

附件 1

金融 IC 卡发卡机构 实施要点

二〇一一年五月

目 录

1. 启动准备.....	8
1.1 政策文件	8
1.2 标准规范	9
1.3 业务规则	9
2. 业务规划.....	9
3. 卡产品选择.....	10
4. 业务流程制定.....	10
5. 系统建设.....	11
5.1 数据准备系统	11
5.2 个人化系统	11
5.3 授权系统	11
5.4 清算系统	12
6. 发卡机构 CA 建设.....	12
7. 联网测试.....	12

为落实《中国人民银行关于推进金融 IC 卡应用的意见》，保证 PBOC2.0(《中国金融集成电路（IC）卡规范》(JR/T 0025-2010)) 标准金融 IC 卡应用工程实施，特制定本要点。本要点适用于计划实施 PBOC2.0 标准金融 IC 卡工程，开展金融 IC 卡发卡业务的发卡机构。

本要点为发卡机构实施 PBOC2.0 标准金融 IC 卡工程提供一个整体引导。描述了发卡机构实施 PBOC 迁移的路线图，提供了 PBOC 迁移过程中所需要注意的相关事项和要点。

发卡机构在正式发行 PBOC2.0 金融 IC 卡前，工程实施通常会经历启动准备、业务规划、产品选型、业务流程制定、系统建设、CA（认证中心）建设、入网检测等几个阶段。各阶段开始的先后顺序可由发卡机构自行确定。与收单业务相关的内容可参见《金融 IC 卡收单机构实施要点》，与转接业务相关的内容可参见《金融 IC 卡转接机构实施要点》。

1. 启动准备

为推动金融 IC 卡发卡业务尽快开展，发卡机构应首先对相关参与人员开展 PBOC 规范、管理办法以及业务规则等相关知识的培训。培训人员范围应包括市场推广人员、客服员工、业务支持员工、后台处理员工、系统开发团队、法律顾问以及风险管理人。

培训主要内容包括：

1.1 政策文件

- ◆ 中国人民银行 发展改革委 公安部 财政部 信息产业部 商务部 税务总局 银监会 外汇局关于促进银行卡产业发展的若干意见（银发〔2005〕103号）
- ◆ 中国人民银行关于规范和促进银行卡受理市场发展的指导意见（银发〔2005〕153号）
- ◆ 中国人民银行 银监会 公安部 工商总局关于加强银行卡安全管理

预防和打击银行卡犯罪的通知（银发〔2009〕142号）

- ◆ 中国人民银行办公厅关于贯彻落实《中国人民银行 中国银行业监督管理委员会 公安部 国家工商总局关于加强银行卡安全管理、预防和打击银行卡犯罪的通知》的意见（银办发〔2009〕149号）
- ◆ 中国人民银行关于推进金融IC卡应用工作的意见（银发〔2011〕64号）

1.2 标准规范

- ◆ 《银行卡卡片规范》（JR/T 0052-2009）
- ◆ 《中国金融集成电路（IC）卡规范》（JR/T 0025-2010）
- ◆ 《银行卡联网联合技术规范》（JR/T 0055-2009）

1.3 业务规则

- ◆ 《银联卡业务运作规章 第七卷 IC卡业务规则》

2. 业务规划

发卡机构应做好金融IC卡发展规划，确定实现的业务功能及策略，可根据自身特长有选择地开展支付应用、行业应用、中间业务、创新业务及管理应用。目前，PBOC2.0标准的金融IC卡主要支持以下功能：

- ◆ PBOC2.0标准借贷记功能。在IC卡上实现银行卡借贷记功能，在安全性上有了极大的提高，可完全替代现有磁条卡的全部功能，适用于现有磁条卡的所有受理范围。
- ◆ PBOC2.0标准小额支付功能。基于借记/贷记应用规范基础上的小额支付功能，适用于脱机业务场景。
- ◆ 非接触式支付功能。采用非接触式技术，可以实现和拓展借贷记及小额支付的支付功能，适用于在快速交易场合及特殊环境场合的支付。

制定业务策略时应考虑：

- ◆ PBOC2.0标准的金融IC卡相对于磁条卡而言，在业务处理、交易确认、清算及差错处理等方面都进行了补充。发卡机构应根据自身业务需求制

定相应业务策略和市场策略，处理好与转接机构和持卡人之间的关系，如：争议处理、客户服务等。

- ◆ 发卡金融机构应按人民银行和有关政府部门的相关政策，与联合发卡的其他行业单位签订合作协议，明确各方的责任与义务。
- ◆ 如采用系统外包，应加强外包机构资质考察，签订安全保密协议，落实应急处置预案及本发卡机构相关管理要求。

3. 卡产品选择

根据不同的应用需求，金融 IC 卡的卡片结构、存储容量、参数设置的要求不同。发卡机构在发行金融 IC 卡产品时应考虑：

- ◆ 卡片应满足 PBOC2.0 标准的相关要求，应通过人民银行认可的检测机构的检测，鼓励使用满足安全、应用等要求的国产芯片；
- ◆ 卡片应支持 PBOC2.0 标准的应用流程，如授权控制、持卡人验证方法、脱机数据认证、联机卡片认证与发卡机构认证、发卡机构脚本处理；
- ◆ 根据业务需要，确定存储器的大小、处理器和协处理器的性能以及接触式或非接触式接口，确保支持所需的金融 IC 卡应用。

4. 业务流程制定

相对磁条卡，发行金融 IC 卡时应关注以下几方面：

- ◆ 申请发卡行证书时，应考虑发卡行证书有效期、签发发卡行证书的私钥对应的公钥模长，以及卡片的有效期。
- ◆ 确定金融 IC 卡需要签名的静态数据列表，并选择合适的 IC 卡风险控制参数，如脱机限额、发卡行行为代码。
- ◆ 多行业应用情况下，应考虑卡片的应用加载流程和卡片发行流程。
- ◆ 确定金融 IC 卡降级交易的风险处理规则。
- ◆ 确定卡片使用和管理的业务规则，如补卡、换卡、销卡对脱机余额的处理。

- ◆ 确定脱机交易明细的查询途径。

5. 系统建设

金融 IC 发卡系统的建设可以通过自主开发、定制、外包或混合等方式完成。主要包括以下内容：

5.1 数据准备系统

发卡机构应建立自己的数据准备系统，用于生成持卡人的数据文件，除了原有磁条卡数据以外，还包括 IC 卡中的特别数据，例如：发卡机构参数、发卡机构行为代码、应用缺省行为、持卡人校验方法等；

数据准备系统中的持卡人数据可以由发卡机构生成，IC 卡数据可以由第三方 IC 卡专业化公司代为生成。

5.2 个人化系统

发卡机构通过建立卡片个人化系统，将数据准备系统准备好的数据以及卡片中的各类密钥和证书以安全的方式写入 IC 卡中。

卡片个人化系统可以由发卡机构独立完成，也可以外包给第三方专业化公司完成（但要做好双方之间的数据和卡片的安全传递与管理）。

5.3 授权系统

发卡机构需根据《银行卡联网联合规范》对 PBOC 交易处理的要求，进行相关改造，主要包括：

- ◆ 联机报文需要能支持 IC 卡信息；
- ◆ 能够提供联机时的卡片和发卡机构的双向认证，主要是 ARQC（授权请求密文）的验证和 ARPC（授权响应密文）的生成；
- ◆ 支持发卡行脚本的生成和下发；

除了传统的风险管理外，发卡机构还需要根据 ARQC 的验证结果以及 TVR（终端验证结果）和 CVR（卡片验证结果）来给出交易的授权结果。

5.4 清算系统

发卡机构清算系统需进行下述改造，以满足金融 IC 卡相关交易的要求：

- ◆ 能接受和处理 IC 卡脱机交易（如发卡机构支持小额脱机交易）；
- ◆ 能对该交易的 TC（交易证书）值进行校验。

6. 发卡机构 CA 建设

金融 IC 卡借记/贷记应用公钥认证体系包括根 CA、各发卡机构 CA 及其发行的 PBOC 标准 IC 卡、收单机构及其 ATM 和 POS。金融 IC 卡借记/贷记应用公钥认证系统使用公钥密码技术进行金融 IC 卡静态数据、动态数据或复合数据的生成及认证，以提供高度安全的金融 IC 卡交易认证服务。为完成 PBOC 相关交易，发卡机构需建立自己的 CA，以完成：

- ◆ 生成发卡机构公私钥对，并将公钥提交给根 CA；
- ◆ 接受根 CA 签发的发卡机构证书；
- ◆ 签发 IC 卡证书。

IC 卡证书签发完成后将被放置入用户卡中，并在用户交易过程中进行安全性验证。发卡机构 CA 可以由发卡机构独立建设，也可以外包给人民银行认可的第三方专业化公司。

7. 联网测试

- ◆ 发卡机构选择的卡片必须通过人民银行认可的检测机构的检测。
- ◆ 按照联网通用的要求，发卡机构在完成内部测试之后，应与中国银联进行入网测试。中国银联应协助发卡机构做好入网测试工作，保障金融 IC 卡联网通用及安全接入和运行。