

金融标准化系列丛书-5

《中国金融集成电路(IC)卡规范(3.0版)》 解读

◎ 主编 李东荣

INTERPRETATIONS OF
CHINA FINANCIAL INTEGRATED CIRCUIT
CARD SPECIFICATIONS 3.0



 中国金融出版社

《中国金融集成电路(IC)卡规范(3.0版)》 解读

◎ 主编 李东荣

INTERPRETATIONS OF
CHINA FINANCIAL INTEGRATED CIRCUIT
CARD SPECIFICATIONS 3.0

责任编辑：吕楠

责任校对：孙蕊

责任印制：丁淮宾

图书在版编目 (CIP) 数据

《中国金融集成电路 (IC) 卡规范 (3.0 版)》解读 (《Zhongguo Jinrong Jicheng Dianlu (IC) ka Guifan (3.0 Ban)》Jiedu) / 李东荣主编. —北京: 中国金融出版社, 2014. 7

(金融标准化系列丛书-5)

ISBN 978-7-5049-7528-7

I. ①中… II. ①李… III. ①金融—IC 卡—行业标准—中国
IV. ①F832.2-65

中国版本图书馆 CIP 数据核字 (2014) 第 092973 号

出版

发行

中国金融出版社

社址 北京市丰台区益泽路 2 号

市场开发部 (010)63266347, 63805472, 63439533 (传真)

网上书店 <http://www.chinafph.com>

(010)63286832, 63365686 (传真)

读者服务部 (010)66070833, 62568380

邮编 100071

经销 新华书店

印刷 保利达印务有限公司

装订 平阳装订厂

尺寸 169 毫米×239 毫米

印张 17.5

字数 299 千

版次 2014 年 7 月第 1 版

印次 2014 年 7 月第 1 次印刷

定价 49.00 元

ISBN 978-7-5049-7528-7/F. 7088

如出现印装错误本社负责调换 联系电话 (010)63263947

一、主编

李东荣

二、编委

王永红 李晓枫 杨 竑 陆书春 潘润红 邬向阳

姜云兵

三、统稿

邬向阳

四、编写人员（按姓氏笔画排序）

邬向阳 刘力慷 汤沁莹 杜 宁 李兴锋 李铭铭

陈则栋 张 栋 张永峰 张家旗 陆 洋 周新衡

林发全 罗时辉 郑元龙 唐 博

序 言

标准化是为在一定范围内获得最佳秩序，对现实问题或潜在问题制定共同使用和重复使用的条款的活动。在现代经济发展过程中，标准化成为一国提升企业核心竞争力、争取发展话语权的重要途径。世界主要发达国家已逐渐将标准化提高到了国家发展战略的高度，成立专门从事标准化工作的组织，开展标准化工作，将发展中的成功经验，通过标准化的形式固化下来。

党中央、国务院历来高度重视标准化工作，并将标准化提高到了国家发展战略的高度，多次就标准化工作作出重要指示。金融作为现代服务业的重要组成部分、现代经济的“血液”，已成为衡量某个国家或地区综合竞争力和现代化标准的重要标志，对于标准化的要求显得更为迫切、更为重要。改革开放以来，我国金融标准化经过近二十年的发展，已逐步成为保证金融业规范化经营、提高整体核心竞争力的重要基础性条件。作为国家的中央银行，中国人民银行承担着制定和执行货币政策、维护金融稳定、提供金融服务的重要职责。随着金融改革的逐步深入，经济市场化程度的不断加深，金融标准化的地位和作用日益提高。在各相关单位的大力支持、积极参与下，中国人民银行和全国金融标准化技术委员会以立足现状、适度前瞻、突出重点、务实可行为原则，在金融领域内稳步推进标准化工作，陆续制定和发布了多项涉及银行、保险、证券、银行卡、征信业务等内容的国家标准和行业标准。同时，根据信息系统建设标准先行的指导原则，推出了一系列标准规范。

为使广大业内工作者和社会各界多渠道、多层次地了解中国金融标准化成果、标准化政策法规、国际标准化发展趋势等方面的内容，中国人民银行决定出版“金融标准化系列丛书”。经过精心的准备和各方面的共同努力，这套

丛书现在可以陆续和大家见面，该丛书的出版必将有力地推动我国金融标准化
的发展，为大家提供有益的参考。希望可以借此推动社会各界更好地了解金融
标准化，并希望金融标准化在全社会的关心支持下，在全行业人员的共同努力
下，得以更好、更快的发展，为金融业持续、健康、创新发展奠定基础。

李東榮

中国人民银行副行长

全国金融标准化技术委员会主任委员

二〇一二年九月

前 言

自 1997 年《中国金融集成电路（IC）卡规范》（以下简称“PBOC 标准”）问世以来，迄今已经历了三个版本，实践证明，PBOC 标准已经成为我国改善金融服务、实现金融服务民生的基础要素。但从实用角度看起来，每一版本标准的贡献度似乎差距很大，1.0 版本的卡在实际应用中基本没有留下痕迹，2.0 版本的卡在现实生活中扮演着大众金融伴侣的角色，而且身影遍及公共服务、小微交易，使得许多银行卡从一月一刷变成一日数刷。在取得如此成绩之际推出 3.0 版本，会不会影响既有成果的继续推进，毕竟，持卡人和银行业现在刚刚尝到甜头，投资尚未完全消化，社会效应也才初步显现。因此，解疑释惑就是本书任务之一。

自从采用了“芯”介质，银行卡的安全性、便利性、时尚性似乎刹那间得到了提升。但是同样用“芯”技术，为什么 1.0 与 2.0 效果不同，而 2.0 到 3.0 到底能有多大改进，显然，这与版本间采用技术不一样有关。现在可以下定论的是标准技术采用应该与社会环境的发展、技术消化吸收能力以及人民生活习惯相适应。一般情况下，技术难度与产生效果是一种正向关系，这也就是高技术在今日社会大受欢迎的基本原因。银行卡产业链条比较长，几乎每一过程都包涵高技术，为了更好发挥标准的高技术作用，技术解读就成了本书的任务之二。

标准要尽快受惠于社会各界，应用是最直接的方法，依赖应用体系的发挥，大家才能看到新版本的必要性。从标准支持的应用形式而言，1.0 的特色在于推

出了电子钱包，从此实现了无网络环境的应用；2.0的成功之处在于有了电子现金、多行业应用以及非接触特性，从此支持了多卡合一和闪付；3.0的创新应用在于有了分时分段计算、线上应用以及多币种，从此将可以在交通、互联网及境外更方便地使用。这些应用是目前社会生活中的大众需求，但怎样才能将成果快速呈现给社会，应用指导就成为本书的任务之三。

PBOC3.0标准成为我国改善金融服务、实现金融服务民生的基础要素，一方面是因为其继续兼容国际主流标准，使我国持卡人可以方便地在国际范围刷卡应用，同时，因为PBOC3.0加入了适合我国国情的电子现金扩展应用和自主可控的安全标准，使社会大众可以享受到更加安全快捷的金融服务，也将极大地带动我国相关产业的发展。

忙碌耕耘十数载，抬头环顾四周，PBOC3.0已然成为国际芯片应用领域的重要标准之一，这当中，社会经济发展给予了大好机遇，因此，尽快投入应用即是最好回报，希望本书的出版能起推动作用。

导 读

第一篇 PBOC 金融 IC 卡标准体系概述



第二篇 PBOC3.0 金融 IC 卡标准规范解析

PBOC 标准发展体系概述

PBOC3.0 主要功能解析

PBOC3.0 重点难点解析

PBOC3.0 安全体系介绍

PBOC3.0 个人化



第三篇 PBOC3.0 金融 IC 卡标准应用

PBOC3.0 标准技术业务支撑体系

PBOC3.0 项目实施与改造建议

PBOC 标准配套支撑体系



目 录

1 PBOC 标准发展体系概述	1
1.1 PBOC 标准的发展与 PBOC3.0 编制情况	1
1.1.1 PBOC 标准的发展历程	1
1.1.2 PBOC 标准与国际金融 IC 卡标准	2
1.1.3 PBOC 标准金融 IC 卡发展现状	4
1.1.4 PBOC3.0 编制背景	6
1.1.5 PBOC3.0 编制原则	7
1.1.6 PBOC3.0 组成部分	7
1.1.7 PBOC3.0 标准体系	8
1.2 PBOC3.0 与 PBOC2.0 的主要差异	9
1.2.1 丰富了金融 IC 卡产品功能	9
1.2.2 优化了非接电子现金流程	10
1.2.3 增加了对 SM 算法的支持	10
1.2.4 废止了对电子钱包的支持	11
1.2.5 完善了原有规范的部分描述	11
1.3 PBOC 标准与金融移动支付标准的关系	11
1.3.1 金融移动支付标准是 PBOC 标准的继承	11
1.3.2 金融移动支付标准是 PBOC 标准的创新	12
2 PBOC3.0 主要功能解析	15
2.1 与应用无关的接触式接口规范	15
2.1.1 文件和命令	15
2.1.2 卡片操作过程	16
2.1.3 复位应答	16
2.1.4 传输协议	17
2.2 与应用无关的非接触式接口规范	17

2 《中国金融集成电路 (IC) 卡规范 (3.0 版)》解读	
2.2.1 工作原理	18
2.2.2 初始化和防冲突	18
2.3 借记/贷记应用规范	19
2.3.1 标准借记/贷记内容	19
2.3.2 交易流程概述	19
2.3.3 交易流程说明	24
2.3.4 基于借记/贷记的小额支付应用规范	73
2.4 非接触式支付应用主要内容	73
2.4.1 交易预处理	74
2.4.2 交易路径选择	74
2.4.3 非接触 PBOC 应用	75
2.4.4 qPBOC 应用	75
2.5 非接小额扩展应用	79
2.5.1 新增文件和数据项	79
2.5.2 主要交易流程	80
2.5.3 业务场合	83
2.6 双币电子现金应用	83
2.6.1 新增数据元	83
2.6.2 基于借记/贷记应用的双币小额支付	84
2.6.3 基于 qPBOC 的双币电子现金	85
2.6.4 业务场合	86
2.7 金融 IC 卡互联网终端规范	86
2.7.1 应用背景	86
2.7.2 证书体系	87
2.7.3 安全通道	87
2.7.4 应用模式	88
2.8 增强型安全算法	89
2.8.1 应用背景	89
2.8.2 认可的算法	89
2.8.3 SM 算法应用方案	90
3 PBOC3.0 重点难点解析	92
3.1 借记/贷记难点分析	92
3.1.1 部分应用选择	92

3.1.2	接触式借记/贷记与非接触借记/贷记	92
3.1.3	CDA/DDA/SDA 区别	93
3.1.4	终端行为分析	94
3.1.5	持卡人认证处理	94
3.1.6	发卡行脚本执行限制	96
3.1.7	密钥种类说明	96
3.1.8	TLV 数据元编码规则	97
3.1.9	AID 编码规则	99
3.2	基于借记/贷记的小额支付难点分析	100
3.2.1	小额支付概念对比解析	100
3.2.2	卡片行为分析	100
3.2.3	电子现金充值流程	100
3.2.4	电子现金参数的修改	100
3.2.5	电子现金圈存日志	101
3.3	快速借记/贷记难点分析	102
3.3.1	可用脱机消费金额	102
3.3.2	与通讯接口有关的判断	102
3.3.3	卡片附件处理中的风险检查	102
3.3.4	Read Record 命令处理	103
3.3.5	金融 IC 卡动态签名的返回	103
3.3.6	交易时间限制	103
3.3.7	fDDA 版本 01	103
3.3.8	闪卡处理	105
3.4	非接触小额扩展应用难点分析	107
3.4.1	扩展应用与借记/贷记、电子现金应用的关系	107
3.4.2	非接小额扩展应用的闪卡处理	107
3.5	增强型算法难点分析	109
3.5.1	椭圆曲线算法概述	109
3.5.2	基于椭圆曲线的 SM2 算法	110
3.5.3	椭圆曲线算法与 RSA 算法比较	110
3.5.4	SM2 算法与通用椭圆曲线算法比较	111
3.6	PBOC3.0 与 EMV 规范的异同	112

4 PBOC3.0 安全体系介绍	117
4.1 密码学基础	117
4.1.1 密码学的发展历史	117
4.1.2 密码算法分类及原理	117
4.1.3 密钥系统安全的重要性	119
4.1.4 密码学的实际应用	121
4.2 金融 IC 卡安全体系架构	121
4.2.1 金融 IC 卡安全体系总体概述	121
4.2.2 金融 IC 卡芯片安全体系	122
4.2.3 金融 IC 卡嵌入式软件安全体系	124
4.2.4 金融 IC 卡应用安全体系	125
4.3 联机安全认证	126
4.3.1 联机安全认证目的	126
4.3.2 联机安全认证中的密码算法及识别方法	127
4.3.3 联机安全认证流程	127
4.3.4 联机安全认证密文计算过程说明	129
4.4 脱机数据认证	130
4.4.1 脱机数据认证目的	130
4.4.2 脱机数据认证类型	130
4.4.3 SDA/DDA/CDA/fDDA 的具体流程	131
4.5 行业密钥管理	137
4.5.1 概述	137
4.5.2 扩展应用下行业应用密钥管理	138
4.6 SM 算法概述	140
4.6.1 SM 算法的现实需求和发布背景	140
4.6.2 PBOC3.0 中使用的 SM 算法	141
4.6.3 关于 SM 算法银行需要做的升级工作	142
4.7 互联网终端安全	143
4.7.1 互联网终端自身安全机制	143
4.7.2 互联网终端与外界交易安全机制	143
5 PBOC3.0 个人化	149
5.1 卡片生命周期	149
5.1.1 芯片阶段	149

5.1.2	预个人化阶段	149
5.1.3	个人化阶段	149
5.1.4	用户阶段	149
5.2	金融 IC 卡通用个人化	150
5.2.1	通用个人化流程	150
5.2.2	金融 IC 卡个人化模板	151
5.3	借记/贷记应用个人化	158
5.3.1	个人化规范	158
5.3.2	个人化流程	158
5.3.3	个人化指令	159
5.3.4	个人化数据分组	160
5.4	借记/贷记卡个人化难点分析	161
5.4.1	数据分组要求	161
5.4.2	数据重复出现	161
5.4.3	数据重复设置	162
5.4.4	个人化安全控制	163
5.4.5	关键数据个人化	163
6	PBOC3.0 标准技术业务支撑体系	167
6.1	PBOC3.0 与银行卡相关规范	167
6.1.1	银行卡相关规范体系	167
6.1.2	PBOC3.0 对银行卡相关规范的影响	167
6.2	PBOC 标准金融 IC 卡业务规则	169
6.2.1	金融 IC 卡（借记/贷记应用）业务规则	169
6.2.2	金融 IC 卡（电子现金）业务规则	172
6.3	根 CA 管理规则/技术规范	175
6.3.1	管理规则	175
6.3.2	技术规范	176
6.4	联网联合技术规范	176
6.4.1	交易处理说明	176
6.4.2	报文接口规范	176
6.4.3	文件接口规范	177
6.4.4	数据安全传输控制规范	177
6.4.5	通讯接口	177

6.5	借记/贷记发卡行/收单行实施指南	177
6.5.1	发卡行实施指南	177
6.5.2	收单行实施指南	178
6.6	PBOC 标准金融 IC 卡风险防范	179
6.6.1	金融 IC 卡降级交易策略	179
6.6.2	金融 IC 卡伪卡风险责任转移	181
6.7	PBOC3.0 检测认证体系	183
6.7.1	检测要求概述	183
6.7.2	卡片检测要求	183
6.7.3	终端检测要求	189
7	PBOC3.0 项目实施与改造建议	194
7.1	PBOC3.0 实施要求	194
7.2	PBOC3.0 实施思路	195
7.3	PBOC3.0 系统改造范围	195
7.4	发卡行实施建议	196
7.4.1	实施准备	197
7.4.2	实施步骤	198
7.4.3	业务完善	199
7.5	收单行实施建议	199
7.5.1	实施准备	199
7.5.2	实施步骤	199
7.5.3	业务完善	199
7.6	发卡行技术改造要求	200
7.6.1	PBOC3.0 必备功能改造	200
7.6.2	非接小额扩展应用改造	203
7.6.3	双币电子现金改造	206
7.6.4	金融 IC 卡互联网终端改造	207
7.6.5	SM 算法应用改造	210
7.7	收单行技术改造要求	212
7.7.1	PBOC3.0 必备功能改造	212
7.7.2	非接小额扩展应用改造	213
7.7.3	双币电子现金改造	217
7.7.4	SM 算法应用改造	217

8 PBOC 标准配套支撑体系	218
8.1 电子现金跨行圈存	218
8.1.1 工程建设概要情况	218
8.1.2 关键技术实现方案	220
8.1.3 系统投产成效初步评估	226
8.2 多应用平台和规范	227
8.2.1 项目背景情况	227
8.2.2 多应用规范设计架构	229
8.2.3 多应用平台建设	230
8.3 交易流程优化	234
8.3.1 受理终端规范修订	234
8.3.2 发卡端关闭磁条芯片复合卡降级交易	238
8.4 金融 IC 卡片安全检测实验室建设	239
8.4.1 项目背景	239
8.4.2 项目建设情况	240
8.4.3 项目成果及意义	243
8.5 非接商圈建设	245
8.5.1 非接商圈建设作用重大	245
8.5.2 非接商圈建设典型方案	245
8.5.3 非接商圈建设推动情况	250
8.6 移动金融安全可信公共服务平台 (MTPS)	251
8.6.1 工程建设概要情况	251
8.6.2 关键技术实现方案	253
8.6.3 系统投产成效初步评估	257
附录: PBOC3.0 标准常见问题	258
参考文献	262

1 PBOC 标准发展体系概述

1.1 PBOC 标准的发展与 PBOC3.0 编制情况

1.1.1 PBOC 标准的发展历程

2000 年以前,金融 IC 卡在金融领域以电子钱包等小额支付应用为主,主要的标准包括 Visa 的 Visa Cash、万事达的 Mondex、EMV 的 EMV96 等。在 EMV96 和 ISO7816 的基础上,结合国内需要,中国人民银行于 1997 年颁布《中国金融集成电路(IC)卡规范》(1.0 版),业内也称之为 PBOC 1.0 规范。

从应用角度区分,PBOC1.0 规范主要定义了电子钱包(Electronic Purse)/电子存折(Electronic Deposit)应用和磁条卡功能(Easy Entry)应用。其中,电子钱包/电子存折采用对称密钥算法,通过全国统一的三级密钥管理体系,解决了脱机情况下跨行、跨地区的支付问题。PBOC1.0 规范通过建立统一的技术标准规范,进一步加强了银行与行业、企业间的沟通合作,在技术创新、业务创新、制度创新和商业模式创新等层面推动了金融 IC 卡跨行业应用新措施和新办法的探索,并在 PBOC1.0 规范试点及其后续的行业合作中,逐步显示出金融 IC 卡的潜力。

PBOC1.0 规范的正式发布对金融 IC 卡产业有着非常重要的意义,电子钱包/电子存折应用为当时跨行、跨地区的脱机支付问题提供了解决方案,标志着我国金融业在金融 IC 卡方面开始有了自己统一的规范,并为今后建立一个全国互通的金融 IC 卡交易系统,实现基于芯片卡的电子货币打下了基础。PBOC1.0 规范的颁布是我国金融 IC 卡事业发展的一个里程碑。

2000 年前后,为了防止日益增长的伪卡欺诈和金融支付应用面临的各种挑战,国际卡组织调整了金融 IC 卡发展重点,开始在全球大力推广借记/贷记卡的金融 IC 卡化,即 EMV 迁移。随着国际银行卡 EMV 迁移进程的加快和我国对外开放交流步伐的加大,中国人民银行高度重视并及时跟踪、研究国际芯片化在全球的应用和最新的动态。2003 年,中国人民银行组织中国银联和有关商业银行对《中国金融集成电路(IC)卡规范》(1.0 版)进行了修订,补充完善了电子钱包/电子存折的应用功能并增加了电子钱包扩展应用指南、借记/贷记卡应用功能、个人化应用指南和非接触式金融 IC 卡通信接口标准。2005 年 3 月修订后的新规范正式颁布实施(业界称该规范为 PBOC2.0 规范)。

PBOC2.0 规范新增的标准借记/贷记产品实现了银行卡的借记/贷记功能,