



中华人民共和国国家标准

GB/T 27909.2—2011

GB/T 27909.2—2011

银行业务 密钥管理(零售) 第2部分:对称密码及其密钥管理 和生命周期

Banking—Key management(retail)—
Part 2: Symmetric ciphers—Key management and life cycle

(ISO 11568-2:2005, MOD)

中华人民共和国
国家标准
银行业务 密钥管理(零售)
第2部分:对称密码及其密钥管理
和生命周期

GB/T 27909.2—2011

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

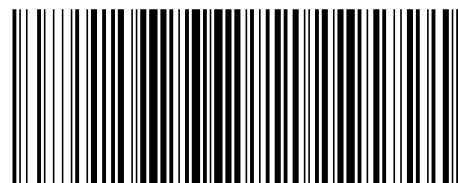
*

开本 880×1230 1/16 印张 2 字数 50 千字
2012年2月第一版 2012年2月第一次印刷

*

书号: 155066·1-44224 定价 30.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107



GB/T 27909.2—2011

2011-12-30 发布

2012-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 密钥管理技术的一般环境 3

 4.1 概述 3

 4.2 安全密码设备的功能 3

 4.3 密钥生成 4

 4.4 密钥计算(变形) 5

 4.5 密钥分级 5

 4.6 密钥生命周期 6

 4.7 密钥存储 6

 4.8 备份密钥的重新获取 8

 4.9 密钥的分发和导入 9

 4.10 密钥使用 9

 4.11 密钥更换 10

 4.12 密钥销毁 10

 4.13 密钥删除 10

 4.14 密钥归档 10

 4.15 密钥终止 10

5 提供密钥管理服务的技术 10

 5.1 介绍 10

 5.2 密钥加密 11

 5.3 密钥变形 11

 5.4 密钥衍生 11

 5.5 密钥变换 12

 5.6 密钥偏移 13

 5.7 密钥公证 13

 5.8 密钥标记 14

 5.9 密钥验证 15

 5.10 密钥识别 15

 5.11 控制和审计 15

 5.12 密钥完整性 16

6 对称密钥生命周期 16

 6.1 概述 16

6.2 密钥生成	16
6.3 密钥存储	17
6.4 备份密钥的恢复	17
6.5 密钥分发和导入	17
6.6 密钥使用	19
6.7 密钥更换	19
6.8 密钥销毁、删除、归档和终止	19
7 密钥管理服务的对照参考	20
附录 A (规范性附录) 本部分使用的符号	21
附录 B (规范性附录) 缩略语	22
参考文献	23

参 考 文 献

- [1] ISO 8732:1988 银行业务 密钥管理(批发)
- [2] ISO 9564-2:2005 银行业务 个人识别码(PIN)的管理和安全 第2部分:核准的 PIN 加密算法
- [3] ISO 9564-3:2003 银行业务 个人识别码(PIN)的管理和安全 第3部分:ATM 和 POS 系统中脱机 PIN 处理的要求
- [4] ISO/TR 9564-4:2004 银行业务 个人识别码(PIN)管理和安全 第4部分:开放网络中 PIN 处理指南
- [5] ISO 10202(所有部分) 金融交易卡 使用集成电路卡的金融交易系统的安全体系结构
- [6] ISO/IEC 11770-2 信息技术 安全技术 密钥管理 第2部分:使用对称技术的机制
- [7] ISO 15668 银行业务 安全文件传输(零售)
- [8] ISO/IEC 18031 信息技术 安全技术 随机数生成
- [9] ANSI X9.31 为金融服务业使用可逆公开密钥密码的数字签名
- [10] MENEZES, A., VAN OORSCHOT, P. 以及 VANSTONE, S. 编著的实用密码学手册, 1996 年 CRC 出版社出版
- [11] 特别报告(800-57)密钥管理建议 第1部分:国家标准和技术机构