新型 Java 智能卡开发

冉 懿
四川大学 川大东大智能建筑有限公司

摘 要 本文在介绍智能卡的基础上，阐述其基本结构，并就 Java Card 应用程序开发中的关键问题作了详细说明。希望能为智能卡的开发者了解新技术提供一点帮助，也能为系统集成商提供一个新的选择方案。

关键词 IC卡 智能卡 Java Card 电子商务

0 前言

随着人们对电子商务的渴求越来越强烈，如何为客户提供安全、可靠的信息，成为了一个电子商务系统解决方案的关键。当前电子商务系统中的安全问题可以概括为：双方必须确定信息接受的对方是谁即身份鉴别；双方的信息对其他人不应该看见即加密；交易的必须不可抵赖即数字签名。随着计算机安全技术的发展，公开密匙技术为解决在不安全网络中安全信息交换提供了可行的方案。在公开密匙系统中，因为使用智能卡比其他方法具有更高的安全性，不易复制，成本低廉，开放性等优点，已成功运用于各种电子商务系统中。智能卡也因此得到了巨大的发展。作为最新的智能卡技术，Java Card 以其安全性好、兼容性强，支持多应用，可在动态下载程序，易于开发等优点，正越来越多的应用于各种系统和设备中。

1 Java Card 是一种更安全，更灵活，更高效的智能卡技术

1.1 Java Card 的特点

Java Card 从本质上讲就是满足 Java Card 规范的 CPU 智能卡。随着智能卡技术的飞速发展，“一卡通”、“一卡多用”已成为现今智能卡的应用主流。在“一卡多用”中使用 CPU 卡已经成为共识；而 MEMORY 卡因受其自身的局限性而逐步被 CPU 卡所取代。虽然 ISO7816 作为接触式智能卡的国际标准，对智能卡从几个方面进行了明确的规范，但由于 ISO7816 并没有规定智能卡提供商如何实现标准接口，大部分厂商都提供了自己专有的 COS(卡操作系统)和接口。这导致了如果为一种智能卡设计的应用程序要在另一个厂商的智能卡上运行必须重新基于完全不同的系统和接口开发。而 Java Card 相比有如下优势：

①更好的互操作性。

Java Card 提供了一个符合 ISO7816 标准的接口，任何实现了 Java Card 运行环境 (Java Card Run - Time Environment) 的智能卡，都可以执行基于 Java Card 接口规范的应用。

②支持多个应用程序

Java Card 通过应用程序防火墙(Applet firewall)将每个应用相互隔离。每个应用运行在自己分配的地址空间内，相互之间没有影响。如果需要相互间共享数据时，Java Card 又可以通过特定的安全机制实现共享。

③可以发行后动态下载和安装应用程序

基于 Java Card 接口的应用程序可以通过网络下载到 Java Card 上安装和执行。Java Card 应用程序编译成与平台无关的字节码后，通过网络下载到 Java Card，通过 Java Card 上的安装程序执行安装后通过 Java Card 的虚拟机解释执行。

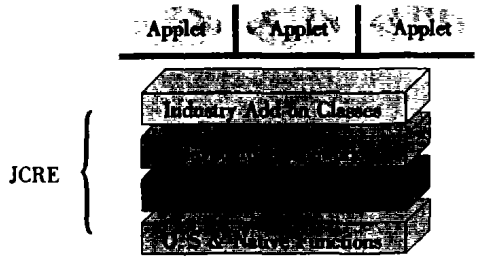
④开发更容易

因为 Java Card 应用程序的开发是基于 Java 语言针对智能卡有限计算能力而优化的一个子集，它具有 Java 语言面向对象等优点。在 Java Card 中，系统类将各种标准的数据和属性都以对象的方式提供给开发者，如 APDU 等，所以 Java Card 应用程序的开发也比其它基于汇编或者 C 语言的开发效率高，也容易得多。

1.2 Java Card 的系统结构

Java Card 系统由两部分组成：Java Card 应用程序，Java Card 运行时环境 JCRE (Java Card Runtime Environment)。JCRE 是 Java Card 的操作系统，包括了：Java Card 虚拟机 JCVM(Java Card Virtue Machine)，系统类库以及各种扩展类。Java Card 通过运行时环境将

应用程序和智能卡提供商专有技术脱离出来，从而实现应用程序与智能卡平台相互独立。其结构如下：



Java Card 结构

2 Java Card 程序编程

2.1 Java 智能卡程序开发的基本要点

2.2.1 应用程序标示 AID(Application Identifier)

在 Java Card 中，使用 ISO7816 规定的 AID 格式确定每个应用程序包(Package)和应用程序。Java Card 程序包和应用程序的 AID 是由 RID 和他们各不相同的专用标示扩展构成的。AID 是 5～11 个字节长，格式如下：

AID

资源标示 RID(5Bytes)	专有标示扩展 PIX(0～11Bytes)

2.2.2 Java Card 与读写器的通讯方式

Java Card 卡和其他智能卡一样，卡上程序与读写器的通讯是通过芯片上的引脚以串行通讯方式进行的。当将卡插入读写器加电后，卡上的程序就用 ISO7816 规定的应用程序协议数据单元 APDU (Application Protocol Data Unit) 的数据格式和读写器以主从方式交换数据，即卡被动地接受并执行读写器的命令，将结果或状态响应给读写器，然后等待下一个命令。

APDU 分为命令 APDU 和响应 APDU 两种格式：

命令 APDU(从读写器到卡)：

类别字 CLA	命令字 INS	参数 1 P1	参数 2 P2	(可选)数据长度 Lc	(可选)数据 Data Field	(可选) 响应数据长度 Le

响应 APDU(从卡到读写器)：

(可选)响应数据 Data Field	状态字 1 SW1	状态字 2 SW2

对 APDU 的编程在其他智能卡系统中是非常麻烦的，也很容易出错。在 Java Card 中，系统提供了标准对象对 APDU 进行封装，操作 APDU 很简单。

2.2.3 应用程序流程。

①安装与注册

因为 Java Card 支持动态安装，当应用程序字节码通过网络完整下载到卡上后，程序就执行安装例程，并且向 JCRE 注册。

②JCRE 选择应用程序

因为 Java Card 支持多个应用程序，因此各个程序的执行是由 JCRE 根据接受的选择 APDU 命令(ISO_SELECT)确定运行哪一个程序。各个程序在没有被选择的时候都是挂起的，即非运行状态。JCRE 根据命令中参数来查找 AID 对应的应用程序，然后选择并运行该应用程序，并将随后的 APDU 都发给该应用程序。

③执行任务，响应读写器

该应用程序接受 APDU，进入其命令处理流程，读取并分析 APDU 命令、参数和数据，根据命令字转到相应的任务，执行其功能，并把结果状态和数据通过响应 APDU 送回到读写器，然后等待下一个命令，直到选择其它程序。注意：由于所有的 APDU 都传递给该应用程序，因此，处理 CDPU 时必须判断是否为选择命令，从而决定是否选择其它程序。

④结束运行。

当其它程序被选择或 IC 卡掉电时，程序立即挂起，直到下一次被运行

2.2.4 应用范例(略)

3 展望

基于 Java Card 技术的智能卡具有安全性好、兼容性强，支持多应用，可以动态下载新应用程序的强大功能，一定会成为今后智能卡的主流。尤其随着后 PC 时代的到来，Java Card 将会被如机顶盒、移动电话、手持电脑等数字终端使用，开发应用于智能卡的应用程序也成为必然趋势。

参 考 文 献

[1]应用密码学－协议，算法与 C 源程序。(美)Bruce Schneier 著，吴世忠等译。机械工业出版社。2001 年 1 月

[2]Java Card 2.1 Runtime Environment Specification. Sun Microsystems, May 2000

[3]Java Card 2.1 API. Sun Microsystems. May, 2000

[4]Java Card 2.1. Virtue Machine Specification May, 2000

[5]How to write a Java Card Applet: A developer's Guide. Zhiqun Chen, Java World July, 1999

[6]Understand Java Card 2.0 Zhiqun Chen, Javaworld, March 1998

[7]Java Card 2.1.1 Development Kit User's Guide, Sun Microsystems, June, 2000

作者简介：

冉懿　男，25 岁，四川大学硕士研究生，主要研究方向：智能建筑、电子商务。