

ICS 35.240.40

A 11

JR

中华人民共和国金融行业标准

JR/T 0025.17—2013

中国金融集成电路（IC）卡规范 第 17 部分：借记/贷记应用安全增强规范

China financial integrated circuit card specifications—
Part17: Enhanced debit/credit application security specification

2013 - 02 - 05 发布

2013 - 02 - 05 实施

中国人民银行 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 符号和缩略语 | 2 |
| 5 脱机数据认证 | 4 |
| 5.1 静态数据认证 (SDA) | 4 |
| 5.2 动态数据认证 (DDA) | 6 |
| 6 应用密文和发卡行认证 | 11 |
| 6.1 应用密文产生 | 11 |
| 6.2 发卡行认证 | 12 |
| 7 安全报文 | 13 |
| 7.1 报文完整性及其验证 | 13 |
| 7.2 报文私密性 | 13 |
| 8 安全机制 | 13 |
| 8.1 对称加密机制 | 13 |
| 8.2 非对称密码机制 | 16 |
| 9 认可的算法 | 16 |
| 9.1 对称加密算法 | 16 |
| 9.2 非对称算法 | 16 |
| 9.3 哈希算法 | 16 |
| 10 算法选择与交易流程 | 16 |
| 10.1 新增数据元 | 16 |
| 10.2 SM 算法应用方案 | 16 |
| 10.3 借记贷记应用流程 | 17 |
| 10.4 基于借记贷记应用的小额支付流程 | 19 |
| 10.5 qPBOC 应用流程 | 20 |
| 10.6 个人化相关密钥的初始化 | 20 |
| 11 PIN 修改/解锁命令数据计算方式 | 21 |
| 11.1 使用当前 PIN 修改 PIN 值 | 21 |
| 11.2 不使用当前 PIN 修改 PIN 值 | 22 |
| 附录 A (规范性附录) 算法标识 | 23 |
| 参考文献 | 25 |

前 言

JR/T 0025《中国金融集成电路（IC）卡规范》分为以下部分：

- 第1部分：电子钱包/电子存折应用卡片规范（废止）；
- 第2部分：电子钱包/电子存折应用规范（废止）；
- 第3部分：与应用无关的IC卡与终端接口规范；
- 第4部分：借记/贷记应用规范；
- 第5部分：借记/贷记应用卡片规范；
- 第6部分：借记/贷记应用终端规范；
- 第7部分：借记/贷记应用安全规范；
- 第8部分：与应用无关的非接触式规范；
- 第9部分：电子钱包扩展应用指南（废止）；
- 第10部分：借记/贷记应用个人化指南；
- 第11部分：非接触式IC卡通信规范；
- 第12部分：非接触式IC卡支付规范；
- 第13部分：基于借记/贷记应用的小额支付规范；
- 第14部分：非接触式IC卡小额支付扩展应用规范；
- 第15部分：电子现金双币支付应用规范；
- 第16部分：IC卡互联网终端规范；
- 第17部分：借记/贷记应用安全增强规范。

本部分为JR/T 0025的第17部分。

本部分依据GB/T 1.1—2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分主要起草单位：中国人民银行、国家密码管理局商用密码管理办公室、总参三部、中国工商银行、中国建设银行、中国邮政储蓄银行、中国银联股份有限公司、中国金融电子化公司、中国金融认证中心、银行卡检测中心、北京中电华大电子设计有限责任公司、北京诺君安信息技术有限公司、北京江南天安科技有限公司、北京华大信安科技有限公司、北京华大智宝电子系统有限公司、上海格尔软件股份有限公司、航天信息股份有限公司。

本部分主要起草人：王永红、李晓枫、陆书春、潘润红、杜宁、陈则栋、吴晓光、安晓龙、谢永泉、刘平、徐志忠、陈芳、汤洋、严伟峰、李东风、张永峰、赵宇、李春欢、张栋、汤沁莹、仲祺、施海平、李一凡、史大鹏、李建峰、李新、陈震宇、郑元龙、董浩然、韩小西、李国、汪朝晖、陈跃、谭武征、罗世新。

本部分为首次发布。