GEMPLUS

Your Passport to the Digital Age

Prise en compte de la dimension personnelle dans les nouveaux réseaux

Olivier Potonniée
Gemplus Research Labs
http://research.gemplus.com

Sommaire

1. L'évolution des réseaux nécessite une gestion de la complexité des *droits d'accès* et de *l'environnement de l'usager*
2. Trois études de cas où la carte à puce intervient : PNDS, Jini, Cesure
3. A l'avenir cette gestion de la complexité doit s'étendre à *la mise en œuvre* des applications
4. Où et comment la carte à puce peut-elle intervenir ?

Les réseaux aujourd'hui

- Omniprésence des accès aux réseaux large-échelle
  - Téléphonie mobile
  - Internet
  - Télévision Numérique
- Multiplication des terminaux numériques
  - PDA, téléphone mobile, PC maison, PC bureau, SetTopBox
- Début d'interconnexions de ces réseaux entre eux

Services et données

- Services spécifiques
  - Les services sont adaptés à un réseau, et dédiés à un type de terminal
  - Chaque [type de] service/réseau à son propre système/service de contrôle d'accès
- Données dispersées
  - Multiplication des sources, des médias et des contenus
  - Pas de solution générique pour personnaliser leur structure et la navigation/recherche/découverte

⇨ **Besoin de simplification**

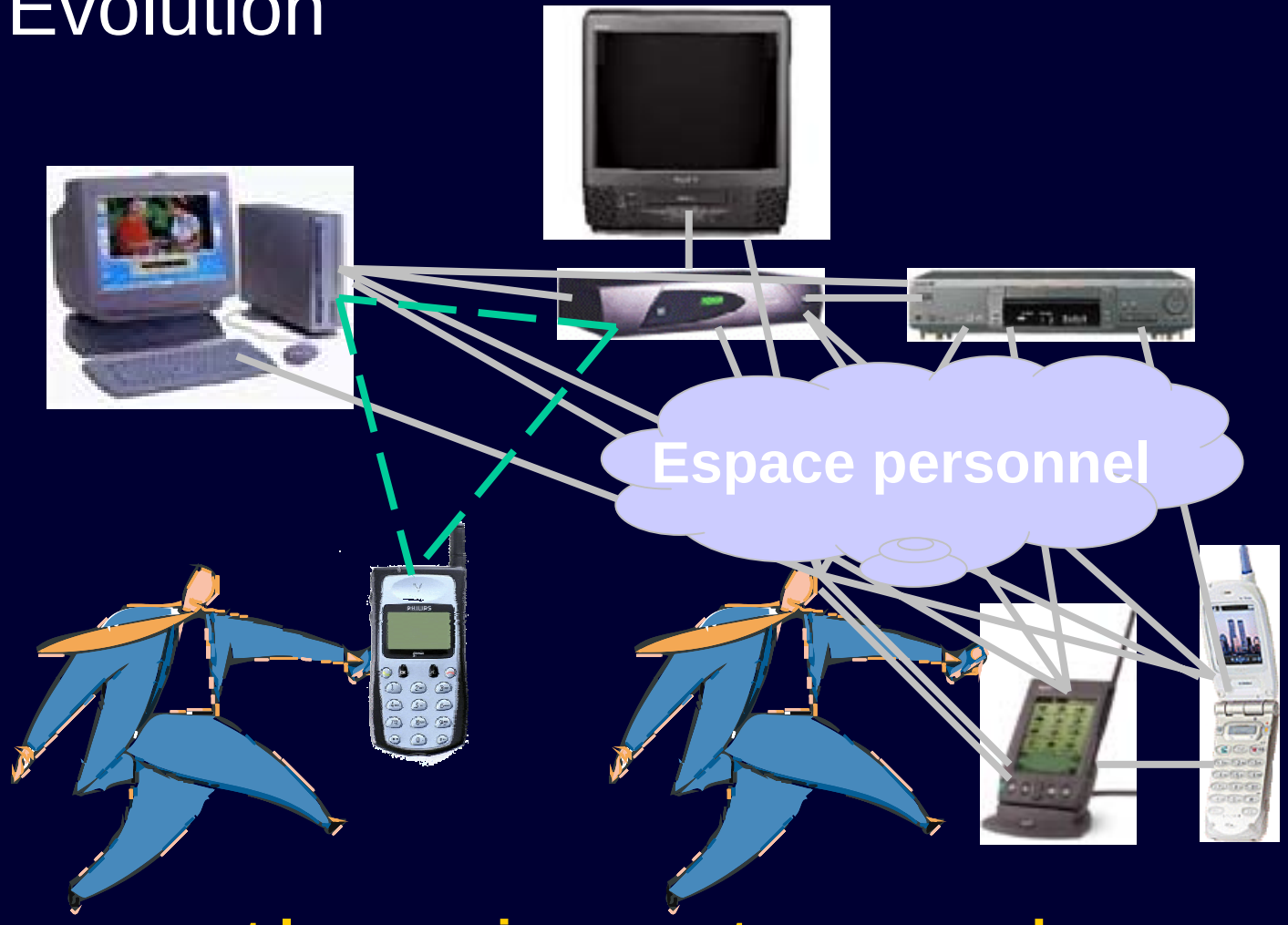
Homogénéisation

- Convergence technologique en cours : IP, Java, HTML/XML, MPEG-x
  - Internet sur PC : Web, Napster, Internet TV...
  - Téléphonie: mobiles J2ME MIDP, IP dans UMTS...
  - TV : ATVEF, DVB-MHP, TV Anytime...
- On peut espérer un homogénéisation des services pour bientôt
  - Le même Web / e-mail sur mobile, PC et TV
  - Les même services en-ligne
  - Données portables d’un terminal à un autre

Une informatique « diffuse »

- De + en + de petits terminaux numériques communicants (téléphones, appareils ménagers, *etc.*)
  - Capacités de calcul et de communication limitées
- De + en + de types de réseaux accessibles (GSM, UMTS, IrDa, Bluetooth, Havi, *etc.*)
  - L'accès aux applications peut prendre plusieurs chemins
- De - en - d'applications en pure mode « client léger / serveur lourd » (modèle Web)
  - Traitements déportés près de l'usager à cause des communications limitées et répartis entre plusieurs petits équipements

Evolution



L’usager et les services sont au cœur de ces nouvelles infrastructures

Gestion de la complexité

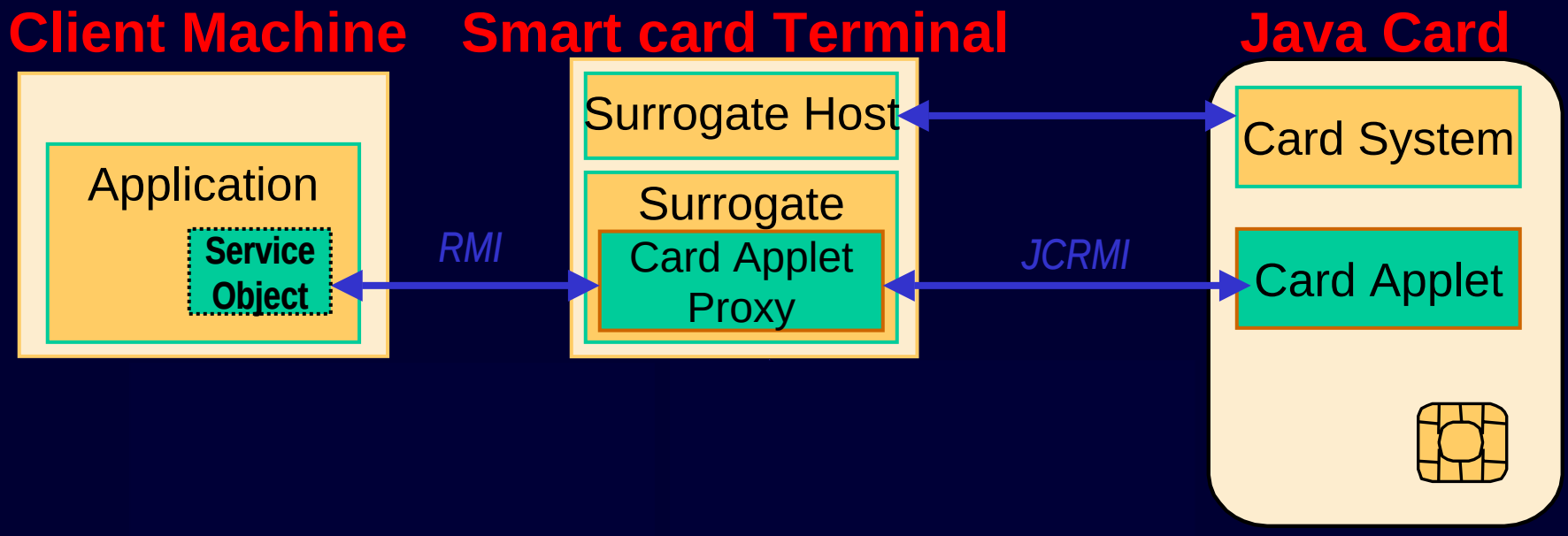
- Gestion des droits d'accès (aux objets, services, données)
  - besoin de pouvoir s'authentifier comme étant le propriétaire
  - besoin de pouvoir donner des droits, temporairement ou définitivement (ex: droit d'utilisation ou de visualisation)
- Environnement personnalisé
  - Accès rapide aux services souscrits
  - Prises en compte des préférences (langues, thèmes, etc.)
  - Interactions adaptées (pubs ciblées, moyen de paiement, etc.)
- Maintient de la cohérence dans un environnement *mouvant*

Rôles de la carte à puce

- Elément de **sécurité** : gestion générique des droits
  - Profiles complexes: multi-applications, multi-domaines
- Elément de **personnalisation** : gestion générique de l'environnement
  - Modèle serveur-serveur, multi-plateformes, multi-réseaux
- Elément de **déploiement** : gestion générique des applications réparties
  - Mise à disposition, répartition, cycle de vie, surveillance, maintenance, administration

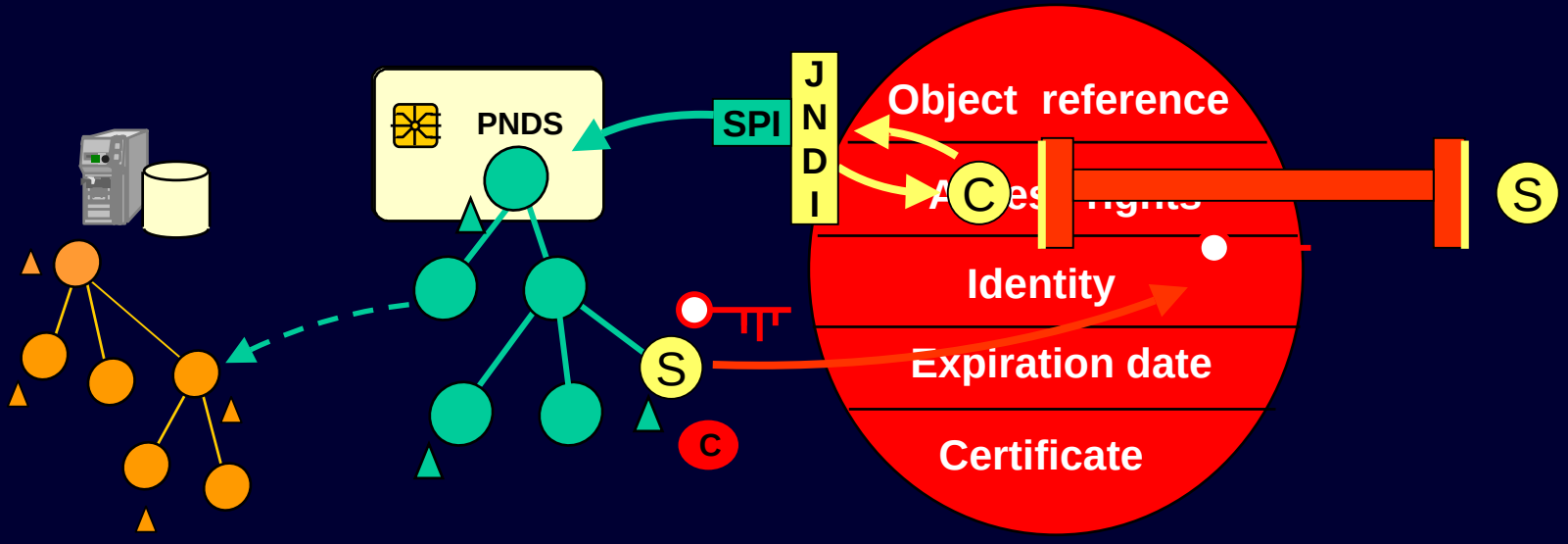
Etudes réalisées (1/3) : Jini

- Insertion de services carte dans une communauté Jini



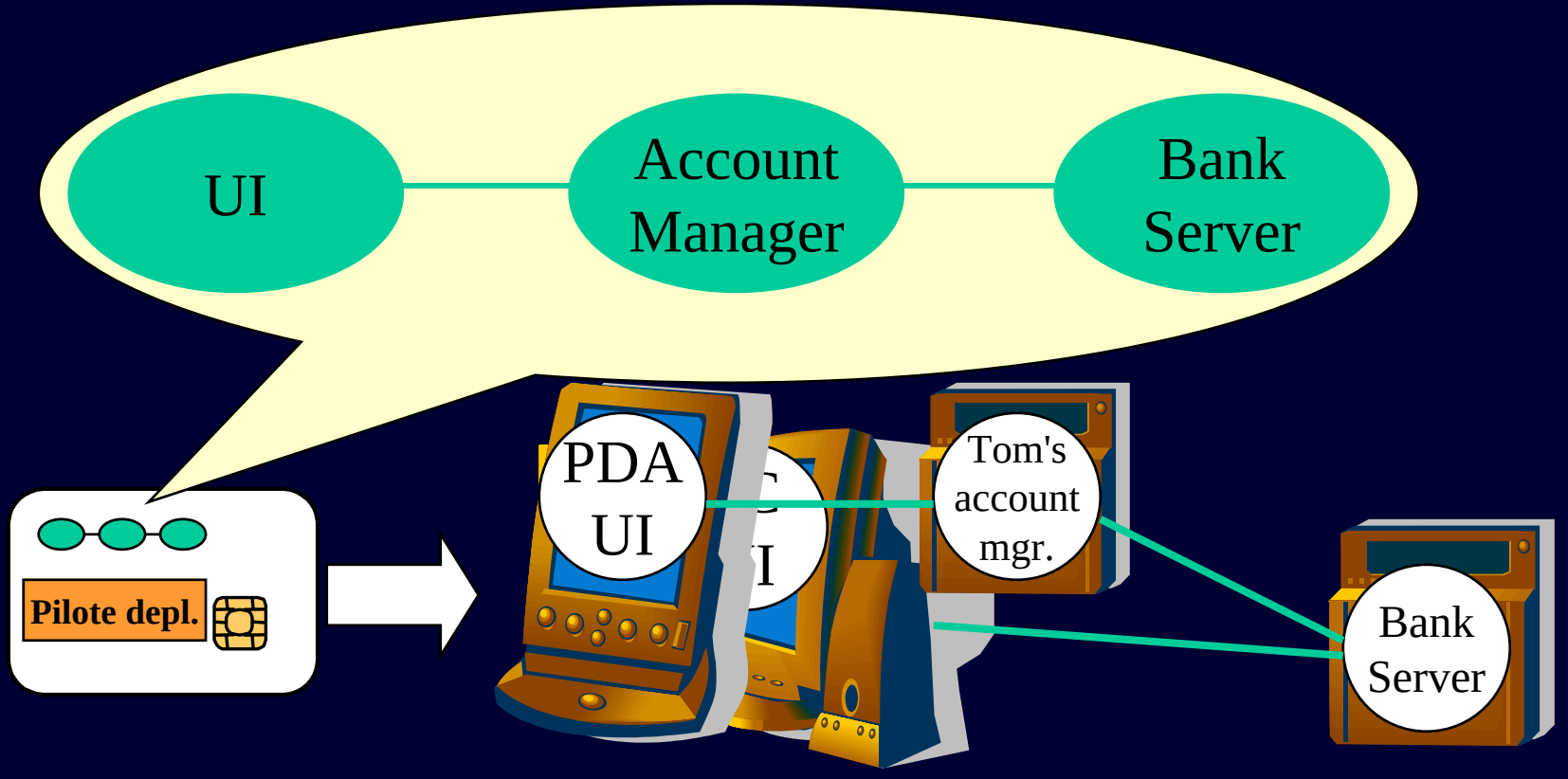
Etudes réalisées (2/3) : PNDS

- Personal Naming and Directory Service
  - Service LDAP-like dans un carte
  - Carnet d'adresses, répertoire de services
  - Déploiement automatique de l'accès (sécurisé) aux services



Etudes réalisées (3/3) : Cesure

- Déploiement d'applications par carte à puce



Etudes à venir (1/2)

- Mise à disposition d'applications au travers de la carte à puce
  - Les opérateurs installent des applications sur les terminaux au travers de la carte à puce qui peut vérifier l'authenticité de l'origine de l'application (et son intégrité), *etc.*
- Participation de la carte à puce à l'exécution des applications
  - Le terminal n'étant pas de confiance la carte à puce intervient lors de l'établissement de connexions sécurisées, pour maintenir l'état des transactions, pour identifier l'usager et fournir ses droits, *etc.*

Etudes à venir (2/2)

- Rôle de la carte à puce comme gestionnaire des applications
  - L'usager étant mobile, et l'opérateur voulant garder un lien vers ses applications, la carte sert de « nœud » pour la gestion des applications
  - Réinstallation/reconfiguration/synchronisation/streaming des applications en fonctions des terminaux et des réseaux
  - Surveillance/collecte de données/maintenance/mise à jour/administration à distance de l'application par l'opérateur ou le prestataire de service

Mises en œuvre

- Pour la télévision numérique
  - Projet RNRT COMPiTV Gemplus / Canal+ / Univ. Lille et Valenciennes
  - Personnalisation de l'environnement et des interactions
  - Contrôle de l'intégrité et la cohérence des applications réparties à base de composants
- Pour les passerelles domestiques
  - Thèse CIFRE Gemplus/Université de Lille
  - Gestion des espaces de services personnels au sein d'infrastructures ouvertes multi-opérateurs

Opportunités

- La carte à puce : support privilégié pour l'exécution d'éléments d'applications clés
- Plate-forme Java Card de nouvelle génération : plus puissante, plus de capacités, plus souple
- L'évolution des technologies carte facilite leur intégration et permet d'imaginer de nouveaux usages (screen-card, carte SUMO à 224 Mo, cartes USB...)

Conclusion : 1 usager = 1 carte

- Aujourd'hui : pour un opérateur, un réseau, un type de terminal, une application/fonctionnalité principale
- Demain : pour des opérateurs multiples, des réseaux différents, des terminaux variés,
  et des applications/services "non prédéfinis"

⇨ **Objectifs : outils de développement et de déploiement de la mise en œuvre de services personnels et sécurisés dans les infrastructures de demain au travers une carte à puce programmable (Java Card)**