Laboratoire Bordelais de Recherche en Informatique

Équipe : Systèmes et Objets Distribués

La technologie Java Card™ et sa sécurité

Damien Sauveron
sauveron@labri.fr
http://dept-info.labri.fr/~sauveron

11 juillet 2002

Plan

Damien Sauveron
sauveron@labri.fr

Présentation de la carte à puce

Damien Sauveron
sauveron@labri.fr

Qu'est ce qu'une carte à puce ?

- ***un morceau de plastique*** de la taille d'une carte de crédit
- ***un circuit électronique*** capable de manipuler (stocker, calculer, etc) des informations

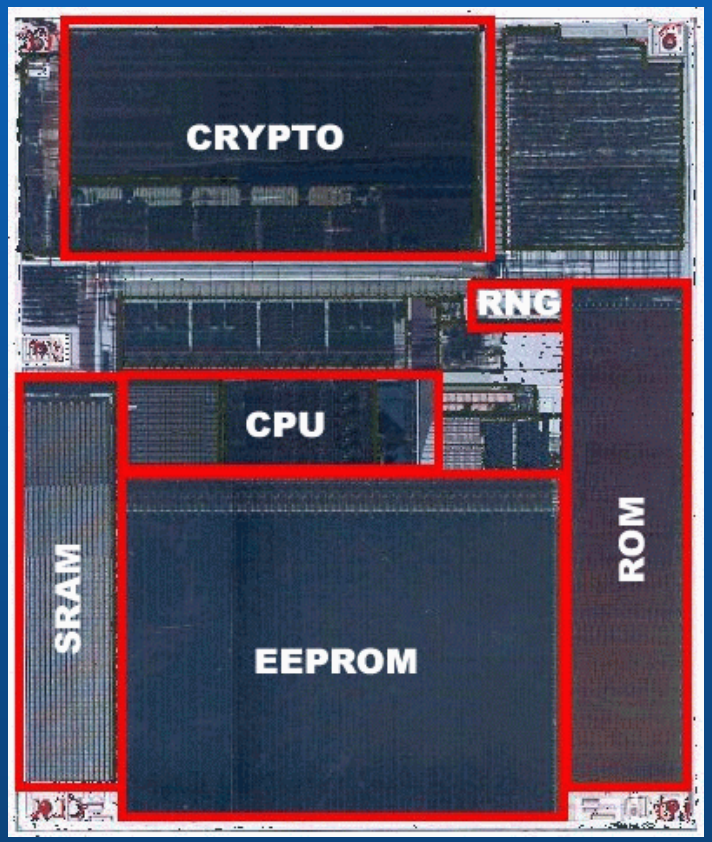
Historique

- En 1968, deux Allemands Jürgen Dethloff et Helmut Grötrupp introduisent un circuit intégré dans une carte plastique
- Entre 1974 et 1978, le français Roland Moreno, ***le père de la carte à puce*** dépose 47 brevets dans 11 pays
- En 1983, apparition des premières cartes téléphoniques à mémoire
- En 1984, adoption par le G.I.E carte bancaire de la " carte bleue "
- Entre 1984 et 1987, normes ISO 7816 (carte à puce à contact)
- En 1997, apparition des premières Java Cards

La carte à microprocesseur

Taille de la puce : $25mm^2$

- ***Microprocesseur*** (CPU) : 8, 16 ou 32 bits (à architecture RISC ou pas)
- ***ROM*** : 32 à 64 Ko
- ***EEPROM*** : 24 à 64 Ko
- ***RAM*** : 1 à 4 Ko
- Coprocesseur cryptographique
- Générateur de nombres aléatoires (RNG)



Avantage : le coût acceptable pour tant de sécurité (entre 1$ et 20$).

Damien Sauveron
sauveron@labri.fr

La technologie Java Card

Damien Sauveron
sauveron@labri.fr

Présentation

Technologie permettant de faire fonctionner des applications écrites en langage Java[a] pour :

- les cartes à puce
- d'autres périphériques à mémoire limitée

La technologie Java Card définit une plate-forme pour cartes à puce sécurisée, portable et multi-applications qui incorpore beaucoup des avantages du langage Java.

[a] Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. The author is independent of Sun Microsystems, Inc.

Historique

- En novembre 1996, ingénieurs de Schlumberger $\Longrightarrow$ la spécification Java Card 1.0 (4 pages).
- En février 1997, Bull et Gemplus se joignent à Schlumberger pour cofonder le *“ **Java Card Forum** ”*.
- En novembre 1997, Sun présente les spécifications Java Card 2.0.
- En mars 1999, spécifications Java Card 2.1.
- En mai 2000, spécifications Java Card 2.1.1.
- En octobre 2000, plus de 40 entreprises ont acquis la licence d'exploitation de la technologie Java Card.
- En juin 2002, spécifications Java Card 2.2.

Avantages de la technologie Java Card

La facilité de développement des applications grâce :

- à la **programmation orientée objet** offerte par Java
- à l'utilisation des **environnements de développement** existants pour Java
- à une **plate-forme ouverte** qui définit des APIs et un environnement d'exécution standard
- à l'**encapsulation de la complexité** fondamentale du système des cartes à puce

Avantages de la technologie Java Card

La sécurité grâce :

- à **plusieurs niveaux de contrôle d'accès** aux méthodes et aux variables (`public`, `protected`, `private`)
- à un **langage fortement typé**
- à l'**impossibilité de construire des pointeurs**
- à un " **firewall** "

Damien Sauveron
sauveron@labri.fr

Avantages de la technologie Java Card

L'indépendance au hardware réalisée grâce au langage Java
$\Longrightarrow$ " Write Once, Run Anywhere "

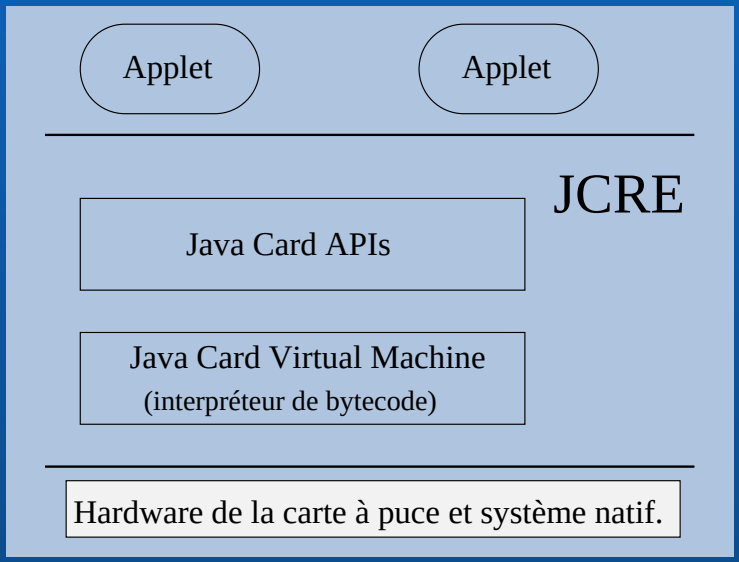
La capacité de stockage et de gestion de multiples applications.
$\Longrightarrow$ possiblité de mise à jour des applications de la Java Card sans avoir besoin de changer de cartes

La ***compatibilité*** avec les standards existants sur les cartes à puce.

Présentation de son architecture

Problème : contraintes mémoires
Solutions :

- un sous-ensemble des caractéristiques du langage Java
- découper la machine virtuelle Java en deux parties



Problème : pas de vérificateur embarqué
Solution :

- fournir des mécanismes sécuritaires avec l'environnement d'exécution

Damien Sauveron
sauveron@labri.fr

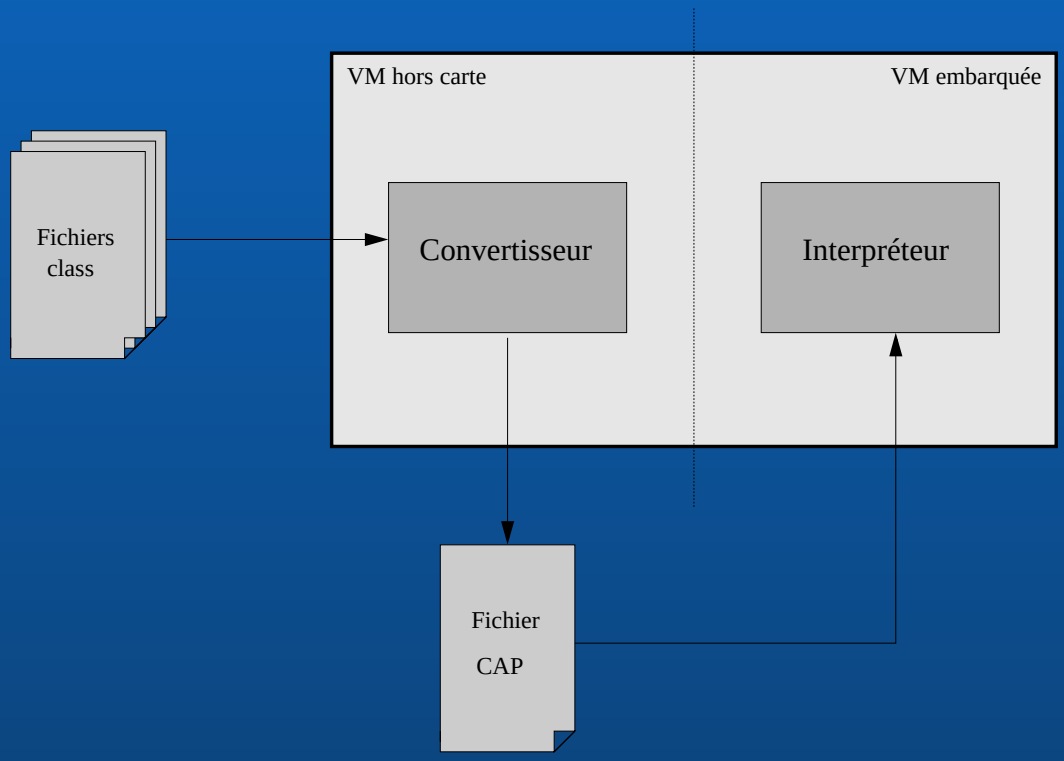
Le langage Java Card

Caractéristiques Java supportées	Caractéristiques Java non supportées
▷ Type simple de donnée de petite taille : `boolean`, `byte`, `short` ▷ Tableaux à une dimension ▷ Paquetages Java, classes, interfaces et exceptions ▷ Caractéristiques orientées objets : héritage, méthodes virtuelles, surcharge et création dynamique d'objets, contrôle d'accès ▷ Le mot clé `int` et le support des entiers sur 32 bits sont optionnels	▷ Type simple de donnée de grosse taille : `long`, `double`, `float` ▷ Tableaux à plusieurs dimensions ▷ Caractères et chaînes ▷ Chargement dynamique des classes ▷ `Security Manager` ▷ Ramasse-miettes et finalisation ▷ Threads ▷ Sérialisation d'objet ▷ Clonage d'objet

La machine virtuelle Java Card : JCVM

Les deux parties implémentent toutes les fonctions d'une machine virtuelle.

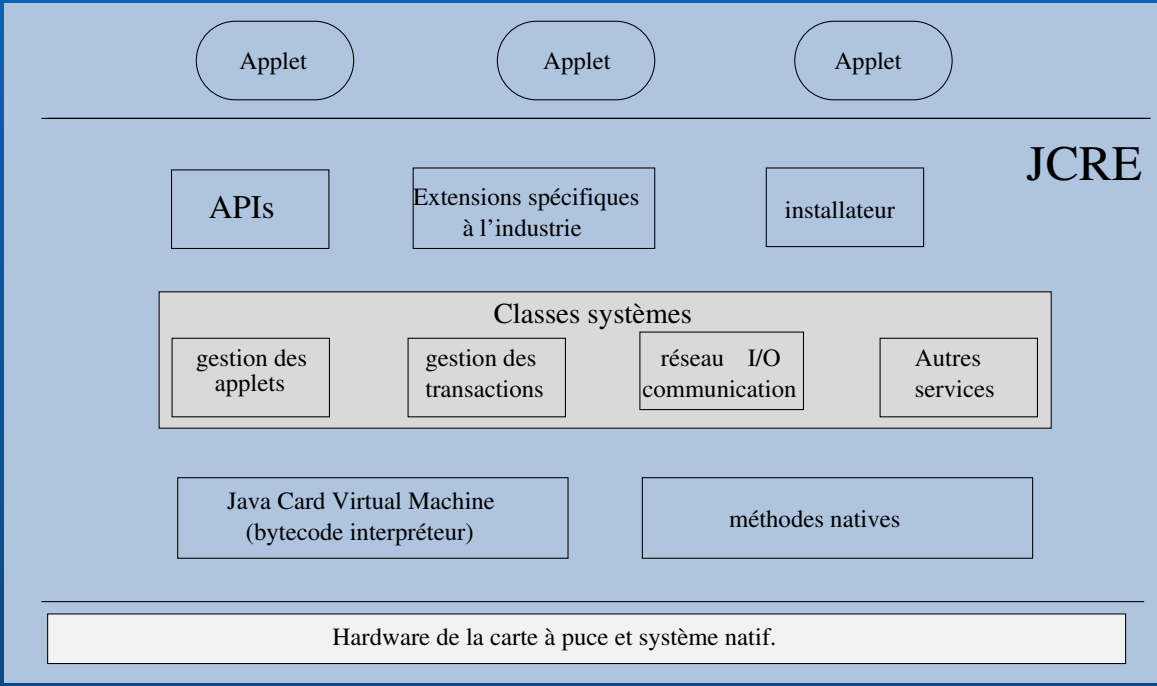
A cause du découpage de la JCVM, ***la plate-forme est distribuée dans le temps et dans l'espace.***



L'environnement d'exécution Java Card

Responsable :

- de la gestion des ressources de la carte
- de la communication réseau
- de l'exécution des applets
- du système de la carte
- de la sécurité des applets



Damien Sauveron
sauveron@labri.fr

L'environnement d'exécution Java Card

Les caractéristiques du JCRE

- ***Objets persistants*** existant au travers des sessions avec le lecteur.
- ***Objets temporaires*** dont les données ne persistent pas au travers des sessions avec le lecteur.

- Chaque opération d'écriture de la JCVM est ***atomique***.
- ***Une transaction*** est un bloc d'opérations atomiques.

- ***Le " firewall "*** isole les applets à l'intérieur de leur espace (contexte).
- Pour mettre en commun des données, il existe des ***mécanismes sécurisés de partage.***

Les APIs Java Card

Ensemble de paquetages optimisés pour la programmation des cartes à puce en accord avec le modèle ISO 7816.

`java.lang` : un sous ensemble strict de son équivalent sur la plate-forme Java

`javacard.framework` : classes et interfaces pour le noyau fonctionnel des applets Java Card

`javacard.security` : modèle pour les fonctions cryptographiques supportées sur la plate-forme Java Card

`javacardx.crypto` : un paquetage d'extension

L'équipe :
les intervenants Java Card

Damien Sauveron
sauveron@labri.fr

L'équipe : les intervenants Java Card

- Serge Chaumette (maître de conférence) coordonne et dirige les activités de recherches relatives à Java Card. Il est aussi le relai avec les partenaires industriels et institutionnels.

- Iban Hatchondo (ingénieur) développe la JCVM, les APIs et les outils nécessaires à la recherche sur la technologie Java Card.

- Damien Sauveron (doctorant CIFRE) partage son temps entre le LaBRI et le CESTI de SERMA Technologies. Il participe aux décisions importantes sur le développement de la JCVM et des APIs. Il a pour but de modéliser des attaques.

Perspectives

Perspectives

En cours

Projet PROGSI : projet sur la sécurité Java Card entre le LaBRI et SERMA Technologies

Journée " carte à puce " : discussions et présentations de la recherche sur les nouveaux enjeux de la carte à puce par les leaders du marché

Perspectives

Le futur (1)

Incorporation du “ Java Card Forum ”

Intégration du LaBRI, au sein du réseau thématique du CNRS sur les systèmes embarqués, de l’action spécifique “ sécurité, modélisation et vérification ”. Le pilotage sera réalisé par SOD. Cette action mobilisera au sein du LaBRI 2 équipes :

- Modélisation, vérifications et test de systèmes informatisés (André Arnold et Alain Griffault)
- Systèmes et Objets Distribués (Serge Chaumette, Iban Hatchondo et Damien Sauveron)

Perspectives

Le futur (2)

Mise en place d'un outil de développement modulaire suivant les caractéristiques des différentes plate-formes Java Card du marché en collaboration avec les industriels.

Participation aux diverses conférences et aux différents workshops sur le thème de la technologie Java Card (e-Smart, VerifCard, Secsafe, eurosmart, global platform, ...)