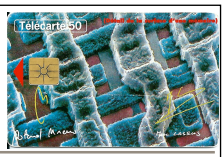
Carte à puce et Technologies de l'information

26 ans Rétro (-per-) spectives

Pierre Paradinas
Cnam
Chaire Systèmes Embarqués

le cnam

Propos



L'entrelacement des technologies de l'information,

de l'informatique et de la carte à puce

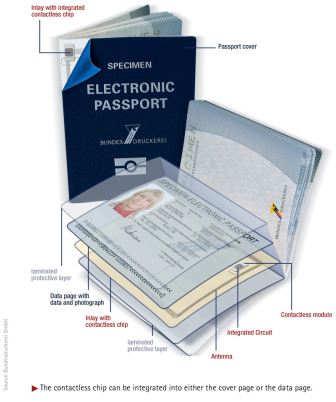
le cnam

26 ans...

- En 1986 durant la conférence IFIP-Sec, il y avait un workshop sur la carte à puce...
- Présentation de Biocarte : une carte à puce utilisée pour le suivi de santé des personnes et son intégration dans un réseau de professionnel de santé...
  - tout un programme (pas réalisé d'ailleurs au niveau nationale !)
  - à l'époque un sujet de thèse (soutenue en novembre 1988 par P. P.)
  - en 1985, le sujet (initial) était comment utiliser une carte à puce comme *base de faits pour un système expert médical*
    - (i) on l'a fait !
    - (ii) mais on a aussi passé *plus* de temps sur la réalisation et le déploiement de l'application carte santé
    - (iii) proposition de langage de développement pour lecteur... puis **la carte**

Les applications de la carte

- Téléphonie Mobile
- Paiement
- Gouvernement/Santé
- Transport
- Entreprise



P. Paradinas - 2011
CC BY NC SA
le cnam

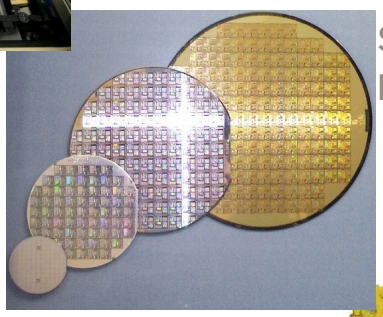
Card Production Figures

- From Eurosmart (contact card)

Millions of Units (Mu)	2010 global	2011 forecast	2011 vs 2010 % growth
Telecoms	4 200	4 600	10%
Financial services – Retail – Loyalty	880	1 010	15%
Government – Healthcare	190	225	18%
Transport	65	80	23%
Pay TV	110	125	14%
Others (including corporate ID)	75	80	7%
TOTAL	5 520	6 120	11%

Les acteurs

De Larue, Imprimerie Nationale, OCS, Solaic, ...



SGS-Thomson (STM), Motorola, Inside-Secure,...

Schlumberger

CII-Honeywell Bull

SPS-7 (1984) MC 6820 @16,67Mhz

Crédits photo : G&D, Wikipedia, http://www.keywordpictures.com, FEB

Un acteur de l'IT : Bull

- Les acteurs naissant de l'industrie sont Bull, Sligos, Schlumberger,...
  - origines variées
- Un politique dirigiste est de mise de la part de la Direction Générale des Telecoms (DGT)
- La carte CP8 de Bull est la référence
  - Bull crée une filiale : Bull CP8 (la carte à micro des années 80 ou les 8K (bits) de la première carte)

La bataille des masques

1 Masque = 1 Carte = 1 Système d'exploitation

Masque (Silicium) = Code (ROM)

Ce ne sont pas des SE !

Les SE de la première génération

- Masque M4 de Bull
  - à la demande de la banque (GIE-CB)
  - pour une machine réduite : Processeur 8 bits; ROM = 1,6 ko; EPROM = 1 ko et RAM = 36o
  - en plus de la cryptographie (Telepass) et de la communication, une organisation mémoire en zones figées à la personnalisation (ZS, ZC, Memac, ZT, ZL et ZF)
    - mapping strict
    - fonction figée
- 1987, durant la conférence Smart Card 2000 à Vienne :
  - conversation privée Ph Maes à P.P : «Il faudrait qu'autour des produits carte se construise un écosystème de développeur à la Apple...»

Le COS

- Le Card Operating System
  - SGS-Thomson fournit des composants pour Bull, ... et puis il faut aider la filière silicium,...
  - SGS propose le COS
    - (Gilles Lisimaque est le COS, il est aussi le «Directeur Informatique» !)
  - Le COS
    - pour une machine réduite : Processeur 8 bits; ROM = 2 ko; EPROM = 1 ko et RAM = 48o
    - zone modulable, fichiers et répertoires
    - possibilité d'ajouter son propre code !
- btw : la marque a été déposée par Schlumberger...

Gemplus

- Un des grands cabinets de consulting précise à la demande de SGS-Thomson que la carte n'a pas d'avenir (merci) !
- 1989 création de Gemplus
  - Extrait de Gemplus 15 ans – Historique pour l'année 1990
    - « Et parce que déjà nous savons que la R&D est vitale au développement de notre activité, nous créons en collaboration avec de grandes universités françaises le groupe de recherche RD2P axé sur la gestion des dossiers portables, notamment dans le domaine de la santé.»

RD2P

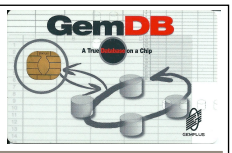
Des cartes et des technologies IT

- Les domaines de la banque et du GSM sont assez figés par :
  - les normes et standards
  - le marché
- Les applications du dossier portable, du contrôle d'accès laisse un espace plus grand aux technologies de l'informatique et à l'innovation
- Des technologies et des cartes…

DosCard

- Gemplus propose la DosCard
- DosCard = Disquette.
  - La carte est assimilée à une disquette. Le PC comporte donc un lecteur de carte et un driver pour gérer ce type de carte
  - les fichiers MS Dos sont protégés par le PinCode de la carte
  - un driver spécifique transforme les commandes Dos:
    - la carte qui est vu comme un périphérique
    - > F:list | copy | delete,...sont transformés en commande pour la carte
- on reviendra sur la connexion avec le monde des PCs...

SQL/CQL



- Un des points importants dans les applications cartes : est de structurer et d'interroger les données ?
  - les fichiers peu adaptés à ce besoin (en 1990 pas d'XML)
  - la sécurité est sur le fichier (granularité forte)
- Proposition CQL : Card Query Language
  - organisation en table et interrogation à la SQL
  - granularité fine basée sur les vues (select & view)
  - c'est un standard ISO 7816-7 à la fin des années 90
    - Merci le SEPT (Paul Deligne et Jean-Claude Pailles !)

Entrer dans le PC

- Le monde du PC devient central. Il est impératif pour la carte d'y être
- L'Alliance HP/Informix/Gemplus se fait au départ autour de CQL mais finira sur des produits de contrôle d'accès aux PCs...
- Microsoft et l'écosystème de la carte travaille à l'intégration de la carte dans le monde Wintel
  - PC/SC deviendra le standard de fait de communication avec la carte dans le monde PC avec la première version en 1997
    - (http://www.pcscworkgroup.com)
    - des version Unix et Mac suivront
- Il y aussi un gros travail sur le chipset en vue de l'intégration dans les PC sous forme de lecteur intégré et ou dans le clavier

Et Java dans tout ça

- Début des années 90, on parle (toujours) de systèmes d'exploitation pour les cartes qui vont au delà des nouveaux masques
  - MP, TB100, MPCOS qui sont des masques multiapplications (services)
  - le besoin de traitements spécifiques est de plus en plus fort
    - apparition d'interpréteur et de langage de script
    - microCombo (RD2P-Lille), Tosca (NL), Multos/Natwest, (UK),...
- Fin 1996, Schlumberger introduit Java Card 1.0
  - C'est un tournant pour la carte !
- Les acteurs de la carte créent le Java Card Forum
  - Premier (grand) chantier commun

La bagarre est rude (Java pas Java ?)

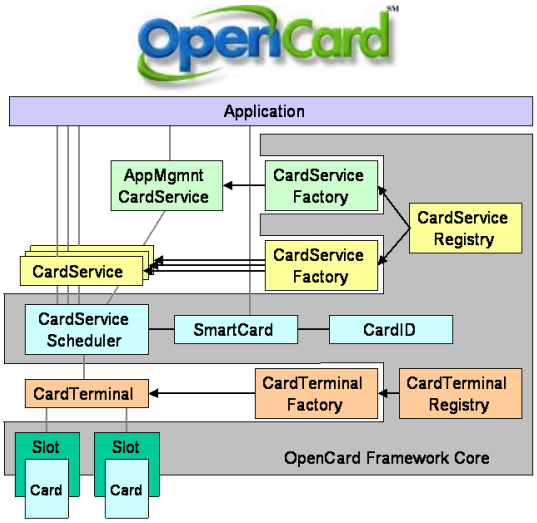
- Autres approches
  - Script de gestion des cartes à l'intérieur et/ou à l'extérieur de la carte
  - Interpréteur divers et variés
  - OO : Carte = (code+donnée)
    - J-M Geib (communication privée) et publication à ACM/Sigops
    - *New directions for integrated circuit cards operating systems,* P.P & Jean-Jacques Vandewalle, January 1995, SIGOPS Operating Systems Review
- W4SC
  - Microsoft propose aussi sa version de Smart Card
    - Windows keys
    - Reviendra aussi au début des années 2000 avec un carte .Net réalisée par une start up Californienne (Hiveminded)

Java Java Java Java... Java Card

- Java est adopté par le monde de la carte
  - Le GSM passe aussi à Java Card (même si...)
  - La carte Java est la plateforme Java la plus répandue dans le monde
- La communauté académique se mobilise
  - de très nombreux travaux sur la sécurité
    - l'isolation, le firewall,...
    - le PCC
    - la vérification de BC embarqué
- Des déceptions
  - ...

Middelware

- Pas ou peu de travaux travaux scientifiques…
- Des efforts pour formaliser des services de haut niveau en Java avec l'Open Card Forum (IBM, Gemplus, SUN, Visa,…)
- JINI-Card
- PC/SC au niveau "service"
- Voir aussi WinScard
- et la 24727

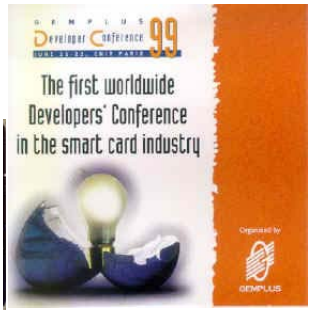


Java Card oui mais

- Java est utilisé :
  - par les industriels comme un bon langage de réalisation d'application
  - pour faciliter les portages et les développements d'applications (cardlet)
- Mais
  - Java Card comme la carte est toujours "engluée" dans
    - un protocole ancien basé sur les APDUs,
    - Pas d'architecture globale sur le modèle Java avec des objets distribués (RMI)
      - Voir thèse de Jean-Jacques [1997] (avec les DMI basé sur Corba !)
    - un modèle ou la carte est que "serveur"
- **où est le CardStore ?**

Le défi du logiciel

- À la fin des années 90 au moment de la bulle internet, les acteurs majeurs se sont positionnés dans le logiciel :
  - Gemplus a créé Gemplus-Software
  - Schlumberger a acquis SEMA en 2001
    - Revendu plus tard 1,5 b$ à Atos
  - En fait deux échecs !



Les enjeux sont néanmoins importants

- Marc Lassus prenait souvent l'exemple de "l'iceberg" ou "de la salle de bain" pour dire que derrière 1$ carte il y 20$ de produits et services...
- Dans les GSM il y a toute la gestion des cartes et des services à distance
- Par exemple aujourd'hui dans le cas du M2M
  - la carte est fixée sur les dispositifs de type téléphone mobile
  - l'opérateurs de M2M ne peut pas choisir l'opérateur au moment de la fabrication, il faut donc revoir/repenser la chaine de personnalisation de la carte
    - Enjeu en cryptographie pour chaine de confiance
    - Enjeu en logiciel-cycle de vie- en lien avec la confiance

Les défis de la carte

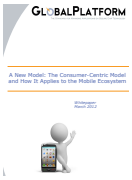
- Connexion/connectique/intégration
  - SIM et MMC et/ou SD card
  - interface USB pour la carte et le lecteur
- Cardlet Store
  - le modèle est passé à coté de la carte ou la carte est passée à coté
- La grande question récurrente : “Où mettre le calcul et les données ?”
  - carte—device—cloud ??????????????????????????????
- et la carte peut aussi disparaître !
  - voir la position d’Apple

La carte : image de la personne numérique

La carte peut disparaitre.

Par contre la représentation numérique de la personne, elle restera !

La carte et ses technologies s(er)ont un des meilleurs candidats pour la représentation numérique de la personne ?



Voir aussi le livre blanc de GP vis à vis du “user centric”

Merci

Questions/Commentaires