与 MASTERCARD 合并，2005 年 JCB 购入 EMV Co.的 1/3 股份，2009 年美国运通也加入 EMV 组织，拥有 1/4 股份。

EMV 标准是关于智能卡及读卡终端用于银行卡支付的规范，着眼于取代磁条卡，实现全球范围的跨国界、跨厂商、跨金融机构的互操作，并提供一卡多功能应用的基础。EMV 建立在 ISO 7816 系列标准基础之上，定义了智能卡及终端之间的通信规范、卡以及持卡人的授权方法以及卡与终端的风险管理框架，从技术上分为两个层次，设备供应商必须取得这两个层次的测试及认可。EMV 标准主要包括：EMV96 (EMV 3.1.1)、EMV2000 (EMV 4.0)、EMV4.1、CCD（EMV 通用核心定义）、CPA（EMV 通用支付规范）、EMV 4.2 等。

EMV 迁移是按照 EMV 标准，在发卡、业务流程、安全控管、受理市场、信息转接等多个环节实施推进银行磁条卡向芯片卡技术的升级，即把现在使用磁条的银行卡改换成使用 IC 卡的银行卡。随着信息技术、微电子技术的发展和 EMV 标准的完善及国际 EMV 迁移计划的实施，而且银行磁条卡存在伪卡、盗卡欺诈等方面的安全隐患，银行磁条卡向 IC 卡的迁移是必然的发展趋势。

### 2．EMV 密码应用需求

银行 IC 卡借记/贷记业务的密码技术需求是由银行卡组织制定的相关 IC 卡标准和 IC 卡芯片技术这两方面决定的。与银行借贷记磁条卡相比，发行银行 IC 卡在技术上要复杂得多。由于每张 IC 卡片中都保存了卡片的唯一密钥和由发卡行签发的静态数据或证书，因而要发行银行 IC 卡片的发卡行必须建设一整套密钥管理体系，同时还需要对相关系统进行改造，整体密码应用需求包括以下几个方面。

（1）密钥管理体系和技术需求。

需要建立一整套银行 IC 卡借贷记应用相关的对称和非对称密钥管理体系结构、安全合理的密钥交换技术等密码需求。

（2）脱机认证密码应用需求。

建立可实现的脱机认证流程和密码算法，通过数字证书和对称算法的交易证书方式实现脱机业务的合法性和可验证性。

（3）数据保护及完整性密码应用需求。

密码技术应用于银行 IC 卡借贷记业务中的数据传输保护和完整性验证等，如 PIN 转加密、验证、数据加密、MAC 计算和验证等。

（4）联机发卡行认证授权密码应用需求。

通过专用密码技术实现银行 IC 卡借贷记和电子现金应用的发卡行授权机制，替代原有银行磁条卡借贷记的卡号密码验证和信用卡 CVV 验证等方式的发卡行授权机制。

### 3．EMV 非对称密钥管理体系

非对称密钥管理体系主要用于支撑 IC 卡脱机业务安全和认证。EMV 非对称密钥采用两级密钥管理体系，如图 3-2 所示，包括根 CA 系统和发卡行 CA 系统。

（1）根 CA 系统。

该系统主要用于生成根 CA 证书；接受发卡行证书申请，为发卡行签发公钥证书；向收单行发布根 CA 公钥，通过收单行将根 CA 公钥分发到受理终端。

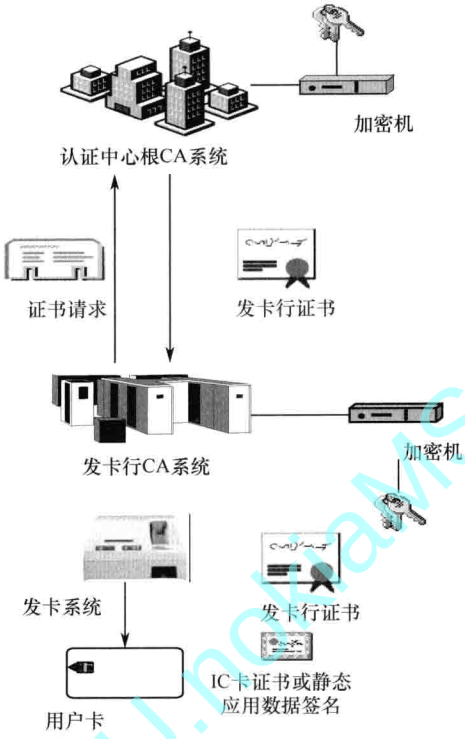


图 3-2　EMV 两级非对称密钥管理体系结构

（2）发卡行 CA 系统。

发卡行借贷记应用 CA 系统是整个系统的安全核心系统，主要负责完成发卡行证书的申请、管理、IC 卡应用相关的密钥（包括应用密钥、卡片个人化交换主密钥等）管理，同时负责分发各类密钥到卡片制造商、卡片个人化中心及业务前置交易加密机等。

### 4．密钥种类

EMV 非对称密钥管理涉及的密钥种类主要有根 CA 公私钥对、发卡行公私钥对和 IC 卡公私钥对三种，如表 3-2 所示。

表 3-2　非对称密钥列表

| 类　型 | 功　能 |
| --- | --- |
| 根 CA 公钥 | 由认证中心产生，以公钥证书文件形式下发。发卡行用于验证发卡证书有效性 |
| 根 CA 私钥 | 由认证中心产生，存储在加密机中。用于签发发卡行公钥证书 |
| 发卡行公钥 | 由发卡行产生，并经过 CA 中心签发后形成发卡行公钥证书。用于发卡时装载到 IC 卡中 |
| 发卡行私钥 | 由发卡行产生，并通过加密机密钥加密后存储在主机数据库中。用于签发 IC 卡静态数据签名及 IC 卡公钥证书 |
| IC 卡公钥 | 采用 DDA 认证方式的卡片需要此密钥，由发卡行私钥签发形成 IC 卡公钥证书存储在 IC 卡 |
| IC 卡私钥 | 采用 DDA 认证方式的卡片需要此密钥，用于 IC 卡与终端进行 DDA 认证 |

### 5．IC 卡证书与网上银行 PKI 证书的差异性

银行 IC 卡证书和网上银行 PKI 证书体系有很大差异，一种是符合 PKI 标准的 X.509 证

书；一种是符合金融 IC 卡标准的证书（EMV 标准的外卡与此方式类似）。以下对这两种证书及体系进行分析比较。

（1）证书格式。

① 证书的数据组织格式完全不同。PKI 证书采用 DER 编码方式，银行 IC 卡证书采用固定长度方式。

② 银行 IC 卡证书数据为密文数据，需解密后才能解析；X.509 证书数据为明文。

③ 银行 IC 卡证书数据中包括的关键数据项与 X.509 证书完全不同，并且证书相关数据项数量比较多，信息也比较复杂，如下：

PKI X.509 证书关键数据项包括：版本号、序列号、签名算法标识符、认证机构、有效期限、主题信息、认证机构的数字签名、公钥信息等。

银行 IC 卡证书关键数据项包括：证书格式标识、应用主账号、应用主账号序列号、证书失效日期、证书序列号、注册的应用提供商标识、认证中心公钥索引、应用交互特征 AIP、应用生效日期、应用失效日期、应用用途控制 AUC、持卡人验证方法（CVM）列表、发卡行公钥证书、发卡行公钥指数、发卡行行为代码（缺省、拒绝、联机）、发卡行国家代码等。

（2）发证方式。

网银 PKI 证书与 IC 卡证书发证方式如表 3-3 所示。

表 3-3　网银证书与 IC 卡证书发证方式的比较

| 比较项 | 网银证书 X.509 | 银行 IC 卡证书 |
| --- | --- | --- |
| 外围系统支持 | 不需要外围系统支持 | 需要申请和接收卡组织支付系统根 CA 系统签发的发卡行证书。<br>需要银行核心系统提供账户账号 |
| 预制证书 | X.509 证书中的“主题信息”项中必须包括持卡人姓名等个人信息。实现预制证书业务会导致证书中持卡人信息项无效，证书绑定制卡人后，通过后台系统进行关联。<br>证书存储介质采用 USB Key，没有配套的批量设备，只能形成证书数据文件，通过柜面交易写入设备 | 与持卡人信息无关，但是需要银行核心系统提供账号号段。<br>证书存储介质采用 IC 卡，由批量设备将预制证书写入 IC 卡内，形成预制卡。<br>通过柜面交易绑定个人后，将制卡人信息写入 IC 卡 |
| 柜面在线发证 | 由 USB Key 产生公私钥对，公钥及相关信息通过 RA 系统等提交后台 CA 系统签发证书 | 不支持 |
| 预约卡 | 不适用，没有此类业务 | 支持贷记 IC 卡的预约制卡业务 |
| 签名及摘要算法 | RSA，SHA-1 | RSA，SHA-1 |
| 证书密钥对 | 两种方式：<br>（1）USB Key 生成<br>（2）密码机生成 | 只支持密码机生成 |
| 证书有效期 | 与证书密钥对无关，由银行网银 CA 系统定义 | 与证书密钥对相关，由银行卡组织（中国银联、EMV）定义 |
| 证书唯一性 | 绑定个人。每个用户只能拥有一张网银证书 | 绑定账户账号。每个账户只能有一张证书，每个用户可以拥有多种证书 |

（3）交易业务。

对于基于网银证书和银行 IC 卡证书开展的银行金融业务来说，差异比较大。网银证书主要为互联网上银行业务服务；银行 IC 卡证书主要为银行卡借记、贷记业务服务，与原有的银行磁条卡的业务相同，如表 3-4 所示。

表 3-4　网银证书与 IC 卡证书交易业务的比较

| 比较项 | 网银证书 X.509 | 银行 IC 卡证书 |
| --- | --- | --- |
| 证书发布 | 支持 | 不支持 |
| 黑名单发布 | 支持 | 不支持 |
| 柜面业务 | 不适用，不需要证书认证 | 需要证书认证 |
| 互联网业务 | 支持，需要证书认证，并实现操作签名和数据加密等功能 | 不支持 |
| 数据加密 | 支持 | 不支持 |
| POS 机交易 | 不支持 | 支持 |

具体技术细节请参考《商业银行密码技术应用》“第五章 借记/贷记/电子现金密码应用体系”。

# 第二部分

# PKI 技术基础