Mise en œuvre et sécurisation d'une plateforme monétique pédagogique

Emilie Sulmont (emilie.sulmont@ensicaen.fr)*
Marc Pasquet (marc.pasquet@ensicaen.fr)*
Joan Reynaud (joan.reynaud@ensicaen.fr) *

Résumé : La Plateforme Monétique et Pédagogique (PMP) est un système d'information reconstituant, à l'échelle d'un laboratoire, un système interbancaire. Elle a été étudiée pour permettre le retrait et le paiement d'un porteur de carte d'une banque appelée ENSIBANK A sur des équipements de service appartenant à une banque ENSIBANK B.
La PMP offre un support pédagogique permettant différentes approches :
– La plus classique sous forme de travaux pratiques : l'ENSICAEN propose 8 travaux pratiques différents qui permettent la manipulation de GAB, analyse de messages protocolaires, manipulation de boitiers de sécurité, développement d'applications cartes, configuration et utilisation de logiciels d'acquisition et de délivrance d'autorisation...
– Sous forme de projet école ou de stage : réalisation d'applications complémentaires à la plateforme (système d'information gérant les comptes et les clients d'une banque), réalisation de cartes personnalisées Eurocard Mastercard Visa (EMV), adaptation d'interfaçage entre deux applications de constructeurs différents, réalisation d'un logiciel de simulation de flux.

Mots Clés : sécurité, monétique, plateforme industrielle, formation

1 Introduction

Cette plateforme a été conçue avec des partenaires publics et privés. Sa spécificité repose sur le fait que, bien qu'installée dans un milieu non bancaire, elle possède des matériels et des logiciels professionnels, parfois sensibles (comme les boitiers sécuritaires). C'est à notre connaissance une plateforme unique en son genre.

2 Plateforme monétique et Pédagogique

2.1 Présentation

Dès 2005, l'Ecole Nationale Supérieure d'Ingénieurs de Caen (ENSICAEN) a débuté l'intégration d'une Plateforme Monétique et Pédagogique (PMP). Lors du 9e colloque du CETSIS en 2011, une présentation de la plateforme avait été faite [Sam11]. Intégrée dans un sous-réseau étanche par rapport au réseau de l'école, elle est constituée d'outils professionnels du domaine. Son architecture a été étudiée pour pouvoir réaliser de bout en bout une transaction de type paiement ou retrait, depuis l'insertion de la carte, dans un terminal

∗. Laboratoire GREYC, ENSICAEN et CNRS Université de Caen Basse Normandie - 6 boulevard maréchal juin 14000 CAEN

(Terminal de Paiement Électronique (TPE) ou Guichet Automatique de Banque (GAB)), jusqu'au crédit/débit des comptes marchand et porteur.

2.2 Cinématique d'une transaction interbancaire

La plateforme permet la cinématique suivante :
On introduit une carte privée et personnalisée à l'école de type bancaire (EMV) de l'ENSIBANK A, dans des équipements tels qu'un guichet automatique bancaire (GAB) ou un terminal de paiement électronique (TPE) appartenant à la banque ENSIBANK B. Cette carte est traitée par un serveur "front-office" gérant l'acquisition des données (lié à ENSIBANK B) puis routée à travers un système simulé vers le serveur "front-office" émetteur (lié à ENSIBANK A) capable de réaliser l'autorisation de la transaction à partir des informations cartes délivrées. Le système "back-office" de l'ENSIBANK A collecte l'ensemble des transactions effectuées sur son "front-office" en fin de journée comptable et les réconcilie avec les informations des opérations de l'autre banque. C'est encore le système "back-office" qui réalise la balance comptable des utilisateurs de sa banque (fig 1).

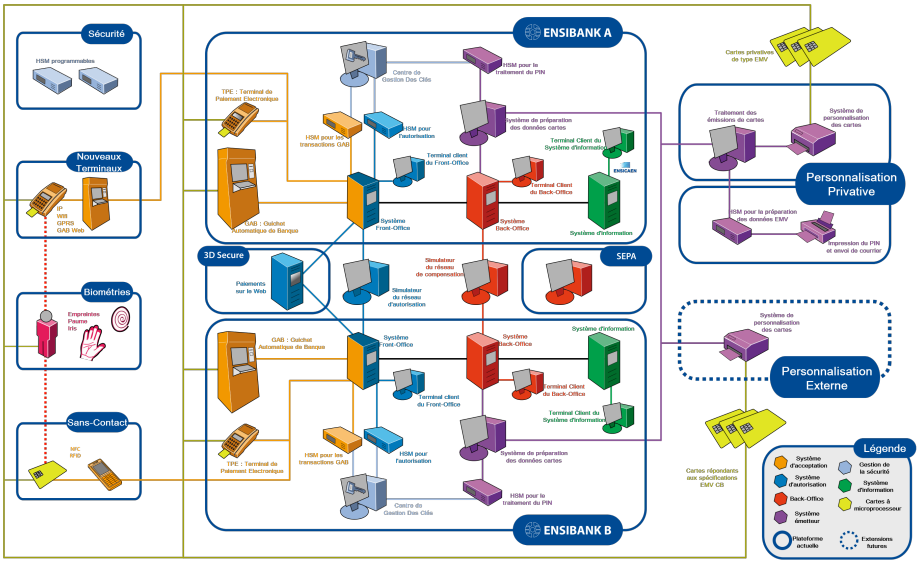

Figure 1: La PMP

2.3 Vision globale sur trois domaines monétiques

La PMP a été conçue pour donner une vision globale de la sécurité monétique aux étudiants. Elle regroupe plusieurs domaines de sécurité :

- La sécurité appliquée aux points d'acceptation(ou points d'interaction),
- la sécurité au domaine acquéreur,
- La sécurité au domaine émetteur.

La sécurité au niveau des points d'acceptation concerne la protection des données porteur au niveau des terminaux ou points de service (TPE , GAB , Tpe Virtuels (VAD) ...) et des Prestataire de Service de Paiement (PSP), intermédiaires entre le marchand et la banque.
La sécurité du domaine acquéreur concerne la protection des données porteurs lors des échanges entre le point d'acceptation et le système d'acquisition appartenant à la banque du marchand.
La sécurité du domaine émetteur intervient au moment de l'authentification, de l'autorisation carte, et aussi de la personnalisation. La personnalisation carte est le processus qui permet l'entrée dans la carte de paramètres liés à la banque, au porteur et à la cryptographie.
Suivant le type de carte, le processus de personnalisation et le niveau de sécurité de chacune d'entre elles diffèrent.

2.4 Personnalisation interne des cartes bancaires

La plateforme monétique et pédagogique contient sa propre Public Key Infrastructure (PKI) permettant de gérer les certificats et son propre atelier de personnalisation de cartes.
Chacune des banques, appelée ENSIBANK A et ENSIBANK B possède son propre certificat fourni par la PKI de la plateforme. La clé publique de la PKI est intégrée dans les TPE et GAB de la plateforme pour permettre l'acceptation des cartes reconnues par l'autorité de certification interne.
Les serveurs en charge de l'autorisation de chacune des deux banques vont être paramétrés avec les données carte et les valeurs des clés secrètes permettant d'effectuer des calculs sécuritaires : l'intégrité du message, l'authentification des données de la carte, la confidentialité, l'intégrité et la signature de la réponse envoyée à la carte.

3 Mise en oeuvre de la sécurité

3.1 Niveau de protection

3.1.1 Sécurité du système d'information

En tant que système d'information, l'infrastructure de la plateforme a été conçue pour correspondre à la norme ISO27002. Cette norme définit un certain nombre de recommandations concernant la sécurité de l'information pour protéger : confidentialité, intégrité, disponibilité, authenticité et contrôle d'accès aux données (fig 2).
Les serveurs permettant l'acquisition, le routage et l'autorisation des transactions sont placés dans une salle sécurisée et équipée d'une climatisation. Le réseau contenant les serveurs dispose d'une sécurité logique, c'est à dire qu'un logiciel qui contrôle les entrées/sorties du réseau. Toutes intrusions extérieures qu'elles proviennent d'Internet ou du réseau père sont interdites. Les seuls accès possibles sont :

- Ceux déclarées provenant des deux réseaux connexes, comprenant les postes de travaux pratiques dédiées à la PMP,
- Les accès provenant des points de service GAB/Distributeur Automatique de Banque (DAB) et TPE,

– Les accès Virtual Private Network (VPN) autorisés aux postes dédiés à l'équipe PMP.

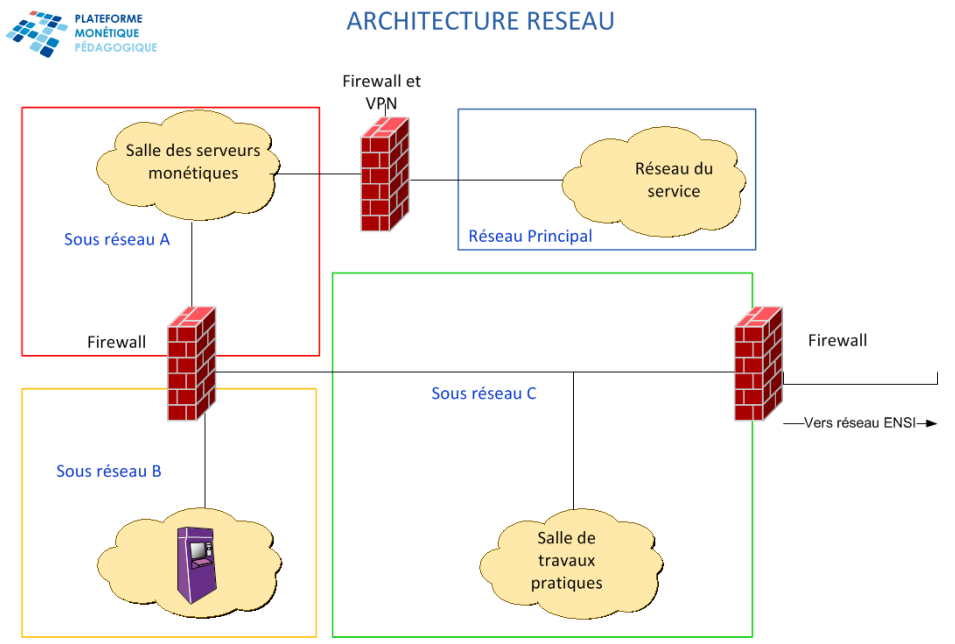

Figure 2: Architecture réseau de la PMP

3.1.2 Sécurité des données porteur (ou carte)

Depuis deux ans, nous avons fait évoluer notre système de protection en se rapprochant d'un standard de l'industrie de la monétique : Payment Card Industry - Data Security Standard (PCI-DSS).
Ce standard s'applique à tous les systèmes de composants (réseau, serveur, application) inclus dans ou connectés à l'environnement des données cartes [pmp13]. Le but est de renforcer la sécurité des données des titulaires de cartes et concerne notamment les commerçants, les entreprises de traitement, acquéreurs, émetteurs et prestataires de service, ainsi que toutes les autres entités qui stockent, traitent ou transmettent des données de titulaires de cartes.
En toute rigueur, la plateforme n'est pas concernée par la norme puisque qu'elle est une réduction d'un système interbancaire, qui utilise, certes des données carte mais dans un contexte pédagogique et non opérationnel. Malgré tout, nous avons souhaité appliquer un maximum des exigences, pour se rapprocher des conditions industrielles.
Ainsi, nous avons entrepris de nombreuses actions dont en particulier :

– Installer des logiciels certifiés Payment Application - Data Security Standard (PA-DSS),
– Développer des outils "maison" conformes à la norme PA-DSS,
– Rédiger et appliquer des procédures dans le cadre d'une Politique de sécurité du Système d'Information (PSSI),

- Rédiger et appliquer des procédures de mise à jour régulière des logiciels,
- Installer et gérer les logiciels de protection des données,
- Restreindre les accès physiques à la salle serveur...

3.2 Risque de vols et de contrefaçon

La protection au niveau réseau de la plateforme a été assurée par le suivi de normes règlementaires, mais d'autres risques peuvent apparaitre liés au vol de matériels ou à la contrefaçon. Dans ce cas, on peut se demander quels sont les risques :

3.2.1 Cas du vol de cartes

Nous pouvons considérer deux situations.
Premier cas : nous effectuons une transaction avec un terminal d'un marchand référencé dans une banque connue. Dans ce cas, cette carte sera refusée dès la phase d'authentification entre le terminal et la carte car les terminaux ne possèdent pas les certificats du PKI de l'ENSICAEN qui ont servi à signer les cartes.
Deuxième cas : nous effectuons une transaction à distance, depuis un site internet ou par téléphone. Dans ce cas, le porteur, lors de la transaction, ne peut pas transmettre les données de la puce, il transmet uniquement le numéro de la carte, la date de validité et le numéro à trois chiffres appelées "CVX2" placés derrière la carte. Ensuite, la banque du marchand, dit "acquéreur", acceptant la transaction route systèmatiquement en fonction du numéro de cartes la transaction vers le serveur de la banque du porteur, dit "émetteur". Pour atteindre, le système d'autorisation et espérer être acceptée, la transaction doit pouvoir passer le traitement d'identification de la carte et le traitement de vérification du "CVX2". Or, chacune des banques ENSIBANK ont un numéro de plage de cartes réservées auprès de l'Association Française de NORmalisation (AFNOR) et qui n'est absolument pas référencé pas les systèmes des banques acquéreurs réels. La transaction ne sera donc pas autorisée.

3.2.2 Cas du vol de terminaux

Imaginons que nous effectuons une transaction avec une carte et un terminal ENSICAEN que nous relions de manière frauduleuse à une banque connue, en remplaçant par exemple un terminal déjà présent chez un marchand. Nous le configurons avec le même identifiant et la même adresse IP afin de l'authentifier correctement à la banque. Dans ce cas, seules les cartes ENSICAEN pourront être acceptées du fait du certificat "maison" introduit dedans. Dans les cas où la transaction est en mode hors-ligne, elles ne seront transmises que plus tard, par télécollecte, au serveur acquéreur. Ensuite, lors du règlement en fin de journée comptable, toutes ces transactions frauduleuses vont être rejetées puisqu'elles ne correspondent à aucune banque valide. L'acceptation de ces cartes par le TPE sera vite repérée comme étant illicite, seules les cartes reconnues par les autorités de certification officielles peuvent être acceptées par les TPE. Le marchand, reconnu comme fraudeur, ne pourra pas être honoré.

3.2.3 Cas du vol de vrai-faux billets

Les vrai-faux billets sont les billets utilisés par les constructeurs de GAB fournis par la Banque de France. L'ENSICAEN en possède quelques uns. Ils permettent de réaliser

des tests de sécurité. Ces billets ont quelques caractéristiques identiques aux vrais billets (granularité du papier, image, bande réfléchissante..) mais n'en ont pas l'aspect (couleur, image...). Un tel billet est inutilisable pour le paiement et n'est accepté par les dépôts des GAB automatiques qu'en "mode test".

3.2.4 Autres cas de vol

On peut imaginer d'autres cas de vol. Concernant les GAB ou la machine à embosser les cartes, étant donné leur poids (respectivement 750Kg et 75KG), nous n'envisagerons même pas le cas possible. Concernant d'autres menus matériels comme les boîtiers de chiffrement, les serveurs et autres matériels informatiques, l'ensemble est inventorié et protégé physiquement en dehors des plages de cours consacré à la plateforme. Si, malgré cela, un vol sans effraction était constaté, il serait possible de tracer les responsables. En effet, des badges sont nécessaires pour entrer dans l'école et des cahiers inventorient les personnes accédant aux salles sensibles de la PMP.

3.2.5 Risque de contrefaçon

La PMP est aussi une source de documentation (spécifications techniques provenant d'industriels ou normes bancaires, pour l'essentiel) fournie lors des cours. Nous nous sommes engagés à ne pas les diffuser en dehors du cadre scolaire et nous demandons à nos étudiants de ne pas copier et diffuser cette documentation : une charte de confidentialité a été signée dans ce sens, entre les partenaires industriels et l'école. Cependant, si pour la plupart les documentations sont au format "papier", au contraire les documents numériques sont eux, faciles à copier.
Or, la publication dans le passé de connaissances en sécurité monétique a montré que le risque de fraude par contrefaçon est une réalité. Prenons l'exemple de la fraude sur la carte bancaire. En 1997, Serge Humpich réussit à contourner deux systèmes de sécurité existant : premièrement, il réussit à créer une carte bancaire capable de répondre toujours "code bon", quelque soit le Personal Identification Number (PIN) entré : la Yescard. Deuxièmement, il réussit en utilisant un logiciel de factorisation, à découvrir la clé secrète utilisée à l'époque par le Groupement des Cartes Bancaires (GCB). Il publie sa découverte en 1999 qui va être exploitée, de manière frauduleuse, deux ans plus tard(Cf [Col01]). En 2002, on constate une augmentation de la fraude de 150% (Cf [Col04]). Cela montre qu'il y a, pour GCB, un risque très important à dévoiler les secrets de conception tels que les algorithmes de chiffrement.
Donc, on peut se demander si l'accessibilité à la documentation n'est pas une faille de sécurité et ne doit pas être remis en cause.
Dans le paragraphe suivant, nous montrerons les apports pédagogiques de la plateforme et nous verrons en quoi elle ne contribue pas à l'augmentation de la fraude, comme on pourrait le penser.

4 Pédagogie

4.1 Travaux pratiques

Les travaux pratiques sont au nombre de huit (GAB, boitiers sécurités, personnalisation de cartes, manipulation de logiciels front-office, Back-office, simulateur, analyse de transactions 3D-Secure, développement NFC sur mobile). Ils durent quatre heures par

TP.
Dans l'exemple du TP sur la manipulation d'un GAB, ils vont réaliser le démarrage à froid, de deux GAB de marque différente. Ils disposent de la documentation utilisateur et technique du fournisseur. Ils rendent en fin de séance, un compte rendu. Ces travaux font surtout appel, à leur capacité d'observation et de curiosité : nommage les différentes parties du GAB, comparaison du mode de fonctionnement des GAB, description de la Nouvelle Architecture Cryptographique, qui est le nom donné au système d'échange de clés des équipements à l'initialisation du GAB.
Cette découverte du GAB leur permet d'apréhender l'objet sous un autre angle : nous sommes nombreux, à avoir utilisé un GAB en tant que client, mais très peu en tant qu'opérateur. Même si ces étudiants ne sont à priori pas destinés à un poste d'opérateur, la vision opérateur est essentielle dans la manière d'aborder leurs futurs projets ; Cela leur permet de mieux communiquer et mieux comprendre les besoins des clients ou les exigences des fournisseurs (fig 3).

Figure 3: Gestionnaire Automatique de Billets

Dans l'exemple du TP sur la manipulation d'un logiciel front office, les étudiants simulent une transaction de paiement qui sera envoyée et traitée par le logciel professionnel d'acquisition et d'autorisation. Les étudiants doivent analyser le journal des transactions, modifier le paramétrage métier du logiciel (diminuer le plafond carte) ou modifier les configurations techniques (le point d'accès réseau). Le compte rendu exige d'eux, de faire une analyse des transactions effectuées et des copier/coller des écrans modifiés. Lors de cette séance, ils ont à leur disposition les manuels opérateur et administrateur des logiciels, les spécifications des protocoles.
Manipuler ce type de logiciel demande tout de suite une grande expertise et les étudiants ressortent de ces activités, avec une plus grande frustration que sur une activité utilisant un GAB. Cependant, cette approche leur permet, une nouvelle fois d'expérimenter la vision opérateur et administrateur. Ils peuvent également appliquer leur savoir théorique. Par exemple, leur connaissance dans le format des protocoles monétiques les aide dans l'analyse d'une trame enregistrée dans le journal de serveur d'autorisation.

4.2 Projets

Des projets pédagogiques ont pu être menés conjointement avec des entreprises ou directement avec l'équipe de l'école. On peut citer, par exemple, le développement d'une application GAB prenant en compte l'insertion d'une authentification biométrique. Leur premier travail a été de réaliser le développement des écrans d'interface utilisateur à l'aide d'un simulateur de GAB puis de le déployer sur la machine équipée d'un lecteur. Leur deuxième travail a été de développer une application sur une carte de test capable de comparer les empreintes authentifiées sur le lecteur et celles enregistrées sur la carte. On peut également citer le développement d'un système d'information d'une banque hébergeant clients, comptes et cartes. Ce projet a été repris sur plusieurs années, par les groupes, soit pour en améliorer le code ou la conception, soit pour le rendre conforme à la norme PA-DSS.
D'autres projets ont traité de l'interfaçage de certains logiciels entre eux, comme le back office avec le système de personnalisation, le front office avec le back office.
Tous ces projets s'appuient sur des matériels ou/et des logiciels industriels. Ce qui apporte une dimension plus réaliste et du coup permet aux étudiants de développer des qualités, essentiellement de gestion de projet, qu'ils ne pourraient pas développer autrement (relations fournisseurs, adaptation à un environnement physique et humain, recherche de solutions à des problèmes faisant intervenir plusieurs acteurs, ...).

4.2.1 Intérêts pédagogiques

Quelque soit la forme que revêt la pédagogie (travaux pratiques ou projets), la PMP offre un double intérêt :

- Le premier intérêt est qu'elle permet aux étudiants de se confronter à des situations réelles sans se limiter à un seul domaine bancaire (front-office ou back-office...). Un ingénieur monéticien a rarement la possibilité dans sa carrière de découvrir l'ensemble des domaines bancaires. En réduisant l'échelle du système interbancaire, l'ingénieur Ensicaennais possède une vision globale de la monétique.
- Le deuxième intérêt est que cette mise à disposition de fournitures aussi sensibles que les systèmes d'autorisation et de personnalisation des cartes est une mise en application directe du principe de la sécurité par la lumière [Ste98],[Pas08]. Les étudiants sont entièrement informés des techniques utilisées pour sécuriser les transactions électroniques aussi bien théoriquement qu'en pratique. Ils peuvent dans leur future profession soit l'appliquer, soit l'améliorer. C'est en formant par la pratique les ingénieurs monéticiens de demain que les systèmes de sécurité bancaire dans leur ensemble pourront évoluer et se défendre des actes frauduleux.

4.3 Résultats pédagogiques

Différentes voies pédagogiques permettent une manipulation des éléments de la plateforme aux étudiants. En plus des étudiants ingénieurs par voie classique ou par apprentissage, un mastère spécialisé est adressé à des jeunes diplômés en informatique ou des salariés désirant se spécialiser en monétique. Ceci porte le nombre d'étudiants formés à 185 par an :

- 70 apprentis
- 100 étudiants classiques
- 15 auditeurs de mastères spécialisés

La plateforme totalise une durée d'exploitation d'environ 1400h par an, dans le cadre de TPs et projets, toutes formations confondues. La plateforme a une influence très positive du point de vue du recrutement des élèves, notamment des apprentis. Les entreprises et les étudiants choisissant cette voie, se tournent naturellement vers l'ENSICAEN. L'école n'a plus à démontrer son attractivité dans ce domaine de compétence.

5 Conclusion

Cette plateforme montre les principes de sécurité que l'on trouve en monétique à tous les niveaux de la chaîne de traitement d'une transaction électronique : Architecture en Nouvelle Cryptographie, personnalisation des données EMV, Infrastructure à Clé Publique (génération de certificats par un tiers puis introduit dans la carte), authentification forte (biométrie)...
Cette ouverture au secret bancaire est cependant protégée et sa divulgation maitrisée. La plateforme suit les recommandations de sécurité d'un système d'information classique et les recommandations propres au domaine de la monétique (PCI-DSS). Les documentations industrielles et confidentielles sont protégées. Techniquement, la plateforme ne peut pas permettre la reproduction ou contrefaire des cartes, billets et systèmes frauduleux.
Cette formation spécialisée permet, au delà de la montée en compétence des étudiants, d'agir indirectement sur la lutte contre la fraude ; d'abord, parce qu'elle forme les futurs ingénieurs concepteurs à de nouveaux principes de sécurité et ensuite parce qu'elle s'adresse également aux étudiants étrangers. Or, la fraude à l'étranger coûte de plus en plus cher au GCB : en paiement par carte, elle augmente sensiblement et atteint 90 millions d'euros [dCB12]. Elle est due essentiellement au manque de sécurisation des systèmes, notamment, à la non conformité à la norme EMV. La montée en compétence des ingénieurs étrangers permettra aux pays d'améliorer la sécurité des systèmes dans le monde et diminuer la fraude. D'ailleurs, l'ENSICAEN, depuis quelques années attire de plus en plus d'étrangers.

Références

[Col01] Pascal Colombani. *Le dossier noir des cartes bancaires.* Carnot, 2001. 37-84.

[Col04] Pascal Colombani. Fraudes à la carte bancaire. 2004. 13.

[dCB12] Groupement des Cartes Bancaires. Rapport d'activités du groupement des cartes bancaires cb, 2012. `http://www.cartes-bancaires.com/IMG/pdf/rapport20112prSiteInternet-2.pdf`.

[Pas08] M Pasquet. La sécurisation d'un système informatique complexe : le cas de la monétique. *Habilitation à Diriger des Recherches, France*, 5, 2008.

[pmp13] Data security standard and payment application data security standard, 2013. `https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf`.

[Sam11] Jolly Samuel. Plateforme monétique pédagogique de l'ensicaen : Enseignement de la monétique par la pratique, 2011.

[Ste98] Jacques Stern. *La science du secret.* Odile Jacob, 1998.