

<<电信智能卡技术与应用>>

图书基本信息

书名：<<电信智能卡技术与应用>>

13位ISBN编号：9787121117534

10位ISBN编号：7121117533

出版时间：2010-9

出版时间：电子工业出版社

作者：张智江 等编著

页数：197

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 前言

近年来, 通信技术的发展给人们的生活带来了巨大的变化, 通信行业伴随着安全技术的发展而发展, 通信的安全一直是备受关注的问题。

智能卡在诞生之初服务于金融行业, 但由于通信技术的发展解决了智能卡与远端计算机的通信问题, 促使智能卡应用于通信领域, 并在通信领域解决安全问题方面获得了巨大的发展。

如今, 智能卡被全世界绝大多数移动通信系统所采用, 是移动通信系统中不可缺少的部分。

起初用来标识用户, 后来很多业务以及安全机制都在智能卡中实现。

第一代移动通信没有采用智能卡, 号码复制和盗打的现象很严重。

第二代移动通信系统GSM首先采用了SIM卡来作为用户的唯一标识, 方便了用户更换手机终端, 在使用之初大大减少了用户号码被复制和盗打的现象发生; CDMA系统在我国商用之初没有采用智能卡, 后来由中国联通主导, 完成了机、卡分离, 这个方法被后来商用CDMA网络的其他国家所采用。

第三代移动通信的三个主要标准WCDMA, cdma2000和TD-SCDMA都使用了智能卡作为用户的唯一标识, 完成用户的认证鉴权。

除了在移动通信系统中标识用户之外, 智能卡被用于储存用户的信息, 如短信和电话号码, 甚至为很多业务提供支持, 并实现一部分安全机制。

智能卡技术在通信行业的发展过程中, 也经历了长足的发展。

首先, 智能卡硬件技术随着微电子技术及半导体技术的发展, 其计算处理能力、存储能力和接口通信速率都得到了提高, 成本也越来越低; 其次, 智能卡中使用了很多新技术, 增强了智能卡的“软”能力, 丰富了智能卡的应用, 如Java技术应用于智能卡, 诞生了JavaCard技术, 被目前大部分的电信智能卡所采用; 智能卡Web服务器技术的应用, 在智能卡中实现了Web服务器, 通过手机中的浏览器访问, 丰富了智能卡的业务菜单展现形式。

智能卡伴随着网络的演进而网络安全中扮演着重要的角色。

目前, 有很多标准化组织都参与了智能卡的标准化工作, 从ISO到3GPP, 3GPP2和OMA, 以及我国的CCSA (中国通信标准协会) 都在进行与智能卡相关的研究和标准化工作, 很多企业和大学等研究机构也致力于智能卡的研究与开发。

本书第1章介绍了智能卡的发展和标准化状况, 并详细介绍了与智能卡相关的各个标准的内容; 第2章介绍了智能卡的架构与关键技术; 第3章介绍了电信智能卡与网络安全, 包括SIM与GSM网络安全以及USIM卡与UMTS网络安全; 第4章介绍了智能卡对通信业务安全的支持; 第5章介绍了智能卡应用工具箱, 第6章介绍了智能卡新技术; 第7章给出了几个智能卡应用的实例。

本书可作为智能卡生产商、电信运营商及相关专业人员的工具书, 也可作为高等院校相关专业师生的教材或教学参考书。

## <<电信智能卡技术与应用>>

### 内容概要

本书阐述了电信智能卡的技术与应用。

第1章介绍了智能卡的发展和标准化状况，并详细介绍了智能卡相关标准的内容；第2章介绍了智能卡的架构与关键技术；第3章介绍了电信智能卡与网络安全，包括SIM与GSM网络安全以及USIM卡与UMTS网络安全；第4章介绍了智能卡对通信业务安全的支持；第5章介绍了智能卡应用工具箱；第6章介绍了智能卡新技术；第7章给出了几个智能卡应用的实例。

本书可作为智能卡生产商、电信运营商及相关专业人员的工具书，也可作为高等院校相关专业师生的教材或教学参考书。

## &lt;&lt;电信智能卡技术与应用&gt;&gt;

## 书籍目录

第1章 概述 1.1 电信智能卡与移动通信发展 1.1.1 移动通信安全机制 1.1.2 智能卡概述 1.1.3 电信智能卡简史 1.2 智能卡标准 1.2.1 智能卡的标准化组织 1.2.2 电信智能卡标准介绍 参考文献第2章 智能卡的架构与关键技术 2.1 智能卡物理特性 2.1.1 常用电信智能卡的格式 2.1.2 触点 2.2 电气特性 2.3 智能卡的操作系统 2.4 智能卡的数据传输 2.4.1 协议和参数选择 2.4.2 ISO协议 2.4.3 USB传输协议 2.5 智能卡的命令 2.6 智能卡文件系统 2.7 与电信智能卡有关的码号资源 参考文献第3章 电信智能卡与网络安全 3.1 SIM卡与GSM安全 3.1.1 GSM网络概述 3.1.2 基于SIM卡的GSM安全机制 3.1.3 SIM卡复制的原理 3.1.4 SIM卡文件 3.1.5 SIM卡命令 3.2 USIM卡与UMTS安全 3.2.1 USIM卡与SIM卡的比较 3.2.2 UICC平台介绍 3.2.3 USIM卡与UMTS安全 3.2.4 EPS安全与USIM卡 3.2.5 USIM卡文件 3.2.6 USIM卡命令 3.3 G/3G共存时期终端与智能卡的兼容性 3.3.1 终端对智能卡的支持 3.3.2 G/3G终端与卡组合 3.3.3 换卡与换号 3.3.4 G/3G共存情况下的认证鉴权 参考文献第4章 电信智能卡与业务安全 4.1 通用自举框架 (GBA) 4.1.1 通用认证框架 (GAA) 介绍 4.1.2 GBA的参考结构 4.1.3 GBA流程 4.1.4 GBA\_U 4.1.5 USIM卡中与GBA有关的机制 4.2 UICC与ME之间的安全机制 4.2.1 参考模型 4.2.2 密钥建立过程 4.3 ISIM与IMS安全 4.3.1 IMS系统概述 4.3.2 IMS安全体系 4.3.3 接入安全 4.3.4 ISIM机制 4.3.5 Early IMS 参考文献第5章 智能卡应用工具箱 5.1 概述 5.2 CAT指令 5.2.1 TERMINAL PROFILE 5.2.2 FETCH 5.2.3 TERMINAL RESPONSE 5.2.4 ENVELOPE 5.3 Profile下载过程 5.4 主动式会话过程 5.4.1 过程描述 5.4.2 主动式命令 参考文献第6章 电信智能卡新技术 6.1 Java Card 6.1.1 Java Card简介 6.1.2 Java Card系统结构 6.2 在智能卡中实现TCP/IP协议 6.2.1 终端与UICC之间的IP配置 6.2.2 协议栈 6.3 智能卡Web服务器 6.3.1 应用场景 6.3.2 SCWS架构 6.3.3 消息流 6.3.4 智能卡Web服务器URL 6.3.5 动态内容支持 6.3.6 本地通信协议 6.3.7 本地传输协议 6.3.8 SCWS的远程管理 6.3.9 全面管理协议 6.4 BIP协议 6.4.1 数据传输 6.4.2 分片管理 6.4.3 传输管理 6.5 GP 6.5.1 GP的目标及历史 6.5.2 GP的结构与相关概念 6.5.3 安全域主要提供的安全功能 6.5.4 生命周期管理 6.5.5 卡密钥管理 6.5.6 GP API 6.6 GSMA提出的Smart SIM 6.6.1 Smart SIM的主要服务 6.6.2 应用案例 6.6.3 Smart SIM给产业链带来的好处 参考文献第7章 应用实例 7.1 叠层卡的原理及应用 7.1.1 叠层卡原理 7.1.2 增值功能分析 7.2 基于智能卡的NFC业务 7.3 基于智能卡的手机电视业务保护 7.3.1 分层密钥管理体系 7.3.2 MBMS业务安全保护过程 7.4 在PC中使用智能卡 参考文献缩略语

## <<电信智能卡技术与应用>>

### 章节摘录

智能卡是一种理想的介质，并可基于密码学达到很高的安全水平，因为它体积小，便于携带，同时也可以存储密钥，可执行加密算法。

今天看来，智能卡的这些特性很适合应用于电信领域，但是在最初，这些新的安全技术被尝试应用于银行卡中，以便去抵御随着磁卡应用的增加伴随而来的安全风险。

在早期，智能卡还被应用于健康保障卡，在德国有超过7 000万张智能卡发给了被国家健康保障计划覆盖的人们。

关于智能卡在非电信领域的应用这里就不花费过多的篇幅来阐述了。

智能卡在20世纪90年代初期的量产规模使智能卡的成本大幅下降，促使人们逐渐引入新的应用，智能卡在移动电话中的使用，对于它在国际间的扩展具有特别重要的意义。

在20世纪90年代，在德国成功地测试了智能卡用于移动电话终端设备后，智能卡成为GSM规定的访问媒体。

智能卡为移动电话网络的访问提供了很高的安全性，给移动电话市场化带来了巨大的商机。

事实上，全世界的移动通信大规模发展与引入SIM卡作为用户标识是有很大关系的，它为网络运营商提供了一种电话销售和电话服务分开的方法。

可以说，没有智能卡，移动电话很难以过去十几年那样的规模迅速扩展到欧洲并遍及全世界。

.....

<<电信智能卡技术与应用>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>