Laboratoire Bordelais de Recherche en Informatique
UMR 5800 – Université Bordeaux 1,
351, cours de la Libération, 33405 Talence CEDEX, FRANCE

Dossier de presse pour la journée :

“ Les nouveaux enjeux de la Carte à puce ”
Sécurisation des technologies multi-applicatives embarquées pour l'utilisation élargie de la carte à puce

(Mercredi 19 décembre 2001 de 8h30 à 17h30)

Responsable : **Serge** CHAUMETTE — Équipe : **Systèmes et Objets Distribués**

La carte à puce multi-applicative et sa sécurité

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

Version : 1.0 — Dernière révision : 2 Décembre 2001

RÉSUMÉ – Avec l'explosion du commerce électronique, de la téléphonie mobile et des besoins d'identification, la confidentialité et la sécurité des échanges sont devenues des priorités. Les solutions actuellement proposées sont basées sur ***la carte à puce***. Cette carte dispose en effet de nombreux atouts sécuritaires et peut s'adapter à de multiples problèmes. Ainsi en l'an 2000, c'est 1,6 milliard de cartes à puce qui ont été vendues, soit un volume de vente trois fois supérieur à l'ensemble de celui des téléviseurs, ordinateurs et téléphones réunis.
Nous présenterons les caractéristiques principales des cartes à puce et quelques applications qui en découlent. Ensuite nous évoquerons quelques ***vulnérabilités*** liées à la ***multi-application embarquée*** sur les cartes à puce. Nous finirons par une présentation des technologies des cartes à puce multi-applicatives. Plus particulièrement nous verrons comment la technologie Java a réussi à s'immiscer avec succès dans le monde de la carte à puce pour construire une carte multi-applicative : ***la Java Card***™[1]. Nous détaillerons donc certaines parties de l'architecture de ***la Java Card*** afin de voir comment la ***gestion sécuritaire*** de la carte a été réalisée.
MOTS-CLÉS : *carte à puce, Java Card, sécurité, embarqué*

---

[1] 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.

Introduction

À l'heure de l'Internet et des nouvelles technologies, alors que la sécurité devient l'une des préoccupations principales, la carte à puce est un des objets les plus sûrs qui puissent exister. Son développement se base sur l'utilisation des technologies matérielles les plus sécurisées et les plus secrètes. Depuis quelques années la carte à puce cherche aussi à s'imposer comme l'objet universel d'authentification et de sécurisation dans les systèmes informatiques et dans la vie quotidienne. Cette révolution est en cours grâce aux cartes multi-applicatives et plus particulièrement grâce à la technologie Java Card.

Première partie
Présentation de la carte à puce

---

1 Qu'est ce qu'une carte à puce ?

De la même taille qu'une carte de crédit, une carte à puce est une carte plastique qui contient un circuit électronique capable de manipuler (stocker, calculer, etc) des informations. Une carte à puce est un ordinateur portable et résistant aux altérations.

2 Historique

- En 1968, Jürgen Dethloff et Helmut Grötrupp deux inventeurs Allemands sont les premiers à introduire un circuit intégré dans une carte plastique.
- En 1970, indépendamment Kunitaka Arimura de l'institut de technologie Arimura au Japon dépose un brevet sur la carte à puce.
- Entre 1974 et 1978, Roland Moreno dépose 47 brevets dans 11 pays. Il est considéré comme l'inventeur de la carte à puce.
- En 1979, la première carte est créée, assemblée à Toulouse, par Motorola pour Bull CP8 avec 1 Ko de mémoire programmable et un cœur à base de microprocesseur 6805.
- En 1983 apparaissent les premières cartes téléphoniques à mémoire.
- En 1984, le G.I.E carte bancaire adopte la " carte bleue " proposée sur un prototype Bull CP8. Cela aboutit à notre carte bleue actuelle version B0'.
- Entre 1984 et 1987, les normes internationales de l'ISO sur la carte à puce à contact voient le jour sous la référence 7816.
- En 1997, les premières Java Cards apparaissent.

3 Les différentes cartes à puce

Il existe plusieurs sortes de cartes à puce que l'on peut classer de plusieurs façons. On peut soit faire un classement entre les cartes à mémoire et les cartes à microprocesseur soit entre les cartes à contact et les cartes sans contact.

3.1 La carte à mémoire

Cette carte possède une puce mémoire et elle peut aussi comporter une logique câblée non programmable (instruction programmée et non reprogrammable) mais pas de microprocesseur. La taille de la mémoire est de 1 Ko à 4 Ko.

3.2 La carte à microprocesseur

Cette carte est composée d'un microprocesseur et de différents types de mémoires. Le plus souvent la carte possède un processeur 8 bits mais il existe des modèles à base de processeurs 16 et 32 bits. On dispose même de processeurs à architecture RISC. Côté mémoire ces cartes en comportent trois types :

- La ROM (Read Only Memory) qui n'a pas besoin d'énergie pour sauvegarder l'information qu'elle contient. Elle sert à stocker le COS (Card Operating System) et des données permanentes. Elle est programmée en usine et ne peut plus être modifiée par la suite. Elle a le plus souvent une taille de 16 Ko mais il en existe disposant de 24 Ko.
- L'EEPROM (Electrical Erasable Programmable Read Only Memory) qui peut comme la ROM préserver son information même quand la carte n'est plus sous tension. La différence avec la ROM est qu'elle peut être modifiée par une application. Sa taille varie de 8 Ko à 64 Ko.
- La RAM (Random Access Memory) qui est utilisée comme espace de stockage temporaire grâce à la rapidité des temps d'accès. Elle possède un caractère non persistent, c'est à dire que dès que la carte n'est plus sous tension, elle perd son contenu. Elle peut être lue et écrite infiniment. Sa capacité est de 256 octets à 1 Ko.

La carte à microprocesseur contient aussi souvent un coprocesseur cryptographique associé à un générateur de nombres aléatoires RNG (Random Number Generator).

3.3 La carte à contact

Cf. `http://www.gemplus.com/basics/what.htm` pour une illustration.

Les cartes à contact pour pouvoir fonctionner doivent être insérées dans un lecteur de cartes. Elles utilisent une communication série via huit contacts.

3.4 La carte sans contact

Cf. `http://www.gemplus.com/basics/what.htm` pour une illustration.

Avec ces cartes, les problèmes rencontrés dans les cartes à contact n'existent plus puisque ces cartes ne sont pas insérées dans un lecteur. Elles communiquent via une antenne dans la carte. La puce tire son énergie soit d'un couplage capacitif (couplage intérieur à la carte, *e.g.*

une batterie) soit d'un couplage inductif (couplage distant, collecté par l'antenne). Le couplage inductif fonctionne sur le principe du transformateur où une bobine induit un courant dans une autre bobine. La fréquence de transmission utilisée est de l'ordre de quelques MHz. La puce est capable en changeant sa résistance, de transmettre le signal qui est capté par le lecteur et interprété comme un signal de donnée.

3.5 La carte combi

Cf. `http://www.gemplus.com/products/contactless/gemtwin.htm` pour une illustration.

Ces cartes ne sont ni plus ni moins qu'une combinaison des cartes à contact et des cartes sans contact. Elles disposent des deux possibilités de communication, ce qui en fait des cartes " idéales ".

4 Applications

Les principaux secteurs qui utilisent actuellement la carte à puce sont :
- l'industrie des télécommunications avec par exemple les cartes téléphoniques pré-payées (comme par exemple les cartes téléphoniques classiques qui sont des cartes à mémoires avec contact) ou bien avec les cartes SIMs insérées dans les téléphones GSM ;
- l'industrie bancaire et monétaire avec les cartes de crédits qui sont des cartes à microprocesseur avec contact (*e.g.* Europay, MasterCard, Visa) ;
- le secteur de la santé (*e.g.* la carte Vitale) ;
- l'industrie audiovisuelle avec la télévision à péage, etc.

Mais de nouvelles applications pour la carte à puce sont aujourd'hui à l'étude pour :
- Le porte-monnaie électronique (*e.g.* Monéo).
- Les transports en commun. Par exemple, l'accès au métro de Séoul se fait via des cartes à puce sans contact. La RATP travaille sur un projet similaire.
- Le contrôle d'accès physique de personnes à des locaux, etc.
- L'identification : à des sites sur l'Internet, etc.
- Les applications de fidélité (*e.g.* l'accumulation de " miles " de voyage en avion gratuits à chaque transaction, etc).
- Les jeux comme le " pocket-gaming " (qui consiste en des terminaux de poche – comme le deviennent les téléphones ou les consoles portables – pour jouer par exemple à des jeux de casino, etc).

Le domaine principal qui permettra à la carte à puce de s'imposer est l'Internet qui au travers des " e-services " exigent de plus en plus une identification et une sécurisation des transactions. Ainsi la carte peut être utilisée pour ces services en stockant par exemple les clefs servant à l'authentification et à la sécurisation. Quelques exemples de " e-services " sont :
- le " e-commerce " ;
- la banque distante ;
- le " e-courrier " ;
- le télétravail ;
- etc.

Deuxième partie

Présentation de quelques vulnérabilités liées à la multi-application embarquée sur des cartes à puce

Dans cette partie, nous allons énoncer une liste non exhaustive de vulnérabilités liées à la multi-application. Chaque technologie de cartes multi-applicatives ayant ses propres spécificités, cela pourra conduire à plus ou moins de problèmes de sécurité. Il n'en demeure pas moins intéressant de voir quelques problèmes récurrents. Mais tout d'abord définissons le concept de base de la multi-application embarquée sur des cartes à puce.

1 Le concept de multi-application embarquée sur des cartes à puce

En général, une carte à puce multi-applicative est un système d'exploitation qui fonctionne sur une puce. Ce système d'exploitation permet de fournir des services aux différentes applications qui sont en mémoire sur la puce. Selon le type de la mémoire qui stocke le code de l'application, divers cas peuvent être envisagés. En effet, si le code de l'application réside dans une mémoire de type ROM, cela signifie qu'elle a été fournie par l'émetteur de carte (*e.g.* banques, etc) et par conséquent, elle peut-être considérée comme " sûre " (aux problèmes de programmation près). Le code de l'application peut aussi résider dans une mémoire de type EEPROM. Dans ce cas, il s'agira souvent d'une application (d'un fournisseur de service) chargée via le service du système d'exploitation permettant l'installation de nouvelles applications. Le système d'exploitation propose aussi souvent la possibilité d'effacement d'une telle application. Ces applications ajoutées après que la carte ait été émise, sont celles qui posent le plus de problèmes d'un point de vue sécuritaire. Les spécifications Open Platform (du groupe de travail Global Platform) définissent un environnement intégré pour le développement et les opérations sur les cartes à puce multi-applicatives. Elles décrivent de façon détaillée la gestion des différents états du cycle de vie de la carte et de ses applications mais aussi des mécanismes sécuritaires qui permettent de pallier à d'éventuels problèmes sécuritaires comme nous le verrons dans la suite.

2 Le problème de l'origine du fournisseur de l'application chargée

Sur les produits actuellement dans le commerce, seuls quelques fournisseurs de services sont autorisés à charger leurs applications sur la carte d'un émetteur tiers. L'autorisation de chargement d'une application se fait au travers de mécanismes d'authentification mutuelle,

permettant de prouver l'origine du fournisseur de l'application. Ce mécanisme sécuritaire a pour but d'empêcher un pirate de charger sa propre application. Dans certains états du cycle de vie de la carte, on créera en plus un " canal sécurisé ", assurant ainsi la confidentialité et l'intégrité de la communication. La spécification de tels mécanismes est décrite par les spécifications Open Platform sous les termes de " mutual authentication " et de " secure channel ". A terme, la sécurité d'une plate-forme multi-applications ne devra plus reposer sur ce mécanisme d'authentification. Ainsi tout le monde pourra développer sa propre application et la charger dans sa carte. S'il s'agit d'une application " virus ", la carte devra être suffisamment sûre pour l'empêcher de nuire. En attendant que ce niveau de sécurité du système d'exploitation de leur carte ne soit totalement certifié, les fabricants préfèrent utiliser de tels mécanismes.

3 Le problème de l'intégrité des données et du code

Il peut se poser un problème d'intégrité :

- Au niveau du code de l'application que l'on va charger. En effet si un pirate réussit à " casser " le mécanisme d'authentification mutuelle, il pourrait espérer charger son application. Pour compléter la sécurité, un mécanisme de signature cryptographique du code de l'application, avant son chargement, est effectuée par un programme hors carte utilisant une clé cryptographique. Cette signature est ensuite vérifiée par la puce après le chargement en utilisant la clé cryptographique correspondante. Ce mécanisme est connu sous le nom de DAP (Data Authentication Pattern) dans les spécifications Open Platform. Une fois encore, le pirate aura face à lui un deuxième mécanisme très difficile à mettre en défaut. A terme, ce mécanisme ne devrait pas être nécessaire à la sécurité d'une plate-forme multi-applicative.
- Au niveau du code et des données des autres applications et du système d'exploitation. Si malgré les mécanismes de " mutual authentication ", de " secure channel " et de DAP, le pirate chargeait son application malicieuse, les cartes multi-applicatives mettent en place, grâce à un mécanisme de " firewall ", un cloisonnement des données et du code de chaque application vis-à-vis des autres applications présentes sur la carte. Les pointeurs ne sont souvent pas autorisés dans les langages compréhensibles par les interpréteurs de code (machines virtuelles) et l'application attaquante ne peut donc pas utiliser ce moyen pour accéder à des informations hors du contexte auquel elle appartient. Les données dans les cartes multi-applicatives ne sont donc accessibles que via des références.

4 La sécurité : l'affaire de tous

Les cartes multi-applicatives proposent parfois des mécanismes de partage de données entre les applications. Ils sont réalisés de manière explicite entre l'application serveur et l'application cliente. Une recommandation fréquente à ce niveau sera de mettre en place une authentification mutuelle entre les deux applications prévenant une éventuelle usurpation d'identité. C'est au développeur d'applications qui souhaite partager ses données de prévoir ce mécanisme. Si l'application serveur n'implémente pas ce mécanisme et si le pirate a réussi à introduire son application malicieuse, il pourra peut-être récupérer des données sensibles de l'application serveur. On voit bien à ce niveau que la sécurité est l'affaire de tous et qu'il

ne suffit pas que la carte soit sûre pour empêcher une attaque. Il faut que les applications qui sont embarquées le soient aussi.

Troisième partie

Présentation des technologies des cartes à puce multi-applicatives

1 MULTOS

MULTOS est la première carte à puce ouverte, hautement sécurisée et possédant un système d'exploitation multi-applicatif (d'où MULT-OS).

Un consortium industriel, nommé MAOSCO, est chargé de promouvoir MULTOS comme système d'exploitation multi-applicatif pour les cartes à puce, de gérer les spécifications de MULTOS, de fournir les licences et les certifications de services MULTOS. Les membres fondateur du consortium MAOSCO sont : American Express, Dai Nippon Printing, Mondex International Ltd, Siemens, Fujitsu, Hitachi, Motorola, MasterCard International, Keycorp.

Les éléments clés de la plateforme MULTOS sont :
- une architecture hautement sécurisée ;
- la possibilité d'avoir plusieurs applications sur la même carte ;
- l'interopérabilité entre les applications ;
- l'indépendance des applications par rapport à la plateforme (au matériel) ;
- le chargement et l'effacement des applications durant la vie de la carte ;
- la compatibilité avec les standards industriels ISO 7816 et EMV.

Pour le développement des applications, Mondex International Ltd a mis en place :
- un langage optimisé pour les cartes à puce : MEL (MULTOS Enabling Language) ;
- des spécifications pour les APIs MULTOS.

MULTOS s'exécute sur la puce de la carte. A l'installation d'une nouvelle application, la carte à puce MULTOS vérifie la validité de l'application qui a été envoyée, alloue un espace mémoire protégé au programme via le “ firewall ”. Chaque nouveau service ou application est gardé rigoureusement séparé, par le “ firewall ”, des autres programmes déjà sur la carte afin qu'aucun d'eux, en cas de disfonctionnements, ne puisse interférer sur une opération d'un autre programme.

2 Windows for Smart Card de Microsoft

La WinCard, proposée par Microsoft, était une carte multi-applicative orientée authentification. Comme cette carte était basé sur un standard fermé, nous ne disposions que de peu d'information, même commerciales. Le projet est depuis abandonné.

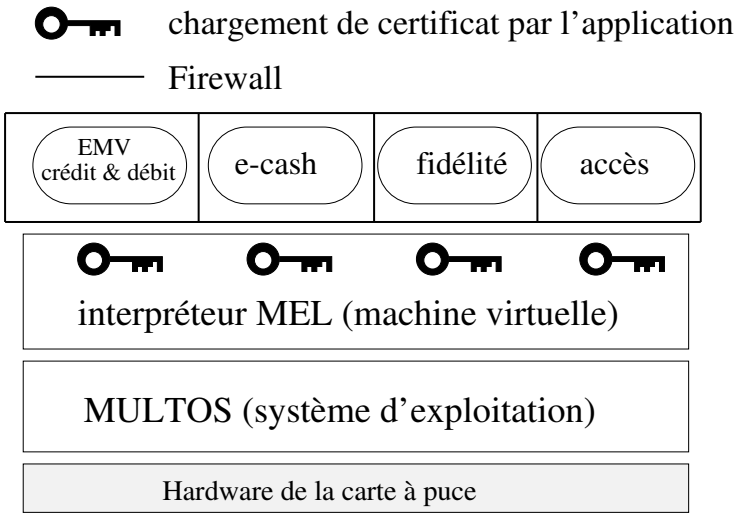

Fig. 1 – Architecture de MULTOS

3 La technologie Java Card

3.1 Qu'est ce que Java Card ?

Cette technologie permet aux cartes à puce et à d'autres périphériques à mémoire limitée de faire fonctionner des applications écrites en langage Java. Une Java Card est une carte à puce qui peut charger et exécuter des programmes écrits en Java. Contrairement aux cartes à puce traditionnelles, les programmes exécutés par la carte ne sont pas forcément fournis par l'émetteur de carte.

Pour résumer, la technologie Java Card définit une plateforme sécurisée pour cartes à puce, portable et multi-application qui incorpore beaucoup des avantages du langage Java.

3.2 Historique

- En Novembre 1996, un groupe d'ingénieurs du centre de production de Schlumberger à Austin au Texas cherche à simplifier la programmation des cartes à puce tout en préservant la sécurité. Le langage de programmation Java fût la solution. Schlumberger devint alors la première entreprise licenciée en proposant un brouillon de quatre pages (la spécification Java Card 1.0).
- En Février 1997, Bull et Gemplus se joignent à Schlumberger pour cofonder le Java Card Forum. Le but de ce consortium industriel est d'identifier et de résoudre les problèmes de la technologie Java Card en proposant des spécifications à JavaSoft (la division de Sun à qui appartient Java Card). Il a aussi pour but de promouvoir des APIs Java Card pour permettre son adoption par l'industrie de la carte à puce. Aujourd'hui, le Java Card Forum regroupe les fabriquants de cartes, Sun et des utilisateurs.
- En Novembre 1997, Sun présente les spécifications Java Card 2.0 qui consistent en un sous ensemble du langage et de la machine virtuelle Java. Elles définissent des concepts de programmation et des APIs très différentes de celles de la version 1.0. Il n'y a encore rien sur le format des applets téléchargeables.

– En Mars 1999 sort la version 2.1 des spécifications Java Card. Elles consistent en trois spécifications :
  • la Java Card 2.1 API Specification,
  • la Java Card 2.1 Runtime Environment Specification,
  • la Java Card 2.1 Virtual Machine Specification.

  Dans cette nouvelle version, il y a eu quelques modifications des APIs notamment au niveau de la cryptographie et des exceptions. L'environnement d'exécution des applets a été standardisé. La contribution la plus significative de la version 2.1 est la définition explicite de la machine virtuelle de la Java Card (JCVM : Java Card Virtual Machine) et du format de chargement des applets, autorisant ainsi une vraie inter-opérabilité.
– En Mai 2000, est sortie une petite correction qui aboutit à la version 2.1.1 de la spécification.

3.3 Les avantages de la technologie Java Card

Les avantages apportés par la technologie Java Card aux développeurs d'application sont en grande partie les mêmes que ceux qu'a pu apporter Java aux langages de programmation classiques :

– La facilité de développement des applications grâce :
  • à la programmation orientée objet offerte par Java (contre l'assembleur avant),
  • à la possibilité d'utiliser les environnements de développement existants pour Java,
  • à une plateforme ouverte qui définit des APIs et un environnement d'exécution standardisé,
  • à une plateforme qui encapsule la complexité fondamentale et les détails des systèmes des cartes à puce.

  Les développeurs peuvent ainsi se concentrer sur les applets ou les bibliothèques qu'ils créent, réduisant le temps de développement.
– 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 qui, sinon, pourraient être utilisés dans des programmes malicieux afin d'espionner le contenu de la mémoire,
  • à un " firewall " qui sépare les applets dans la plateforme.

  Grâce à tous ces mécanismes, le système empêche un programme hostile de créer des dommages à une autre partie du système.
– L'indépendance par rapport au " hardware " réalisée grâce au langage Java, exécutable sur n'importe quel système car son code pré-compilé en bytecode est exécuté par la machine virtuelle Java. Cette portabilité permet d'écrire du code qui fonctionnera sur n'importe quel microprocesseur de carte à puce (" Write Once, Run Anywhere ").
– La capacité de stockage et de gestion de multiples applications. En effet les Java Cards peuvent héberger de multiples applications de fournisseurs et de natures totalement différents. Un mécanisme de " firewall " interdit l'accès d'une applet à une autre si celui-ci n'est pas explicitement permis. Une fois la carte fournie à son propriétaire il est encore possible de télécharger des applets. Les applications de la Java Card peuvent

ainsi être continuellement mises à jour sans avoir besoin de changer de cartes.
– La compatibilité avec les standards existants sur les cartes à puce. La technologie Java Card est basée sur le standard ISO 7816 autorisant le support d'applications compatibles ISO 7816. Les applets peuvent donc interagir non seulement avec toutes les cartes à puce Java mais aussi avec les lecteurs existants.

3.4 Présentation de son architecture

Comme nous l'avons vu précédemment, les configurations mémoires des cartes à puce sont de l'ordre de 1 Ko de RAM, 16 Ko d'EEPROM et de 24 Ko de ROM. Un grand défi de la technologie Java Card a été de s'adapter à ces contraintes pour construire une carte Java tout en conservant assez de place pour les applications.

La solution fut de supporter seulement un sous-ensemble des caractéristiques du langage Java et de découper la machine virtuelle Java (JCVM) en deux parties. Une partie qui s'exécute en dehors de la carte et une partie qui s'éxecute sur la carte. La partie de la JCVM embarquée sur la carte comprend principalement l'interpréteur de bytecode. Beaucoup de tâches ne sont plus réalisées à l'exécution mais sont déportées vers la partie de la machine virtuelle hors carte (*e.g.* le chargement de classes, la vérification de bytecode, la résolution de liens, l'optimisation, etc).

Pour palier aux problèmes de sécurité dû à l'absence de vérificateur embarqué, la technologie Java Card a fourni un environnement d'exécution, le JCRE (Java Card Runtime Environment) chargé de fournir des mécanismes sécuritaires qui permettent une séparation claire entre le système de la carte à puce et les applications (*e.g.* le " firewall ", etc). C'est le JCRE qui encapsule la complexité fondamentale et les détails du système des cartes à puce (*cf.* Fig. 2). Les applets demandent des ressources et des services systèmes au JCRE à travers les APIs.

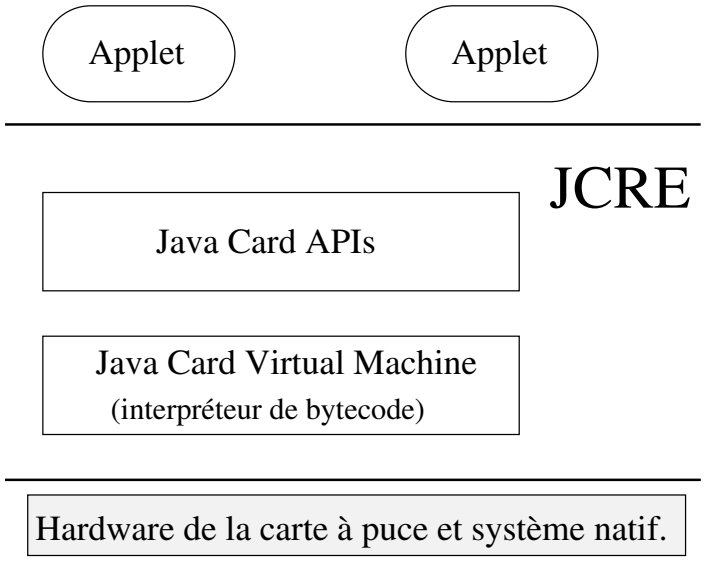

Fig. 2 – Architecture de la Java Card

À cause du découpage de la JCVM, la plateforme est distribuée entre la carte à puce

et la machine de développement dans le temps et dans l'espace. Cette architecture de la technologie Java Card est définie par les trois parties de la spécification suivante :

- la Java Card 2.1 Virtual Machine Specification définit un sous-ensemble du langage de programmation Java et la définition de la machine virtuelle nécessaire pour les applications pour des cartes à puce ;
- la Java Card 2.1 Runtime Environment Specification décrit précisément le comportement de l'exécution de la Java Card, comme la gestion de la mémoire, des applets et d'autres caractéristiques ;
- la Java Card 2.1 API Specification décrit l'ensemble du noyau et des extensions des paquetages et des classes Java pour la programmation des cartes à puce.

Conclusion

Depuis sa création dans les années 1970 jusqu'à aujourd'hui la carte à puce a subit une lente mais importante évolution. Au fil du temps sa sécurité s'est renforcée et son importance dans la vie quotidienne en Europe s'est accrue. Aujourd'hui elle est incontournable. Malgré tous ces avantages, il lui reste encore un marché énorme à conquérir et en particulier celui des États-Unis. La Java Card saura peut-être grâce à sa technologie séduisante lancer la révolution qui banalisera la technologie de la carte à puce à travers le monde. Mais pour réussir ce pari, il lui faudra prouver qu'elle est parfaitement sûre.