État des lieux et orientations des projets concernant les cartes à puce et autres supports d'identité dans l'Éducation Nationale et l'Enseignement Supérieur.

Dominique Launay
Comité Réseau des Universités
dominique.launay@cru.fr

Résumé

Depuis l'arrivée des cartes à microprocesseur et l'ajout de fonctions cryptographiques dans celles-ci, les cartes à puce sont devenues des supports d'identité et peuvent permettre une authentification forte. La taille de leur mémoire augmentant, elles peuvent embarquer plus de données et éventuellement des applications. Les administrations et les établissements désirent exploiter ces capacités, les motivations étant variées. Le but de cet article est de présenter l'état actuel de l'utilisation de la carte à puce et de ses avatars (token Cryptoki) comme support d'identité avancé dans l'enseignement supérieur notamment à travers l'exemple de mises en oeuvre et de projets. Nous verrons les usages associés ou espérés. Enfin, à travers des projets plus globaux, nous verrons les orientations envisageables pour ces outils.

Mots clefs

Authentification, cartes à puce, identification, monétique, token Cryptoki, interopérabilité

1 Rappel des principaux types de cartes

Les établissements utilisent généralement des cartes magnétiques simples (sans puce) destinées aux personnels pour l'accès aux bâtiments et des cartes d'étudiant comportant des informations visuelles et souvent des code-barres pour les bibliothèques universitaires. Ces cartes d'étudiant ont été successivement en papier, puis en plastique dans un format type carte de crédit qui est souvent le même que le format des cartes à puce[1]. Seules les cartes magnétiques rentrent dans la catégorie des « smartcards ». Ces systèmes sont limités en usage et on ne peut en ajouter de manière aisée. Les informations stockées sont, soit visuelles, soit limitées à un code-barres ou un numéro de série délivré par la bande magnétique. On ne peut pas par exemple y associer un véritable porte-monnaie électronique (stockage du solde sur la carte).

Les cartes à puce permettent d'étendre les usages grâce, entre autre, à une capacité de stockage de données. Il en existe trois types principaux [1] :

– La carte à mémoire : elle embarque simplement un système de fichier. Ce système peut être protégé et les données non modifiables. (Exemple : les télécartes)

– La carte à microprocesseur à contact : cette carte embarque un microprocesseur capable d'exécuter des applications stockées sur celle-ci. Pour certains processeurs, ces opérations incluent la cryptographie (génération de clés, signature, chiffrement). Les tokens Cryptoki (norme PKCS#11[2] développée par RSA [2]) entrent dans cette catégorie. Elle est qualifiée de « carte à contact » car le lecteur nécessite un contact physique avec la carte pour l'alimenter en courant, l'interroger et lui faire exécuter des opérations. On trouve couramment des cartes cryptographiques dotées d'une EEPROM (la mémoire de masse de la puce) de 32ko. (Exemples : les cartes bancaires, les javacards embarquant une JVM)

– La carte à microprocesseur sans contact. Elle intègre une antenne. Le contact physique avec la puce n'est plus nécessaire pour l'interroger. L'alimentation et l'interrogation de la puce passent par un champ électrique ou magnétique. (Ex : la carte Navigo de la RATP). Leur capacité est en général de 1ko à 4ko d'EEPROM. Les puces sans contact implémentent les variantes de la norme ISO-14443 (A, B). Le codage des communications est différent et celui de la variante A est protégé par des brevets.

Deux types de cartes supplémentaires combinent les deux dernières technologies : les cartes hybrides et les cartes duales. Les cartes hybrides contiennent deux puces. L'une des deux est sans contact et l'autre avec contact. Leurs usages sont alors complémentaires. On peut aussi avoir à faire à des cartes duales. La puce présente sur de telles cartes est à la fois sans contact et avec contact. Une antenne est intégrée dans le corps de la carte et connectée à la puce. Elle peut être interrogée à partir d'un lecteur de carte à puce traditionnel ainsi que d'un lecteur sans contact. Bien entendu, ces types de cartes sont pourvus d'un espace mémoire permettant l'exécution des applications et d'un autre pour stocker ces applications et des données.

[1]Format ID-1 définit dans la norme ISO-7816, utilisé aussi bien pour les cartes magnétiques que les cartes à puce.

[2] Ce standard spécifie une API, aussi appelée Cryptoki, pour les périphériques qui contiennent de l'information cryptographique et exécutent des fonctions cryptographiques. Cette API suit une approche objet qui permet à de multiples applications d'accéder à des périphériques cryptographiques multiples indépendamment de la technologie utilisée.

Toutes les cartes à puce sont conçues autour d'un masque. C'est le système d'exploitation. Il ne changera pas au cours de la vie de la carte. Il gère les communications avec les lecteurs ainsi que les accès au système de fichier interne.

Le type de carte qu'on peut utiliser dépend de l'usage qu'on veut en faire. Pour de l'accès aux bâtiments, on choisira naturellement une carte avec une interface sans contact, beaucoup moins contraignante à l'usage (pas besoin d'insérer systématiquement sa carte dans un lecteur).

Certains usages sont définis par la loi, la signature électronique par exemple. Dans ce cas, la carte utilisée devra être capable d'opérations cryptographiques et donc plus généralement à contact avec un code de protection.

En effet, chaque fois qu'une session PKCS#11 commence, il faudrait entrer un code PIN[3] pour s'assurer que le porteur est bien le propriétaire de la carte. Celle-ci prend fin dès que la carte est retirée (et avec elle les transactions en cours). Tant qu'une transaction est en cours, le porteur ne doit pas enlever sa carte d'un lecteur. Dans le cas des ondes électromagnétiques, le lecteur émet un champ. La carte peut sortir de ce champ de manière involontaire. Les cartes sans contact sont donc plus adaptées à des transactions très courtes à l'inverse des cartes à contact.

2 Contexte général

2.1 Des thèmes porteurs

La carte à puce est un sujet d'actualité pour plusieurs raisons. Il y a d'abord des motivations économiques. En effet, la possibilité d'embarquer un nombre croissant d'applications permet d'envisager leur usage en remplacement de nombre de cartes différentes (carte d'étudiant, carte de transport, carte d'accès à des bâtiments...) qui sont souvent des cartes comportant au plus un code barre et/ou une bande magnétique.

On peut imaginer que remplacer toutes ces cartes permettrait d'économiser aux différents acteurs une gestion de cycle de vie par carte en regroupant celles-ci au sein d'une seule. Le support carte à puce permet l'ajout d'informations visuelles traditionnellement utilisées sur les cartes professionnelles ou cartes d'étudiant (code-barres, photo, nom...). Ces processus de personnalisation de cartes sont déjà maîtrisés. Une carte intégrant un porte-monnaie électronique permet de s'affranchir de la gestion de la monnaie et de ses inconvénients : les erreurs de rendu de monnaie sont supprimées, il n'y a plus de monnaie à distribuer et collecter entre différents sites et les distributeurs, s'ils permettent ce mode de paiement, ne contiennent plus d'argent et sont moins exposés aux dégradations.

Il existe aussi des raisons techniques. Une carte à puce est un support d'identité. Cette identité peut se limiter à un numéro de série qui permettra d'identifier le porteur. Mais si la carte est pourvue de fonctionnalités cryptographiques, on peut avoir accès à des fonctions avancées liées au chiffrement asymétrique (authentification, signature, chiffrement) et donc y stocker un certificat personnel. Ce dernier peut fournir directement l'identité patronymique et l'email du porteur. Les fonctionnalités cryptographiques permettant l'authentification forte d'un individu rendent possible l'accès sécurisé à un environnement de travail (HTTPS, EAP/TLS, Smart Logon...).

Dans un cadre multiservice avec plusieurs acteurs, il est aussi possible de choisir d'y stocker des données propres à certaines applications : pour éviter la redondance d'informations variables et propres au porteur (statut, solde) entre la carte et un applicatif, la carte les contient. Les fonctionnalités que peut offrir une carte à puce adresse les domaines de la gestion des identités, de l'authentification et de la gestion de privilèges.

Politiquement enfin, le ministère soutient les opérations liées aux environnements numériques de travail et à l'accès aux ressources informatisées. On pense à l'opération MIPE[4] par exemple. Les projets d'utilisation de cartes à puce profitent du même engouement. L'ADAE[5] les soutient et s'en fait écho [3]. Donner l'accès à une grande variété de ressources électroniques au plus grand nombre et participer aux projets renvoie une image positive des institutions auprès des usagers. Le carte peut alors devenir un outil de communication.

2.2 Besoins des établissements d'enseignement supérieur

Devant l'émergence de projets concernant les cartes à puce, la cellule technique du Comité Réseau des Universités a lancé une enquête [4] afin de cerner les besoins des universités et des établissements d'enseignement supérieur et de recherche. L'autre but était d'avoir une idée plus précise du nombre d'établissements se lançant dans un tel projet.
Les questions posées par l'enquête portaient sur :

- l'état du projet (réflexion, pilote, production) ;
- le public visé par le projet ;
- la coopération inter-établissement ;
- les quantités ;
- les usages potentiels pour chacun des publics ;
- les types de cartes, fabricant, l'utilisation ou non de certificats ;
- les difficultés éventuelles ;

[3] PIN : Personal Identification Number

[4] MIPE : micro portable étudiant, un portable pour un euro par jour

[5] ADAE : Agence pour le Développement de l'Administration Électronique

– les coûts et le recours ou non à des sociétés extérieures.

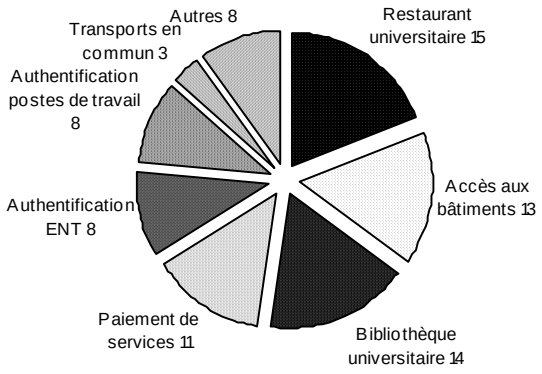

Figure 1 : usages pour les étudiants

Cette enquête a recueilli vingt et une réponses concernant trente sept établissements (universités, CROUS, IUFM, écoles d'ingénieurs). Seule une partie des établissements ayant des projets a répondu a cette enquête (il existe environ deux cent vingt établissements d'enseignement supérieur et de recherche).

Les usages les plus fréquemment cités concernent le restaurant universitaire, le contrôle d'accès aux bâtiments (pour le personnel et les étudiants), la bibliothèque universitaire et la monétique. L'utilisation d'une carte au restaurant universitaire est assimilable à de la monétique plus avancée qu'un simple porte-monnaie électronique du fait de la diversité des publics concernés. Le tarif appliqué est calculé en fonction de la catégorie d'usager (étudiant, personnel, indice) et cette information doit donc être conservée soit dans la carte (utilisation du système de fichier), soit de façon centralisées.

Chacun de ces services est traditionnellement rendu par des technologies plus simples type code-barres (bibliothèque universitaire par exemple) ou cartes magnétiques. Mais la volonté est d'utiliser un support unique. Á moins de combiner ces technologies différentes sur une carte, la multiplication des cartes semble inévitable sans l'utilisation d'une carte à puce. C'est aussi l'occasion de travailler avec d'autres institutions car la mise en place d'une solution pour le restaurant universitaire se fait obligatoirement avec le CROUS. Cela implique un partage d'information ou une compatibilité des informations échangées côté CROUS et côté établissement.

L'interopérabilité des systèmes d'information est donc importante. Elle l'est d'autant plus qu'une solution commune adoptée par un établissement et le CROUS auquel il est attaché implique les autres établissements éventuels pour lesquels les étudiants dépendent de ce même CROUS. Une solution mise en œuvre par ces établissements doit donc être concertée ensemble et avec le CROUS. C'est ce que font les établissements en montant ces projets dans le cadre des UNR[6]. L'exemple des restaurants universitaires peut être étendu à tous les services potentiellement concernés par l'usage des cartes à puce et la participation de plusieurs acteurs. Ce peut être le cas du transport urbain par exemple.

Le type de carte à utiliser est fortement dépendant du type de service associé. Les établissements utilisant ou

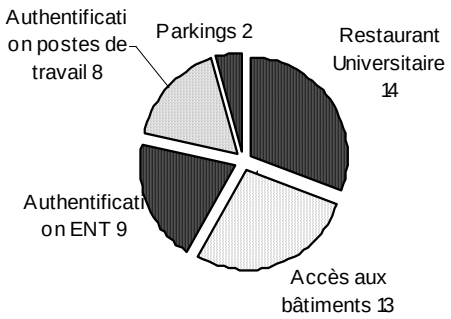

Figure 2 : usages pour les personnels

souhaitant faire du contrôle d'accès avec les cartes se tournent naturellement vers des cartes sans contact type MIFARE ou Calypso[7]. Si le but est de faire de l'authentification forte avec un certificat sur les postes de travail, les cartes avec contact embarquant des fonctionnalités cryptographiques sont plus adaptées. Au cours de l'enquête, les établissements interrogés ont dit préférer les cartes hybrides ou duales (48% des réponses, 38% préférant les cartes avec contact et 14 sans contact seul), permettant le panachage de ces deux usages sur les cartes.

Plus le nombre d'usages espérés pour la carte est grand, plus la variété des solutions l'est aussi. Les choix technologiques adaptés à chacun des services peuvent se révéler incompatibles entre eux lorsqu'on les met en commun. Le besoin d'information et de partage d'expérience se fait alors beaucoup sentir. C'est pourquoi les établissements précurseurs, qui communiquent sur leurs projets, se font contacter par ceux qui en initient de nouveaux.

[6] Universités Numériques en Région. Créées en 2003. Ce sont des consortiums d'établissements d'enseignement supérieur associés aux collectivités locales concernées et à l'État représenté par le préfet de région.

[7] Implémentations partielles de la norme ISO/IEC-14443, MIFARE implémentant ISO-14443A et Calypso ISO-14443B.

3 Projets en cours

Nous allons ici nous intéresser plus particulièrement à quelques projets précis afin d'exposer la variété des solutions possibles faces à des besoins parfois équivalents.

3.1 Exemple d'une carte avec développement privatif : Université de Nancy (avec le CROUS de Nancy-Metz)

L'université avait lancé un appel d'offre cartes à puce dans le cadre du contrat quadriennal 2001-2004 sur la base de deux services : la gestion de temps et la monétique. Cet appel d'offre a été abandonné du fait du nombre trop élevé de solutions présentes. Les cartes proposées embarquaient beaucoup d'applications pour chacun des usages. Cela compliquait la mise en œuvre et l'évolution des produits. Le projet et ses développements ont été repris dans leur intégralité par les équipes de l'université. Celle-ci est en œuvre depuis la rentrée 2005-2006.

Le CROUS ayant mis en œuvre une carte baptisée Clé (Carte lorraine de l'étudiant, 25000 cartes émises 366000€ de budget) [5], les équipes de l'université ont travaillé sur des cartes MIFARE et ont intégré l'application développée pour le CROUS. L'application étant la même, le recto reste celui de la carte Clé mais le verso intègre le visuel de l'université et les informations standards présentes sur une carte d'étudiant. Ceci à l'exception de la mention de l'UFR car c'est une carte de cursus et non une carte annuelle. En effet, les coûts induits par l'utilisation d'une carte à puce étant beaucoup plus élevés que ceux d'une simple carte plastique ou papier, la carte à puce doit être utilisable pendant la durée du cursus. Dans la même optique, le remplacement de la carte en cas de perte est à la charge du titulaire de la carte. L'application de gestion de temps a été développée en interne.

La carte s'adresse aux étudiants et aux personnels de l'université. Lors de la délivrance, les soldes des étudiants ayant déjà une carte Clé CROUS sont reportés dans la nouvelle carte. Des bornes de rechargement pour l'application CROUS vont être mises en place dans l'université.

Afin de préserver la vie privée, les méthodes utilisées pour partager des informations entre les applications sont à sens unique (toutes les informations ne sont pas accessibles à toutes les applications). Des échanges de clés se font entre elles afin d'éviter la redondance. L'identifiant de la carte est unique et construit à partir de son numéro de série.

Les usages intégrés à cette carte sont actuellement :

– carte d'étudiant simple pour justification du statut d'étudiant (examens, accès aux ressources des BU, tarifs réduits accordés au statut d'étudiant) ;

– porte-monnaie électronique CROUS pour les repas au restaurant universitaire ;

– accès aux amphis, salles de TP, salles informatiques et garages à vélo ;

– gestion de temps pour les personnels (pointage).

L'université compte distribuer 18000 cartes. Afin de pouvoir partager des informations entre les collectivités locales et l'université et ainsi rendre la carte multiservice, on évoque la fédération d'identité. En effet, la ville de Vandœuvre-lès-Nancy distribue une carte de vie quotidienne [6] (accès aux transports publics et à la piscine) et a retenu Liberty Alliance avec la communauté urbaine de Nancy (via LASSO) pour l'échange d'un certain nombre d'attributs. Il est aussi envisagé de rajouter une puce pour l'accès logique et peut-être l'utilisation des certificats électroniques.

3.2 Autre exemple de développement privatif : Université de Lyon 1

En 2000, les universités de Lyon 1 et Lyon 2 ont un projet de carte multiservice [7]. La région subventionne alors une étude commune aux deux universités. La faisabilité d'une solution Monéo est étudiée avec une expérimentation sur l'IUT. Il existe deux types de porte-monnaie CROUS, un de type Monéo et une solution privative. Les deux projets divergent et l'Université de Lyon 1 reste sur le projet exploitant une puce Monéo, l'autre établissement s'orientant vers l'autre solution. Malheureusement, le projet est stoppé en Novembre 2004 à cause d'un problème d'agrément entre Billettique Monétique Services (BMS) et la banque émettrice de la carte.

En effet, il faut savoir que les cartes Monéo sont issues du monde bancaire. BMS, qui est un groupement de banques, de sociétés de transports et d'opérateurs de télécommunication, a en charge la conception de ces cartes, leur développement commercial et leur exploitation. Elles doivent être systématiquement émises par une banque. Lorsqu'un établissement veut déployer une solution de type porte-monnaie électronique, il doit obligatoirement trouver un partenaire bancaire. Ces cartes peuvent servir de support de données pour d'autres applications appelées Applications Non Bancaires (ANB). Toute application de ce type doit recevoir l'agrément de BMS qui s'assure de l'étanchéité de l'application avec le système Monéo. En cas de doute, l'application est refusée.

L'établissement décide alors de revenir à une solution simplifiée. Une carte MIFARE pour le personnel est choisie afin de permettre le contrôle d'accès aux bâtiments et le paiement de la cafétéria. La carte est émise par lot et revient environ à 3€ (quelques centimes pour la carte d'étudiant traditionnelle).

Ici les applications sont centralisées. La carte est une MIFARE simple qui délivre un numéro de série lorsqu'elle est interrogée par un lecteur. Elle ne contient pas d'autres données. C'est le système d'information qui gère les privilèges liés à cet identifiant ainsi que le solde disponible pour la cafétéria.

Quant aux évolutions de ce projet, le coût de carte étant assez élevé au regard des services rendus (il n'y a pas de service important qui rendrait indispensable la carte), l'établissement ne se lancerait probablement dans une extension du projet que si il est pas multiservice (carte ville ou projet régional) et s'il implémente des solutions de monétique non privatives (pas de porte-monnaie qui ne serait pas exploitable en dehors de l'établissement).

3.3 Une carte multiservice en partenariat avec le CROUS : Université de Lyon 2

La carte CUMUL [8] est partie de l'étude commune citée précédemment. Elle est actuellement en exploitation pour les étudiants et les personnels. Il s'agit d'une carte MIFARE dans laquelle est intégrée l'application monétique du CROUS. Le budget de l'opération est de 500000€ tout compris sur 3 ans. Certaines opérations nécessitent la frappe d'un code PIN par le possesseur de la carte. Elle permet d'intégrer les services suivants :

– gestion de scolarité (bornes de mise à jour, délivrance de certificats de scolarité, relevés de notes) ;

– contrôle d'accès aux salles ;

– paiement des photocopies et des impressions ;

– paiement à la cafétéria (CROUS) en mode sans contact (problème de flux, un paiement par carte avec contact nécessite l'insertion de la carte dans un lecteur et prend plus de temps) ;

– identification à la bibliothèque universitaire.

Les personnels disposent quasiment des mêmes services (à l'exception des services de scolarité). Des bornes de rechargement monétiques sont disposées sur le campus. Les distributeurs de boisson nécessitent aussi le paiement à partir de la carte. Cela permet d'éviter les problèmes de gestion de monnaie et de dégradation associée. Le concessionnaire est ici gagnant car il s'épargne une gestion d'approvisionnement en monnaie des distributeurs et évite des réparations fréquentes. Les problèmes de dégradation se déportent sur les bornes de rechargement. Celles-ci sont alors installées sur des lieux protégés. La non bancarisation d'un certain nombre d'étudiants a donné lieu à certains aménagements avec le CROUS (rechargement possible contre paiement en espèces aux caisses des cafétérias au lieu d'utiliser les bornes de rechargement par carte bancaire).

30000 cartes ont été distribuées depuis septembre 2004. Les avantages notés sur cette solution multiservice concernent le désengorgement des services de scolarité à certaines heures, la gestion facilitée des clé et serrures (en cas de perte, on invalide la carte). Concernant la bibliothèque universitaire, la migration a été progressive avec, dans un premier temps, l'ajout d'un code-barres sur la carte. Celui-ci n'est plus nécessaire, le changement de lecteurs à la BU permettant maintenant de s'en passer. Cette carte est aussi une carte d'étudiant. Pour des raisons équivalentes à celles de Nancy, les informations visuelles ne comportent pas l'UFR. C'est une carte de cursus.

3.4 Utilisation de Monéo : École Nationale d'Ingénieurs de Tarbes

L'ENIT, en partenariat avec le CROUS Toulouse, a lancé un pilote de carte basée sur Monéo [9]. Le cahier des charges prévoit que la carte permette le contrôle d'accès aux bâtiments (personnels et étudiants) et une solution monétique pour le restaurant universitaire (et éventuellement les autres services payants comme les photocopies). Le CROUS a travaillé avec Monéo sur une application non bancaire intégrée à une carte Monéo permettant de gérer les spécificités de la tarification du CROUS (catégories de tarif du personnel, dossier étudiant au CROUS…). C'est cette solution qui a été choisie. Elle revient à 5€ par carte (tout compris).

Dans un premier temps, pour le pilote, BMS a intégré sa puce sur la carte magnétique utilisée précédemment pour le contrôle d'accès à l'établissement. Dans les prochains mois, ce procédé sera remplacé par un accès sans contact. Des tests sont actuellement en cours. La carte BMS2 devrait intégrer Calypso prochainement (pour tous les services nécessitant une puce sans contact). Cela nécessitera alors le remplacement des lecteurs de cartes.

Afin de gérer les informations contenues dans la carte, une application web permet de mettre à jour des informations comme l'indice de rémunération des personnels (permettant de calculer le tarif). Ces informations sont mises à jour dans la carte lors de la transaction Monéo suivante (effectuée à l'intérieur de l'établissement). Aucun développement interne n'a été nécessaire et une société assure l'infogérance. Celle-ci étudie d'ailleurs une extension des usages pour les services payants supplémentaires.

3.5 Projet Campus Virtuel Ile de France

Le projet CVIF [10] regroupe des universités franciliennes[8] autour d'un ENT et d'une carte à puce multiservices. Il est intéressant à plus d'un titre car les acteurs de ce projet sont nombreux et les choix technologiques le sont aussi. Le projet est en phase d'étude.

Les objectifs premiers de cette carte multiservice sont les suivants :

– identification visuelle,

– code-barres pour la BU,

– accès physique sans contact,

– monétique,

– billettique transport,

– authentification forte (certificats).

Quelques contraintes supplémentaires viennent s'ajouter à cela. En effet, le système de billettique sans contact de la RATP, appelé Navigo, est basé sur une puce Calypso alors

[8] Université Pierre et Marie Curie, Université Paris Sud, Université Paris Nord, Université Évry Val d'Essonne

que sur certains établissement, l'accès physique est basé lui sur une puce MIFARE. Les deux systèmes étant incompatibles au niveau de la puce, il faut se tourner vers des lecteurs qui peuvent intégrer les deux technologies.

Du fait de la diversité géographique des établissements concernés, les étudiants sont susceptibles de demander les services de trois CROUS différents. Il semble alors difficile d'envisager une solution de porte-monnaie privative du fait de la séparation des compatibilités. Il est dès lors difficile d'imaginer trois porte-monnaie différents avec des soldes différents.

Différentes solutions se présentent, intégrant la plupart des services. En partant du principe qu'un porte-monnaie privatif est difficilement envisageable dans ces conditions, la solution la plus répandue concernant cet usage est alors Monéo. Mais cette technologie est incompatible avec l'utilisation des certificats X.509 dans l'état actuel des choses. Il est donc peu probable qu'à l'heure actuelle une seule carte accomplisse tous les services demandés à l'origine. Le projet semble s'orienter vers un état intermédiaire qui n'inclurait pas l'authentification forte dans la carte mais regrouperait les autres services en attendant de pouvoir voir un jour la carte unique. Il semble en tout cas qu'il faille deux cartes pour rendre tous ces services.

Parmi les différentes possibilités, les deux suivantes paraissent envisageables :

– cohabitation d'une carte universitaire cryptographique (avec accès physique MIFARE, identification visuelle et BU) et d'une carte monétique et billettique (BMS2) ;

– cohabitation d'une carte universitaire BMS2 (avec identification visuelle, accès physique Calypso, monétique et billettique Calypso) et d'une carte cryptographique ou d'un token pour l'authentification forte.

Les autres solutions non compatibles avec Navigo paraissent inenvisageables.

4 Conclusion

À travers ces différents projets, on peut voir les difficultés rencontrées dans un projet de cartes à puce. D'un côté la nécessité de rendre la carte viable économiquement (du fait de son coût) incite à multiplier les services qu'elle peut rendre et à travailler avec d'autres acteurs. Les UNR sont le cadre idéal pour cela car les collectivités locales sont parties prenantes. Le travail doit donc être effectué dans un souci d'interopérabilité des technologies et des systèmes d'informations, dans le respect de la vie privée.

Mais la multiplication des services et des acteurs complique le choix d'une solution satisfaisant les contraintes technologiques et opérationnelles de tous. De plus, cela augmente les probabilités de pannes de tout ou partie d'un élément. Il faut probablement prévoir un accueil unique concernant la carte afin d'orienter l'étudiant dont la carte ne fonctionne plus à l'université ou dans le métro. Les orientations vers l'authentification forte à base de carte à puce ne semblent pas séduire beaucoup. Il est probable que la lourdeur d'un processus de délivrance de certificat associée à la difficulté de trouver des cartes cryptographiques compatibles avec les autres services indispensables (par exemple la monétique) sont les principaux freins.

Un certain attentisme semble être de mise car on nous annonce des projets qui pourront remettre en cause tout ou partie des cartes de campus. Par exemple, la future carte nationale d'identité sécurisée pourra-t-elle assurer les besoins d'authentification forte et de signature électronique ?

Un groupe de travail interministériel réuni par l'ADAE a récemment travaillé à la rédaction d'un cahier des charges type à l'intention des ministères pour les futurs appels d'offres « carte d'agent public »[11]. Un socle commun appelé socle IAS[9] pour les futures cartes à puce administratives a été mis au point (en cours de convergence avec le socle commun allemand) [12]. Il va concerner les futures cartes d'identité [13], cartes d'agent public, cartes de vie quotidienne et cartes vitale 2, compatibles alors entre elles. Ce socle commun définit la structure des cartes à puce et les zones de stockage utilisables par d'autres applications. Les usages associés par défaut à ce socle concernent l'authentification, le chiffrement et la signature électronique.

La carte à puce Monéo n'inclut pas ce socle. Mais le déploiement des cartes IAS et leur généralisation pourraient inciter de tels consortiums à y intégrer leurs solutions. On peut espérer que l'avènement de ces cartes et l'implémentation de ce socle commun simplifient et pérennisent les choix que pourront faire les administrations.

[9] Socle commun IAS : Identification, Authentification, Signature, spécification technique élaborée par le GIXEL

5 Bibliographie

[1] Wolfgang Rankl, Wolfgang Effing, *Smart Card Handbook Third Edition.* Wiley & Sons, 2003.

[2] RSA labs, *PKCS.* Site web. http://www.rsasecurity.com/rsalabs/node.asp?id=2124

[3] ADAE, *Les 140 fiches du projet ADELE*. Site web. http://www.adae.gouv.fr/rubrique.php3?id_rubrique=85

[4] CRU. *Synthèse de l'enquête réalisée du 16 décembre 2004 au 7 février 2005*. Site web. http://www.cru.fr/igc/cartes_puce/resultats_enquete.html

[5] CROUS Nancy-Metz. *Monétique*. http://www.crous-nancy-metz.fr/Restauration/monetiquessommaire.htm

[6] ADAE. *ADELE 8 : La carte de vie quotidienne.* Site web. http://www.adae.gouv.fr/article.php3?id_article=364&artsuite=4#sommaire_1

[7] Université de Lyon 1. *Carte CUMUL.* Site web. http://cri.univ-lyon1.fr/projet/edit.asp?num=6

[8] Université de Lyon 2. *Carte CUMUL Lyon 2*. Site web. http://etu.univ-lyon2.fr/etu1179/0/fiche___article/

[9] André Arguimbaud, Jean-Claude Blanc. *Carte étudiant multi-service, Projet CROUS-ENIT*. http://www.csiesr.jussieu.fr/IMG/pdf/cartes-cr-enit-crous-tlse-2005.pdf

[10] Université Paris Sud. *Lancement du projet CVIF*. Site web. http://www.u-psud.fr/ja.nsf/cvif?OpenPage

[11] ADAE. *ADELE 76. : La carte d'agent public.* Site web. http://www.adae.gouv.fr/article.php3?id_article=421&artsuite=3

[12] ADAE. *ADELE 125. : Standard commun à l'ensemble des cartes à puce.* Site web. http://www.adae.gouv.fr/article.php3?id_article=378&artsuite=2#sommaire_1

[13] ADAE. *ADELE 35 : Carte nationale d'identité électronique.* Site web. http://www.adae.gouv.fr/article.php3?id_article=379&artsuite=2#sommaire_1