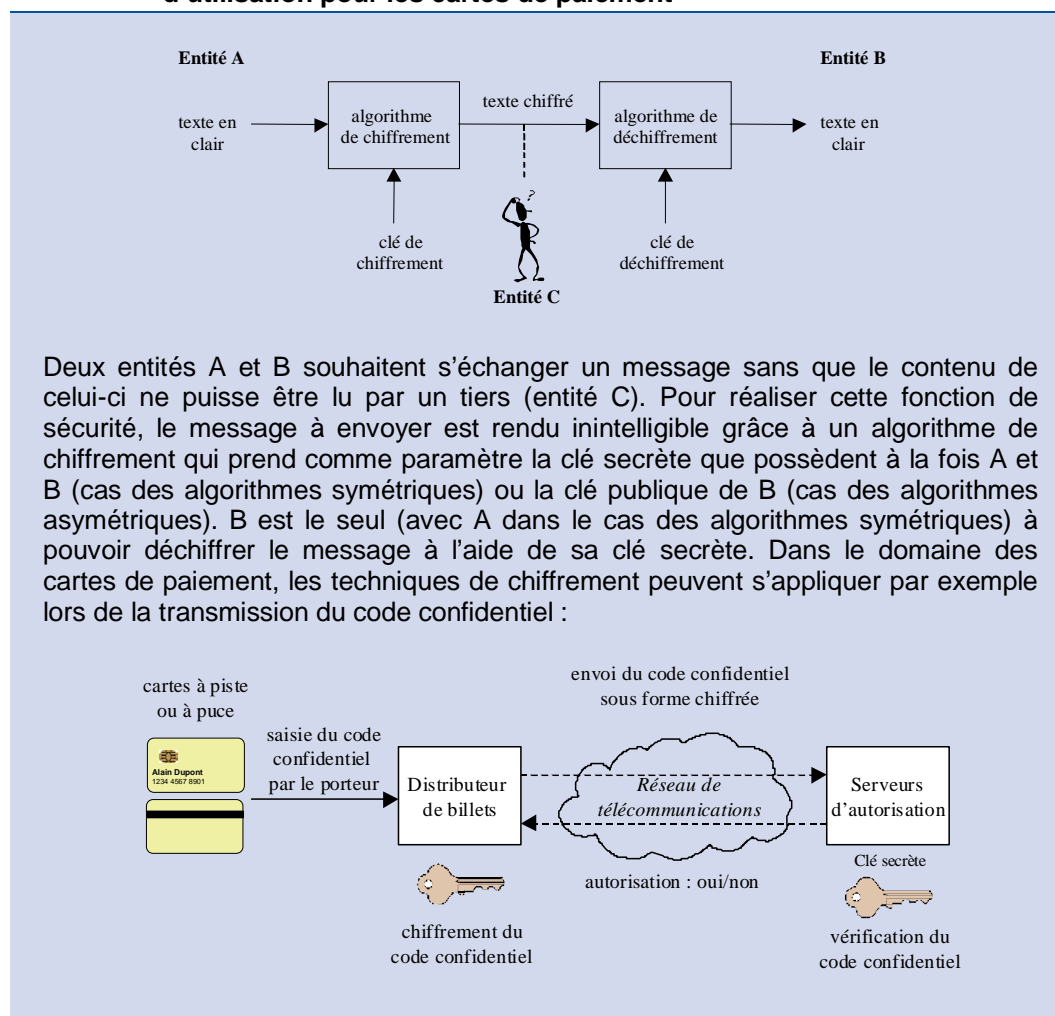
²⁰ La cryptologie regroupe la cryptographie et la cryptanalyse.

²¹ Data Encryption Standard

²² Advanced Encryption Standard

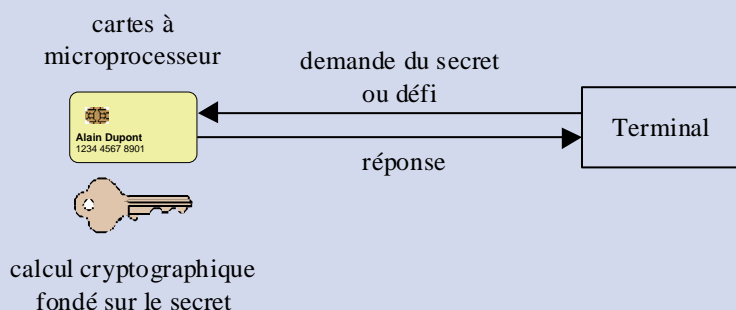
²³ Rivest Shamir Adleman

Encadré 9 : Principe du chiffrement et exemple d'utilisation pour les cartes de paiement



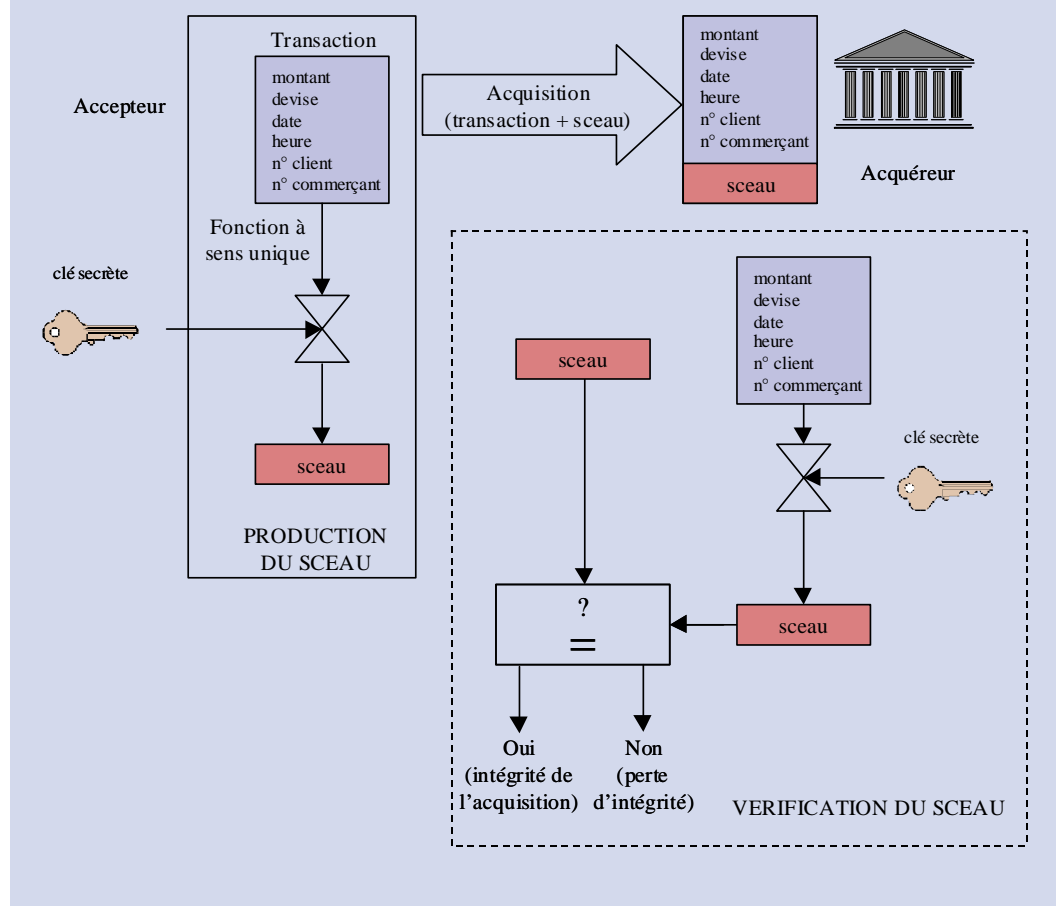
Encadré 10 : Exemple d'utilisation de la cryptographie pour l'authentification des composants

Le schéma suivant décrit le principe d'une authentification – basée sur des techniques cryptographiques – de la carte par le terminal ; ce principe général est applicable à tous les composants constituant un système de cartes (authentification de la carte par le serveur d'autorisation, du terminal par la carte, etc.). Les méthodes d'authentification sont soit statiques soit dynamiques. Dans le premier cas, le terminal demande toujours à la carte de lui fournir la même preuve de la connaissance du secret. Dans le second cas, l'élément secret transmis entre la carte et le terminal est à usage unique. Pour cela, la technique du « défi - réponse » est souvent employée : le terminal envoie un défi à la carte (par exemple un nombre aléatoire) qui réalise une opération cryptographique fondée sur ce défi et sur le secret stocké dans la puce ; le résultat de cette opération est transmis au terminal qui réalise à son tour un calcul cryptographique permettant de vérifier que la carte a bien connaissance du secret.



Encadré 11 : Principe d'un scellement cryptographique, certification des transactions

Le scellement cryptographique est une technique qui permet de certifier l'authenticité et l'intégrité des transactions. Cette technique utilise une fonction à sens unique dépendant d'une clé symétrique partagée. Le sceau ainsi obtenu permet de garantir l'origine de la transaction (il est nécessaire de connaître la clé secrète pour produire le sceau) et l'intégrité des données transactionnelles (toute modification, même mineure, du fichier de transaction entraîne la création d'une empreinte différente).



Principales menaces

Les cryptanalyses visent à porter atteinte à la confidentialité des données sensibles et à l'intégrité de la transaction ou de la carte. Les vulnérabilités provenant des techniques cryptographiques employées peuvent être regroupées en trois catégories principales : choix de l'algorithme et des longueurs de clés, implantation des algorithmes cryptographiques et gestion des clés secrètes.

Encadré 12 : Quelques cryptanalyses

Les attaques par recherche exhaustive ou en force brute consistent à essayer toutes les clés possibles. Ainsi, l'algorithme DES à clé de 56 bits est vulnérable aux tentatives de recherche exhaustive : en 1999, une clé DES fut découverte grâce à un calcul partagé entre 3 000 machines ordinaires pendant 20 jours ; une machine dédiée – dont les spécifications sont publiques et qui peut être construite pour un coût limité (environ 100 000 euros) – a pu atteindre le même résultat en 3 jours. La communauté scientifique considère actuellement qu'un algorithme cryptographique dont la recherche exhaustive peut être réalisée avec un ordre de grandeur de 2^{64} opérations n'est pas sûr. Pour garder une marge de sécurité significative, la recherche exhaustive doit nécessiter un ordre de grandeur de 2^{80} opérations au moins ; ce seuil évolue d'un bit environ tous les 18 mois. Des attaques théoriques sur les algorithmes cryptographiques sont également possibles ; les plus connues sont les attaques linéaires et différentielles. Les algorithmes sont toutefois normalement conçus pour y résister.

Des algorithmes asymétriques comme RSA sont basés sur un problème mathématique jugé difficile comme la factorisation d'entiers. Or, grâce à l'augmentation de la puissance de calcul des ordinateurs et aux avancées théoriques des méthodes utilisées, les records de factorisation d'entiers sont en perpétuelle amélioration. Les records de factorisation actuels indiquent ainsi que les clés RSA de 576 bits sont dès à présent compromises et que les clés de 640 bits devraient l'être à court terme (un à deux ans) ; les clés RSA de 768 bits n'offriront plus alors une marge de sécurité suffisante. Sur la base des connaissances théoriques actuelles (sous réserve de découvertes mathématiques fondamentales concernant la factorisation d'entiers), les menaces pesant sur les clés RSA d'au moins 1 024 bits semblent improbables avant 2013.

Anticipation des menaces

L'évolution des techniques de cryptanalyse doit être prise en compte pour éviter l'affaiblissement des mécanismes sécuritaires qui protègent les systèmes de paiement par carte. Ceci est particulièrement important pour les clés présentant un risque systémique. Les émetteurs réévaluent donc régulièrement la sécurité de leurs systèmes, en révisant notamment leurs choix cryptographiques pour garder une longueur d'avance suffisante par rapport aux fraudeurs. De nouveaux algorithmes – basés sur les courbes elliptiques par exemple – pourraient ainsi contribuer à maintenir la sécurité des cartes de paiement dans le futur. Afin d'anticiper les menaces, certains émetteurs ont adopté au niveau international la norme EMV qui prévoit dès à présent les évolutions en matière de cryptographie jusqu'en 2011.

Normes EMV

Les réseaux VISA et MASTERCARD ont établi avec leurs membres des spécifications communes, baptisées EMV²⁴, permettant l'interopérabilité internationale des transactions de paiement et de retrait par cartes de type « interbancaire » à puce dans un contexte multi-applicatif²⁵. Les normes EMV visent à la fois à permettre le développement de nouveaux services et à améliorer la sécurité des transactions.

À ce jour, deux versions majeures des normes EMV ont déjà été publiées : une première version, baptisée EMV 96, finalisée en mai 1998 et une seconde version, baptisée EMV 2000, publiée en décembre 2000.

Les normes EMV s'appuient sur des normes ISO ou interbancaires²⁶ afin de permettre une offre ouverte et concurrentielle de la part des fournisseurs de cartes et de terminaux. Elles définissent l'ensemble des fonctionnalités et des procédures nécessaires au dialogue entre une carte et un terminal pour effectuer des transactions de paiement et de retrait. Elles précisent notamment les caractéristiques physiques, électriques et d'étanchéité entre applications que doivent respecter la carte et le terminal, les traitements à effectuer de part et d'autre, ainsi que les échanges de données entre la carte et le terminal pendant tout le déroulement de la transaction.

Concernant la sécurité des transactions, les normes EMV apportent 4 types d'améliorations :

- L'apport sécuritaire majeur est le renforcement important de la protection contre la fraude par contrefaçon de la piste magnétique, grâce à l'utilisation de la puce de la carte pour toutes les transactions de paiement et de retrait réalisées sur un terminal ou un automate conformes aux normes EMV ;
- Le deuxième apport sécuritaire réside dans l'amélioration de la protection contre l'utilisation frauduleuse des cartes perdues ou volées, grâce à la généralisation (au niveau international) de l'usage du code confidentiel pour authentifier le porteur sur les terminaux EMV, que la transaction se déroule avec ou sans demande d'autorisation ;
- Le troisième apport sécuritaire est l'amélioration de la gestion du risque porteur par l'émetteur (par exemple, pour déclencher une demande d'autorisation en fonction, non seulement des caractéristiques de la transaction en cours, mais également des transactions précédentes enregistrées sur la carte). L'émetteur a en outre à sa disposition plusieurs méthodes d'authentification du porteur ; il a la possibilité de définir un ordre de priorité dans l'emploi de ces protocoles d'authentification en fonction des méthodes supportées par le terminal et du montant de la transaction ;
- Le dernier apport sécuritaire réside dans l'enrichissement des services cryptographiques disponibles au niveau de la carte et du terminal pour valider la transaction, et dans le renforcement de la robustesse des mécanismes cryptographiques associés. L'encadré suivant donne quelques détails techniques sur les services cryptographiques formalisés par les normes EMV.

²⁴ Europay MasterCard Visa

²⁵ Plusieurs applications différentes (paiements domestiques, paiements internationaux, porte-monnaie électronique, programme de fidélisation, etc.) peuvent ainsi être présentes sur la même carte.

²⁶ Telles que la norme intersectorielle ISO 7816 relative aux cartes à microprocesseur.

Encadré 13 : Services cryptographiques formalisés par les normes EMV

Les services cryptographiques définis par les normes EMV couvrent l'authentification off-line de la carte par le terminal, l'authentification du porteur, l'authentification on-line de la carte par l'émetteur lors d'une demande d'autorisation, l'authentification de l'émetteur par la carte lors de la réponse à une demande d'autorisation, la certification en intégrité et en authenticité de la transaction lors de sa finalisation et l'envoi de scripts sécurisés en intégrité et/ou confidentialité à la carte par l'émetteur en fin de transaction.

En France, l'une des différences majeures par rapport aux services cryptographiques disponibles actuellement sur les cartes de type « interbancaire » est la possibilité de réaliser une authentification dynamique off-line de la carte. La norme EMV 96 prévoit ainsi un mécanisme optionnel au niveau de la carte baptisé DDA (Dynamic Data Authentication). La norme EMV 2000 prévoit en outre un second mécanisme baptisé CDA (Combined Data Authentication) permettant de combiner l'authentification off-line de la carte par le terminal et l'authentification on-line de la carte par l'émetteur.

Les banques et les commerçants français sont aujourd'hui engagés activement dans la migration vers les normes EMV. Une première génération de cartes EMV, répondant à la norme EMV 96, sera déployée progressivement au cours du 1^{er} semestre 2004 en France. Une seconde génération de cartes EMV, répondant à la norme EMV 2000 et supportant des mécanismes additionnels, devrait être disponible un an plus tard. Les distributeurs de billets sont déjà en cours de migration EMV. Côté terminaux d'acceptation, un accord a été signé entre les banques françaises et les représentants du grand commerce, afin d'arriver en 2004 à une mise à niveau massive du parc d'acceptation.

Systemes de détection automatique de la fraude

La détection précoce des cas de fraude est une préoccupation majeure des émetteurs de carte. En effet, on estime que la majorité des utilisations frauduleuses sur les cartes de paiement intervient dans les quatre premiers jours suivant la première fraude. Afin de réduire les conséquences à la fois financières et en terme d'image, les émetteurs ont recours à des systèmes de détection automatique de la fraude.

Les émetteurs utilisent ces technologies afin, notamment, d'analyser les dossiers d'ouverture de compte et d'évaluer le risque lié à chaque transaction. Lorsqu'elles sont employées pour détecter les transactions frauduleuses, elles interviennent à différents stades : traitement en temps réel de la demande d'autorisation, étude a posteriori des transactions collectées et analyse des transactions impayées.

Les besoins des différents acteurs impliqués dans les systèmes de paiement par carte diffèrent et un traitement uniforme de la fraude semble difficile à organiser. En particulier, les réseaux privés ne sont pas soumis aux mêmes contraintes que les réseaux ouverts où un manque d'harmonisation des pratiques, résultat de la pluralité d'établissements émetteurs et acquéreurs, est parfois constaté.

Encadré 14 : Exemple de systèmes de détection automatique de la fraude

Les outils, qui peuvent être simples ou très sophistiqués, sont multiples et adaptés aux risques spécifiques identifiés par les émetteurs ; ils peuvent être communs à plusieurs émetteurs ou développés en interne. Parmi ceux-ci, on recense les systèmes d'intelligence artificielle (par exemple, réseaux de neurones), les systèmes experts ou les dispositifs analysant des séquences comportementales.

Les données exploitées sont généralement les attributs relatifs à la transaction (montant, numéro de la carte, date, identifiant de l'accepteur, éléments de l'autorisation ou du refus...) et les informations présentes dans les fichiers financiers de compensation²⁷. D'autres données descriptives (informations liées aux clients ou aux commerçants notamment) peuvent être utiles pour appréhender l'environnement de la carte dans sa globalité : ce sont par exemple les habitudes du porteur ou la localisation du commerçant.

L'utilité des systèmes de détection automatique de la fraude est incontestée. Toutefois, une analyse particulière est nécessaire lors de l'utilisation de ces technologies. D'abord, un arbitrage est nécessaire entre le nombre de fausses alertes (« faux positifs ») et les cas de fraude non détectés, notamment pour ne pas provoquer une éventuelle gêne au niveau des utilisateurs (par exemple, risque de blocage d'une transaction suite à une suspicion erronée de fraude) ; ce paramétrage est à l'appréciation de l'émetteur en fonction du niveau de risque qu'il juge acceptable. Ensuite, les données transactionnelles transmises aux systèmes de détection de la fraude sont parfois incomplètes ou inexactes, ce qui nuit à l'efficacité des analyses réalisées. Enfin, la compréhension et le suivi de la fraude sont rendus complexes en raison des différences de codification des motifs d'impayés entre émetteurs. La fiabilité de la collecte d'informations sur la fraude est pourtant cruciale pour alimenter la base d'apprentissage des systèmes de détection automatique de la fraude et maintenir un paramétrage optimal de ces systèmes.

²⁷ Étape au cours de laquelle deux établissements se présentent le solde net de leurs créances réciproques

Recommandations

Les arguments précités conduisent l'Observatoire à formuler les synthèses et les recommandations suivantes.

Biométrie

La sécurité et la fiabilité des dispositifs biométriques en matière d'authentification n'étant pas aujourd'hui au niveau de sécurité requis pour les paiements par carte et l'utilisation de la biométrie par des émetteurs privés posant des problèmes d'acceptabilité particulièrement sensibles pour des systèmes de paiement de masse, l'Observatoire estime que le remplacement des solutions fondées sur la vérification d'un secret par des méthodes biométriques n'est pas souhaitable pour le moment et que les efforts doivent prioritairement porter sur d'autres domaines de la sécurité des cartes de paiement. Toutefois, la biométrie peut venir en appui dans une logique d'aide à l'identification, permettant d'en recommander l'usage dans certains environnements particuliers, et il conviendra de suivre les évolutions techniques qui permettront d'améliorer la fiabilité des méthodes d'authentification biométrique.

Cryptologie

L'Observatoire considère que la cryptographie est incontournable pour assurer la sécurité des transactions. Toutefois, l'emploi de certains algorithmes cryptographiques ou de certaines longueurs de clés présente des risques : l'Observatoire constate en particulier que les clés DES de 56 bits et RSA de moins de 640 bits n'offrent plus un niveau de sécurité suffisant pour les cartes de paiement. L'Observatoire appelle également l'attention des émetteurs sur les risques liés à l'implantation des algorithmes et à la gestion des clés ; ces thèmes seront approfondis lors de prochains travaux. L'amélioration des techniques de cryptanalyse, qui va de pair avec celle des algorithmes cryptographiques, doit être anticipée pour que les systèmes de paiement utilisent à chaque instant des technologies cryptographiques sûres.

Normes EMV

Les réseaux VISA et MASTERCARD ont établi avec leurs membres des spécifications communes, baptisées EMV, permettant l'interopérabilité internationale des transactions de paiement et de retrait par cartes de paiement à puce.

L'Observatoire constate que certains émetteurs de cartes sont aujourd'hui engagés activement dans la migration vers les normes EMV ; il les encourage à poursuivre le mouvement de migration en cours. Dans la lutte contre la fraude internationale, il est dans l'intérêt commun des banques, des porteurs et des commerçants français que la migration aux normes EMV de ces cartes et de leurs terminaux d'acceptation soit la plus rapide possible.

Systemes de detection automatique de la fraude

L'Observatoire constate que les systemes de detection automatique de la fraude mis en place par les emetteurs sont souvent tres utiles pour identifier le plus rapidement possible les scenarios de fraude ; il recommande aux emetteurs de poursuivre les efforts entrepris dans ce domaine.

La fiabilite des donnees fournies en entree des systemes de detection automatique de la fraude est cruciale pour la pertinence des analyses menees. L'Observatoire appelle par consequent l'attention des emetteurs ayant recours a ce type d'outils sur l'importance d'assurer de bout en bout l'exactitude et la coherence des informations transactionnelles transmises du commerçant aux systemes centraux.

Pour maintenir un paramétrage adapté, les outils d'intelligence artificielle doivent disposer d'une connaissance maximale de la fraude constatée a posteriori. Une classification commune de la fraude aiderait les emetteurs, notamment dans un contexte international, a fiabiliser le suivi de la fraude. Des travaux sont en cours dans ce sens, notamment au sein du groupe « Statistiques » de l'Observatoire.

Enfin, il conviendrait que soit étudiée l'opportunité d'un échange, dans le respect du cadre légal et concurrentiel, des informations sur la fraude. Cet échange de données permettrait d'accroître la taille des bases d'apprentissage et contribuerait à améliorer la connaissance de la fraude. La faisabilité et les conséquences de ce projet feront en 2004 l'objet d'une étude au sein de l'Observatoire.