第一图书网, tushu007.com

<<商业银行密码技术应用>>

图书基本信息

书名：<<商业银行密码技术应用>>

13位ISBN编号：9787121133893

10位ISBN编号：712113389X

出版时间：2011-5

出版时间：电子工业出版社

作者：张明德

页数：328

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

内容概要

《商业银行密码技术应用》是中国第一部系统介绍密码技术在商业银行中应用的书籍，同时也是第一部系统介绍密码技术在行业应用的书籍。
《商业银行密码技术应用》共分六章，全面介绍了商业银行业务系统中四套密码应用体系；主要内容包括：银行业务及技术基础、密码技术基础、磁条卡密码应用体系、电子钱包/存折密码应用体系、借记/贷记/电子现金密码应用体系、网上银行密码应用体系（PKI）；附录部分包括了国内密码相关政策法规、国内金融行业标准列表、关键标准汇总及简介等，可作为读者很好的速查手册。

书籍目录

第一章 银行业务及技术基础
1.1 中国银行业相关机构
1.1.1 中国人民银行
1.1.2 中国银行业监督管理委员会
1.1.3 全国金融标准化委员会
1.1.4 中国银行业协会
1.1.5 国有大型商业银行
1.1.6 股份制商业银行
1.1.7 城市商业银行
1.1.8 其他类银行金融机构
1.1.9 中国银联
1.2 国际银行卡组织
1.2.1 Visa
1.2.2 万事达（MasterCard）
1.2.3 JCB
1.2.4 American Express
1.2.5 Diners Club
1.2.6 EMV组织
1.3 商业银行主要业务种类
1.3.1 资产业务
1.3.2 负债业务
1.3.3 中间业务
1.4 商业银行IT架构
1.4.1 IT总体架构
1.4.2 核心业务系统
1.4.3 网点柜台系统
1.4.4 网上银行系统
1.4.5 无卡交易服务系统
1.4.6 有卡交易服务系统
1.4.7 代理业务系统
1.4.8 跨行交易清算系统
第二章 密码技术基础
2.1 密码概述
2.2 抽象文法描述语言ASN.1及其编码规则
2.2.1 抽象文法描述语言ASN.1
2.2.2 ASN.1编码规则
2.3 密码算法
2.3.1 算法分类
2.3.2 对称算法
2.3.3 非对称算法
2.3.4 摘要算法
2.4 工作模式
2.5 扩展机制
2.5.1 MAC
2.5.2 OTP

2.5.3 数字签名
2.5.4 数字信封
2.6 密码协议
2.6.1 SSL
2.6.2 IPSec
2.6.3 Kerberos
2.6.4 时间戳
2.6.5 SET
2.6.6 3-D Secure
2.7 密码应用实践
2.7.1 软件加密与硬件加密
2.7.2 网络层加密与应用层加密
2.7.3 密钥管理基本原则
2.8 我国商用密码政策
第三章 磁条卡密码应用体系
3.1 概述
3.1.1 银行卡发展历程
3.1.2 银行卡分类
3.1.3 密码技术应用的意义
3.2 应用总体架构
3.2.1 磁条卡卡片介绍
3.2.2 磁条卡支付系统
3.3 密码技术应用目的及总体框架
3.3.1 磁条卡安全风险分析
3.3.2 磁条卡应用对系统数据安全的要求
3.3.3 使用密码技术实现数据安全的总体框架
3.3.4 银行卡应用系统数据安全的四个阶段
3.4 密钥管理技术
3.4.1 密钥分层与分类
3.4.2 密钥管理
3.5 密钥应用技术
3.5.1 PIN传输安全性
3.5.2 PIN存储安全性
3.5.3 MAC算法及应用
3.5.4 卡片验证码（CVN/CVV/CVC）
3.5.5 密钥分发方式
3.5.6 卡主机系统
3.5.7 发卡系统
3.5.8 中间节点系统
3.5.9 ATM系统
3.5.10 POS系统
3.5.11 柜面系统
3.5.12 网银系统
3.5.13 ISO 8583报文协议
3.5.14 交易示例
第四章 电子钱包/存折密码应用体系
4.1 应用总体框架

4.1.1 IC卡
4.1.2 密钥管理系统
4.1.3 个人化发卡系统
4.1.4 终端设备系统
4.1.5 业务管理系统
4.1.6 PSAM卡
4.1.7 符号和缩略语
4.2 密码应用目的及总体框架
4.2.1 基本安全要求
4.2.2 总体框架
4.3 密钥管理技术
4.3.1 三级密钥管理
4.3.2 密钥管理自身安全性
4.3.3 交易密钥
4.3.4 子密钥推导算法
4.3.5 过程密钥的产生
4.3.6 安全报文加密/解密计算方法
4.3.7 MAC/TAC计算方法
4.4 密钥应用技术
4.4.1 PSAM卡
4.4.2 安全报文传送
4.4.3 发卡流程
4.4.4 交易预处理
4.4.5 圈存交易
4.4.6 圈提交易
4.4.7 消费交易
4.4.8 取现交易
4.4.9 复合应用消费交易
4.4.10 灰锁消费交易
4.4.11 联机解扣交易
4.4.12 补扣交易
4.4.13 补充交易
4.4.14 修改透支限额交易
4.4.15 查询余额交易
4.4.16 查询明细交易
4.4.17 应用维护功能
4.5 典型案例
4.5.1 社会保障领域
4.5.2 城市一卡通领域
4.5.3 石化加油领域
第五章 借记/贷记/电子现金密码应用体系
5.1 业务概述
5.1.1 背景
5.1.2 借记业务介绍
5.1.3 贷记业务介绍
5.1.4 电子现金业务介绍
5.2 系统总体构架

5.3 密码应用需求
5.4 密码应用体系
5.5 非对称密钥管理技术
5.5.1 两级密钥管理
5.5.2 密钥种类
5.5.3 证书格式
5.5.4 公钥获取与验证
5.5.5 IC卡证书与网银证书的差异
5.6 对称密钥管理技术
5.6.1 一级密钥管理
5.6.2 卡片交易密钥
5.6.3 系统交换密钥
5.7 密钥应用技术
5.7.1 脱机静态数据认证
5.7.2 脱机动态数据认证（DDA\CDA）
5.7.3 应用密文和发卡行认证
5.7.4 安全报文
5.7.5 IC卡安全性
5.7.6 终端安全性
5.7.7 借记/贷记消费交易
5.7.8 电子现金支付交易
5.8 典型案例
5.8.1 金融IC卡试点项目（宁波市民卡）
5.8.2 中国工商银行金融IC卡建设
第六章 网上银行密码应用体系
6.1 概述
6.1.1 背景
6.1.2 主要业务
6.1.3 特点
6.1.4 发展趋势
6.2 密码应用目的及总体框架
6.2.1 密码应用需求
6.2.2 密码应用总体框架
6.2.3 PKI体系框架
6.3 公/私钥对及数字证书
6.3.1 什么是数字证书
6.3.2 RSA公/私钥对格式
6.3.3 X.509数字证书格式
6.3.4 证书分类
6.3.5 私钥存储方式
6.3.6 CSP和PKCS 11接口
6.3.7 PC/SC规范
6.4 数字证书签发与管理
6.4.1 基本功能模块
6.4.2 主要业务流程
6.4.3 OCSP服务
6.4.4 CRL服务

6.4.5 LDAP服务
6.5 数字证书应用技术
6.5.1 证书有效性验证
6.5.2 防止假网站与Web服务器证书
6.5.3 防止假网银软件与代码签名证书
6.5.4 身份认证与SSL
6.5.5 交易抗抵赖与数字签名
附录A 国内密码相关政策法规
A.1 商用密码管理条例
A.2 商用密码科研管理规定
A.3 商用密码产品生产管理规定
A.4 商用密码产品销售管理规定
A.5 商用密码产品使用管理规定
A.6 境外组织和个人在华使用密码产品管理办法
A.7 电子签名法
A.8 电子认证服务管理办法
A.9 电子认证服务密码管理办法
A.10 无线局域网
附录B 国内金融行业标准列表
B.1 国家标准
B.2 行业标准
附录C 关键标准汇总及简介
C.1 国内密码相关规范
C.2 中国金融集成电路卡规范
C.3 EMV支付系统集成电路卡规范
C.4 PKCS系列标准
附录D 主要密码服务厂商
D.1 江南科友公司介绍
D.2 北京江南歌盟科技有限公司
D.3 北京创原天地科技有限公司介绍
参考文献

第一图书网, tushu007.com

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