CRU

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

JRES 2005

Dominique Launay

6 décembre 2005 - Marseille

Qu'est-ce qu'une carte à puce ?

« Define: Carte à puce » dans Google, 3 réponses :

- *carte plastifiée aux dimensions de 85,6 × 54 millimètres comportant un circuit intégré (la puce).* http://fr.wikipedia.org/wiki/Carte_à_puce
- *Support cryptographique physique, permettant la fabrication et le stockage sécurisé du certificat électronique* http://www.keynectis.com/glossaire.html
- *Carte de dimension similaire à une carte de crédit, dans laquelle il est possible de charger de l'argent électronique.* http://adevim.ifrance.com/dicocont/dicoc.htm

Standards

- Norme ISO 7816 : format et caractéristiques des cartes à puce avec contact
- Normes ISO 14443, ISO 10536, ISO 15693 : cartes sans contact
- PC/SC : standard d'intégration des cartes à puce pour les ordinateurs personnels
- PKCS : standards cryptographiques. Le 11 et le 15 permettent d'utiliser les cartes à puce (dotées de coprocesseur crypto) et tokens cryptographiques

- Usages
- Intérêts des cartes à puces ?
- Enquête réalisée par le CRU
- Projets en cours
- Besoins des établissements
- Perspectives

Usages

- Cartes à mémoire :
  - Cartes prépayées (télécartes)
  - Cartes d'identification dans des systèmes non critiques (assurance santé)
- Carte à microprocesseur :
  - Identification + authentification
  - Contrôle d'accès (physique et logique)
  - Stockage sécurisé
  - Signature électronique, chiffrement
  - Chargement de nouvelles applications
  - Cartes uniquement cryptographiques
  - Porte-monnaie

Usages

- Contact :
  - Authentification poste de travail et logicielle
  - Signature électronique, chiffrement
  - Porte-monnaie
  - Carte de crédit
- Sans contact :
  - Contrôle d’accès physique
  - Billettique (transports en commun)

Usages

- Solution : les cartes hybrides ou les cartes duales :
  - Cartes hybrides : déconnexion des deux interfaces
  - Cartes duales (porte-monnaie en contact + et billettique sans contact par exemple)

- Usages
- Intérêts des cartes à puces ?
- Enquête réalisée par le CRU
- Projets en cours
- Besoins des établissements
- Perspectives

Raisons économiques

- Multiplication des services sur une puce : remplacement de plusieurs cartes
- Durée de vie et gestion de cycles de vie
- Processus de personnalisation souvent déjà maîtrisé
- Porte-monnaie : économie de gestion de monnaie (rouleaux, caisses, erreurs…)
- Gestion des clés
- Partage des coûts si plusieurs partenaires

Raisons techniques

- Support d'identité
- Informations stockées
  => un endroit sécurisé pour stocker des données à partager entre plusieurs systèmes (carte professionnelle + restaurant du personnel)
- Applications embarquées
- Cryptographie asymétrique (certificat => identité patronymique et @email)
- Authentification forte pour :
  - Accès aux postes de travail (smart logon, pam_pkcs11)
  - Accès aux ENT (https)
  - Accès au réseau (802.1x)

Raisons politiques

- Sujet d'actualité :
  - Carte de Vie Quotidienne, Identité Nationale Electronique Sécurisée, Vitale2
  - MIPE
- Projets soutenus par l'ADAE
- Renvoi d'une image positive
- Outil de communication

- Usages
- Intérêts des cartes à puces ?
- Enquête réalisée par le CRU
- Projets en cours
- Besoins des établissements
- Perspectives

Enquête réalisée par le CRU

- Écho de projets (Lyon 1 et Lyon 2, Nancy-Metz, ENIT)
- Projets en gestation
- Buts :
  - Cerner les besoins
  - Quantifier les projets
  - Mutualiser les connaissances
- 2 mois
- 37 établissements

Thèmes abordés

- État des projets
- Publics visés
- Coopération inter établissements
- Quantités
- Usages potentiels
- Types de cartes, technologies utilisées
- Difficultés éventuelles
- Coûts et recours à des sous-traitants

- Usages
- Intérêts des cartes à puces ?
- Enquête réalisée par le CRU
- Projets en cours
- Besoins des établissements
- Perspectives

Projets en cours

- Du plus simple au plus complexe :
  - Carte simple sans ajout de fonctionnalité
  - Porte-monnaie électronique
  - Carte avec ajout d'une ou deux applications
  - Carte multiservice
- Partenaires variés (souvent avec le CROUS)
- Liste non exhaustive

Université de Lyon 1

- Projet ambitieux :
  - Lyon 1, Lyon 2 et CROUS
  - Deux types de solutions monétique CROUS :
    - Embarquée dans une application sur carte
    - Carte Monéo
  - Choix de Monéo
  - Projet bloqué pour problème d'agrément

Université de Lyon 1

- Solution simplifiée :
  - Carte MIFARE simple pour personnel
  - Porte-monnaie privatif (cafétéria du personnel) :
    - Identification par numéro de série
    - Les soldes sont gérés par le SI
  - Contrôle d'accès :
    - Identification par numéro de série
    - Privilèges gérés par le SI
  - Services limités pour le coût (3€/carte)
  - 5000 cartes distribuées

Université de Nancy

- Appel d'offre sur gestion de temps + monétique :
  - réponses trop complexes (beaucoup d'applications pour chaque service)
  - Mise en oeuvre et évolution trop complexes
- Carte CROUS Nancy-Metz baptisée Clé (Carte lorraine de l'étudiant, 25000 cartes, budget 366000€)
- Travail sur cartes MIFARE :
  - Intégration de l'application CROUS
  - Application de gestion de temps développée en interne

Université de Nancy

- Caractéristiques :
  - Recto identique à la carte Clé
  - Verso personnalisé
  - Carte de cursus (coûts)
  - Carte distribuée au personnel
- Usages :
  - Carte d'étudiant pour justification de statut
  - Porte-monnaie CROUS pour RU
  - Accès aux amphis, salles de TP, informatiques et garages à vélos
  - Gestion de temps pour le personnel

Université de Nancy

- Chaque application ne peut accéder qu'aux données qui lui sont utiles (respect de la vie privée)
- Évolutions :
  - Rendre la carte multiservice (compatible avec les applications de la communauté urbaine)
  - Authentification logique (certificats : nécessite une puce supplémentaire
- 18000 cartes escomptées

Université de Lyon 2

- Carte CUMUL issue du projet cité précédemment
- Application CROUS intégrée dans une carte MIFARE
- Budget : 500000€ tout compris sur trois ans
- 30000 cartes
- Partenaires :
  - Cartes Gemplus
  - Solutions Monécarte
  - RW conseil pour assistance
- Carte étudiants et personnels

Université de Lyon 2

- Services proposés :
  - Gestion de scolarité
  - Contrôle d'accès aux salles
  - Paiement des photocopies et impressions
  - Paiement à la cafétéria en mode sans contact
  - Distributeurs de boissons
  - Identification à la BU (plus de code-barres)
- Gains constatés :
  - Dégradations sur distributeurs en baisse
  - Gestion des clés et serrure facilitée

École Nationale d'Ingénieurs de Tarbes

- Cahier des charges :
  - Contrôle d'accès bâtiments
  - Monétique pour RU (+autres services éventuels)
- Partenariat avec CROUS Toulouse :
  - Carte Monéo
  - Application non bancaire CROUS intégrée

École Nationale d'Ingénieurs de Tarbes

- Pilote :
  - Carte magnétique traditionnelle
  - Ajout de la puce Monéo
- En cours :
  - Passage en sans contact
  - BMS2 avec Calypso intégré
- Au total :
  - 5€ par carte
  - Aucun développement en interne
  - Applicam assure l'infogérance

CVIF (Campus Virtuel Île de France)

- Objectifs :
  - Carte étudiant (id. visuelle)
  - Code-barres BU
  - Accès physique sans contact
  - Monétique
  - Billettique transport
  - Authentification forte

CVIF

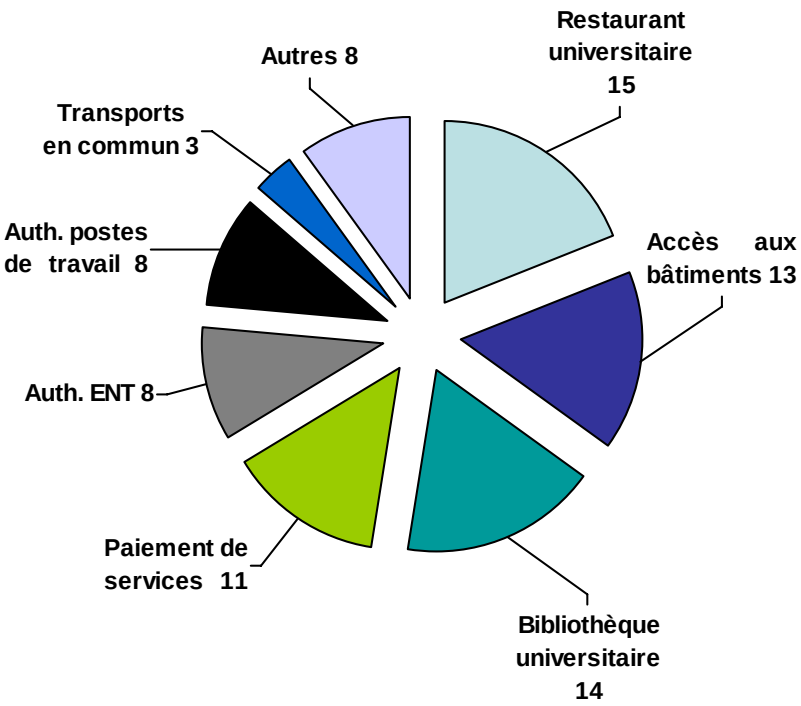
- Contraintes :
  - Des accès sans contact existent dans certains établissements, basés sur MIFARE
  - Trois CROUS concernés : la solution monétique doit être répandue (Monéo)
  - La carte doit permettre l'utilisation de certificats X.509
  - Billettique RATP (Navigo) basée sur Calypso

CVIF

- Incompatibilité de toutes ces contraintes actuellement
- Orientation temporaire sur deux cartes
- Deux possibilités :
  1. Une carte universitaire crypto (avec MIFARE id. visuelle et BU) + deuxième carte monétique et billettique (BMS2)
  2. Une carte universitaire BMS2 (id. visuelle, accès physique Calypso, monétique et billettique Calypso) + carte crypto pour authentification forte

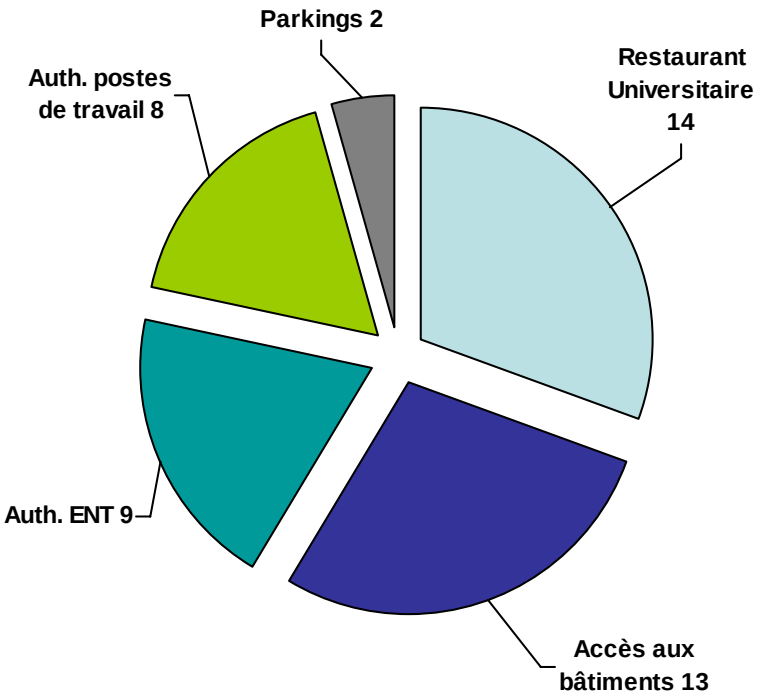
- Usages
- Intérêts des cartes à puces ?
- Enquête réalisée par le CRU
- Projets en cours
- Besoins des établissements
- Perspectives

Usages étudiants



- Beaucoup de services
- Orientés vers la vie étudiante
- Deux thèmes principaux :
  - Monétique
  - Identification

Usages pour le personnel



- Services moins variés
- Plus professionnels
- Monétique moins prégnante

Besoins des établissements

- Usages fréquemment cités :
  - RU
  - Contrôle d'accès bâtiments
  - BU
  - Monétique (services autres que RU)
- Regroupement de moyens auparavant séparés (code-barres, tickets, carte étudiant, carte magnétique…)
- Services d'origine diverse (CROUS, communes, transport, UNR…)

Besoins des établissements

- Type de carte dépendant de l'usage
  - Sans contact pour contrôle d'accès
  - Solutions hybrides ou duales privilégiées
- Peu de certificats (3 réponses)
- Peu de projets passés au stade exploitation
- Manque de retour sur expérience (présent article + www.cru.fr)

Monétique

- Monéo
  - BMS
  - Porte-monnaie partagé
  - Toujours émis par une banque
  - Applications non-bancaires mais cohabitation limitée
- Porte-monnaie privatif
  - Interne à l'établissement
  - Indépendant du secteur bancaire

- Usages
- Intérêts des cartes à puces ?
- Enquête réalisée par le CRU
- Projets en cours
- Besoins des établissements
- Perspectives

Perspectives

- Difficultés générales :
  - La carte doit être viable économiquement
  - Elle doit rendre beaucoup de services
- Résultat :
  - Multiplication des partenaires
  - Contraintes augmentées
  - Solutions très variées mais pas de solution miracle

Perspectives

- Projets nationaux :
  - Carte INES
  - CVQ
  - Carte agent public
  - Socle IAS
- Interopérabilité
- Orientés crypto (IGC)
- Simplification ou choix supplémentaires ?
- Coûts ?