



# Logiciels embarqués et participatifs

Pierre.Paradinas @ cnam.fr

Cnam/Cedric

Chaire : Systèmes Emfouis et Embarqués



# Introduction

## ● De Gemplus au CNAM

## ● L'exposé

- La carte à microprocesseur : une plateforme d'exécution de confiance
- Le projet CESURE, ou une carte au coeur du déploiement d'application à base de composants



GEMPLUS

# De G+ ... au Cnam

## ● Créateur du Software Research Lab en 1996

- 1er 32 bit RISC pour carte (CASCADE)
- Java Card 2.0
- Introduction des Méthodes Formelles
- Carte à écran et clavier
- 1er Vérifieur de BC Java embarqué

2003 création de la chaire  
Systèmes Embarqués et Enfouis



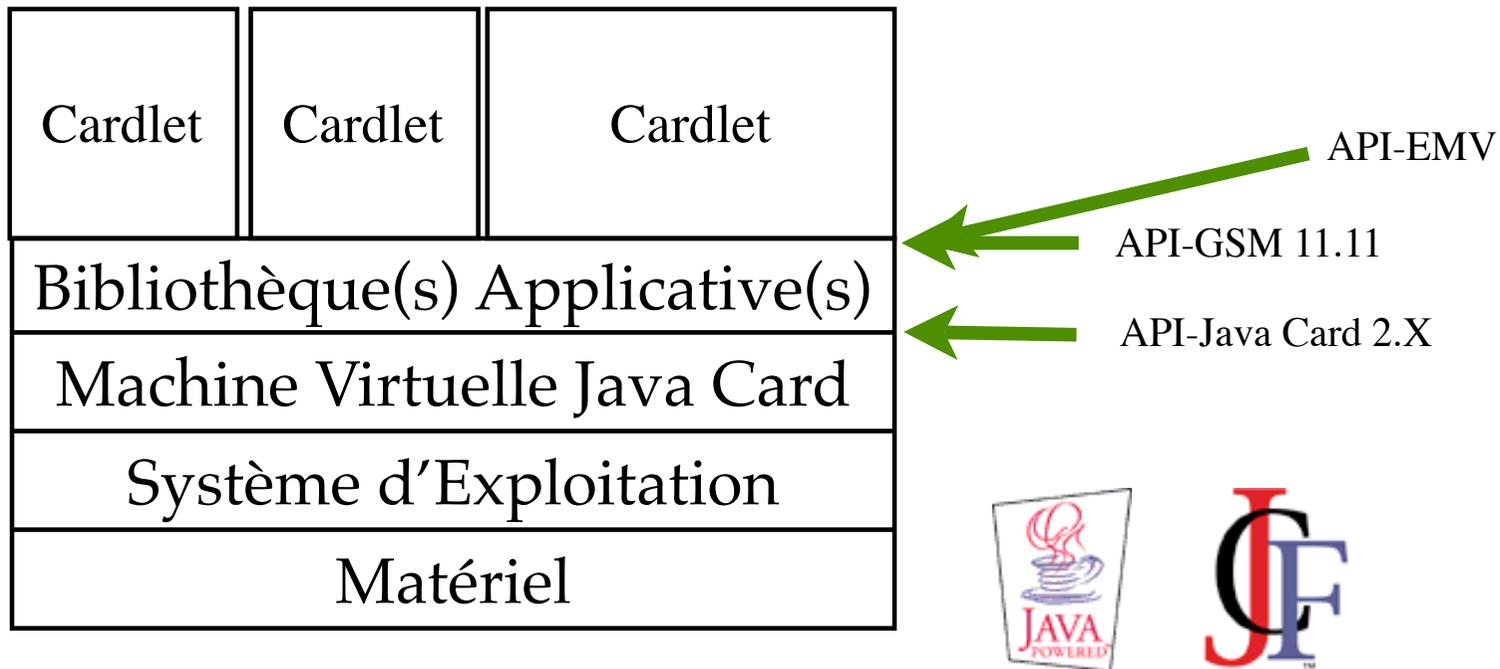
# La carte à microprocesseur

## ● Micro-contrôleur :

- CPU (8, 32)
- Rom => Program
- NVM => EEPROM / Flash
- SRAM
- Crypto co-processeur
  - Tension et horloge sont fournies par le monde extérieur



# La carte à microprocesseur (architecture logiciel)



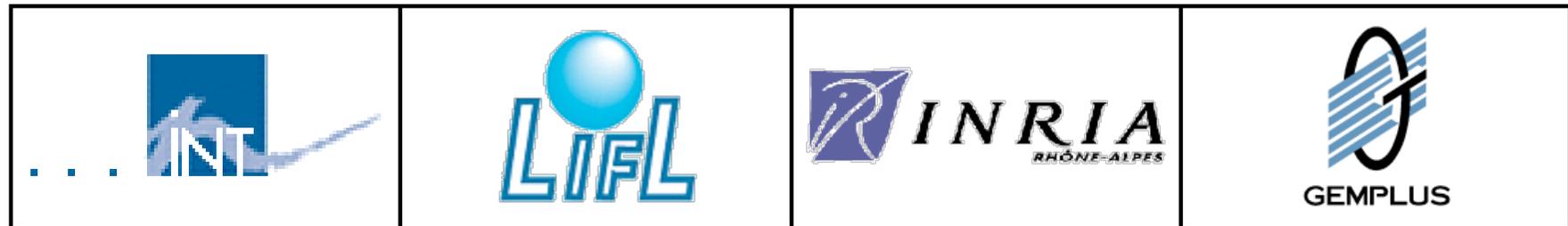
# La carte à microprocesseur logiciel (suite)

- Le sécurité nécessaire au chargement de code est assurée par le modèle Java Card :
  - typage
  - mécanisme de sécurité (sand box, firewall)
  - BC vérification et/ou signature des codes chargés
- La carte est une plateforme de confiance :
  - pour l'exécution de services cryptographiques (signature, chiffrement)
  - pour l'exécution de services...

# Le projet

● Projet : 

● Partenaires :



○ <http://gemplus.com/cesure>

# Projet CESURE suite

- A partir du terminal de l'utilisateur :
  - configurer,
  - déployer,
  - superviser le système.
- La carte à microprocesseur stocke la description de l'application.
- Les services sont vus comme un assemblage de composants spécifique à chaque utilisateur.

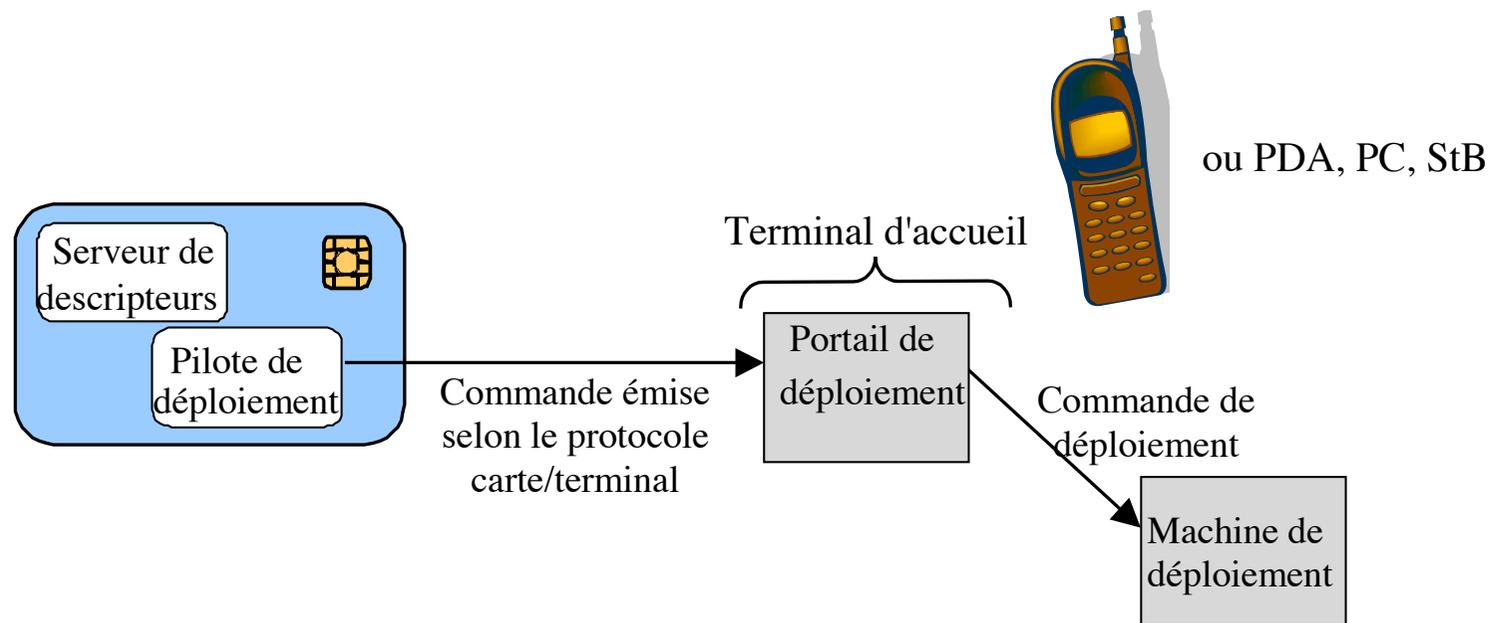
# Le rôle de la carte dans CESURE

- Identification et authentification du porteur (souscripteur) par rapport aux services.
- Contrôle d'accès aux services et aux données.
- Stockage des descripteurs d'applications.
- Adaptation de l'application en fonction:
  - du terminal,
  - du réseau,
  - des préférences de l'utilisateur.

# La mise en oeuvre

- Un serveur de descriptions des applications.
- Un pilote de déploiement, qui émet des ordres vers le portail de déploiement.
- Portail de déploiement :
  - exécuté par le terminal,
  - médiateur (carte / usager) et (carte / portail de déploiement),
  - informe la carte sur le contexte (QoS, niveau de confiance,...).

# Répartition



# Conclusion

- La carte est le lien entre le fournisseur de services et l'utilisateur
- Au delà de la sécurité, c'est un élément de personnalisation et de contrôle de votre environnement
- Cesure illustre comment une carte peut être un élément clé du contrôle de la mise à disposition intelligente de services.