④ 对于不同密码算法的介质，访问接口应统一管理。如可采用 CSP（需扩展）或国密接口统一访问 SM2 算法或 RSA 算法的介质等。

⑤ 用户证书更新时可能需要自己输入介质口令，发证点可考虑配置用户密码键盘。

6. 发证点管理（LRA）

发证点特指能为证书申请者提供纯证书业务（证书申请/补办/更新、证书作废、证书冻结/解冻、证书解锁等）和支撑类业务（计费收费、档案管理、项目及产品管理、发证点管理、用户管理等）且独立经营的业务单元。

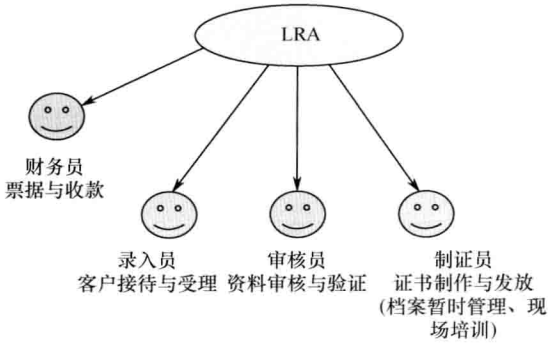

图 25-8　发证点岗位设置

从岗位设置考虑，发证点的主要业务工作可分为客户接待与受理、证书资料审核与验证、证书制作与发放（档案暂时管理、现场培训）、票据与收款等 4 类。为控制风险，证书受理、资料审核与验证不应由同一个人承担，其他岗位可一人多岗。发证点岗位设置如图 25-8 所示。

发证点管理基本要求如下：

① 应能对发证点进行控制或授权。具体包括：发证数量（包括总发证数量、某项目总发证数量、某项目某类证书总发证数量等）、能发哪些项目的证书、能发项目中的哪类证书、设定管理员、是否允许自主管理（如创建下级发证点、增加操作员、变更操作员角色、给操作员授权等）、某类证书允许使用的介质等。

② 发证点自身安全控制。具体包括：应支持多级；上级发证点业务人员具有下级发证点的对应权限；发证点人员至少分 2 类（管理员和操作员。操作员应分为多类角色：录入员、审核员、制证员、财务员，管理员可对操作员进行管理）；发证点所有人员应使用数字证书进行身份认证；发证点操作员应负责资料收取、信息录入、业务审核、费用收取等职责；发证点管理员应负责资料归档及上报、费用汇总及结算等职责；发证点应不用部署任何系统，直接通过浏览器进行业务操作；管理员对操作员进行授权（如哪些项目、哪类证书等）。

③ 应支持发证点的调整或合并，保证针对原有证书的各种业务不受影响。具体包括：某些发证点的上级发证点发生变更；某些发证点合并。

④ 发证点应能验证用户信息。

⑤ 跨发证点业务办理。具体包括：不同发证点可能属于不同的利益集团；当用户在发证点 A 申请证书，在发证点 B 更新证书时，属于跨发证点业务办理，应提供支持。

7. 业务类型管理

证书业务类型主要包括：证书申请、证书作废、证书解冻、证书冻结、证书解锁、证书更新（信息不变）、证书变更（信息变化）等。

业务类型管理基本要求如下：

① 应记录每笔证书业务的详细信息，包括时间、类型、费用、操作对象、操作者、签名等。业务记录不仅包括发证点业务操作，也包括用户自助服务业务操作。

② 当发证点操作员的业务操作失误时（如 DN 项录入错误后制证成功），应允许重新制证（原证书应作废），并增加标记，不影响证书或业务统计查询、计费收费。

③ 针对证书更新时存在的 RSA 更新为 SM2、单证书更新为双证书等情况，可增加不同

的证书更新业务类型来实现，如证书更新 I（RSA 到 SM2）、证书更新 II（单证到双证）等。

④ 证书业务流程主要包括以下环节：受理、审核、收费、制证、绑定、发票、结算、归档等，如图 25-9 所示。

⑤ 应支持批量申请和批量下载功能。如基于 Excel 文件批量提交、按照特定顺序批量下载（如 Excel 文件顺序）等。

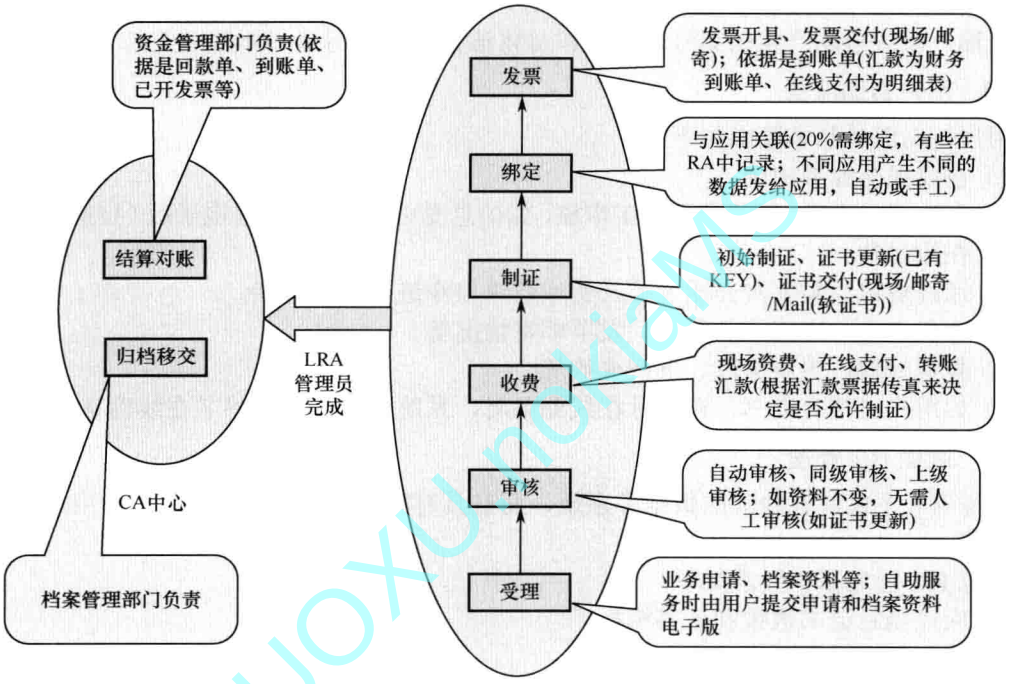

图 25-9 证书业务流程

8. 计费收费

证书业务收费有两种模式：用户自主付费和客户承担费用。客户是指应用系统所有者，如国税局，用户是证书申请者，如报税企业。

用户自主付费模式下，计费收费管理基本要求如下：

① 发证点需按照计费策略，实时计算费用并收取。

② 业务费用应包括介质费、证书服务费、增值服务费等。

③ 应支持用户以多种方式缴费：现场缴费（现金/支票）、远程汇款（邮局汇款/银行转账）、网上支付（个人网银/企业网银/第三方支付）等。

④ 支持多种优惠促销政策。

⑤ 支持证书变更时，新证书有效期可能小于一个完整计费周期时的计费规则。

⑥ 支持退费业务。

⑦ 应支持多种发票送达方式：现场交付、事后自取、事后邮寄（需录入邮寄地址）等。

9. 档案管理

档案特指证书业务中需要用户提交的各种书面资料。

档案管理基本要求如下：

① 可以给项目设定该项目允许的档案清单，也可以直接给项目中某类证书设定该证书允许的档案清单，或者给某类证书的某类业务设定该业务允许的档案清单。如营业执照复印件、经办人身份证复印件、证书申请书、企业介绍信等。

② 证书业务所需档案清单，应依据 CPS 设定。

③ 为方便档案管理，在进行业务处理时，操作员选择或录入用户实际提交的各种书面资料名称，系统自动产生档案号，由操作员将该档案号书写到书面资料上。

10. 用户自助服务

用户自助服务基本要求如下：

① 在线提交业务申请。

② 在线证书更新：可能需要人工审核，如信息变更，需上传资料电子版（扫描件/照片）。

③ 在线付款。

④ 远程解锁：需要对介质主控密钥或解锁口令进行统一管理。

⑤ 业务查询：申请业务状态、发票邮寄情况等。

⑥ 异常处理：更新失败、下载失败等。

⑦ 如用户已拥有证书，在进行在线业务时，系统可通过用户签名在线确认用户身份。

11. 远程 RA 管理

远程 RA 不仅具有独立的数据库系统，而且具有独立的发证点/项目/产品/用户/计收费管理功能。

远程 RA 管理基本要求如下：

① 应控制总证书数量和证书模板。

② 用户数据是否向上同步。

③ 远程 RA 应通过服务器证书保证安全性。

④ 应能控制远程 RA 管理员。

12. 证书追溯（生命周期展现）

证书追溯是指对与某用户、某证书或某介质关联的所有证书进行查询并显示出来。

证书追溯机制具体要求如下：

① 针对某用户，应能展示所有历史证书，即使用户名称发生变更。

② 针对某证书，应能展示所有更新的历史证书，即使密钥发生变化。

③ 针对某介质，应能展示所有历史证书，即使用户发生变化；包括返修 KEY。

25.1.3 管理模式示例

1. 示例 A

图 25-10 给出了一种管理模式的实现形式，其中证书模板中的属性项可自定义，功能比较强大；证书模板支持授权管理；支持独立的用户管理功能；支持双证书和两种模式单证书（用户端产生和 KMC 产生密钥对）等。

2. 示例 B

图 25-11 给出了一种管理模式的实现形式，其中证书模板中的属性项不允许自定义，

证书模板不支持授权管理，不支持独立的用户管理功能，只支持双证书等。

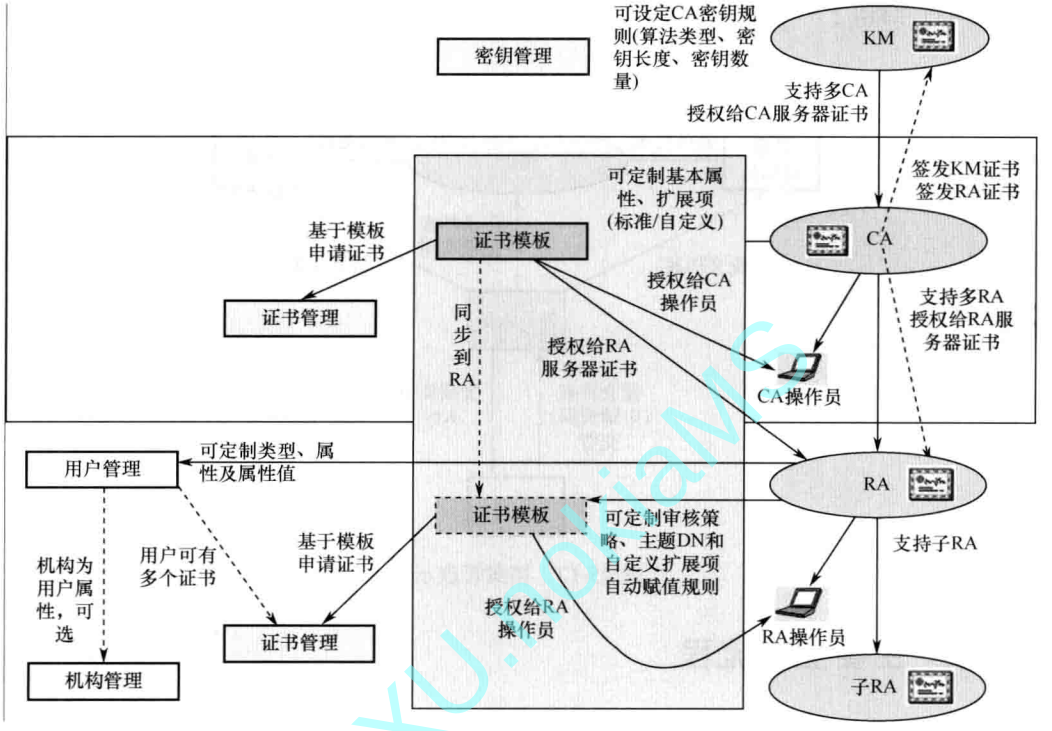

图 25-10　管理模式示例 A

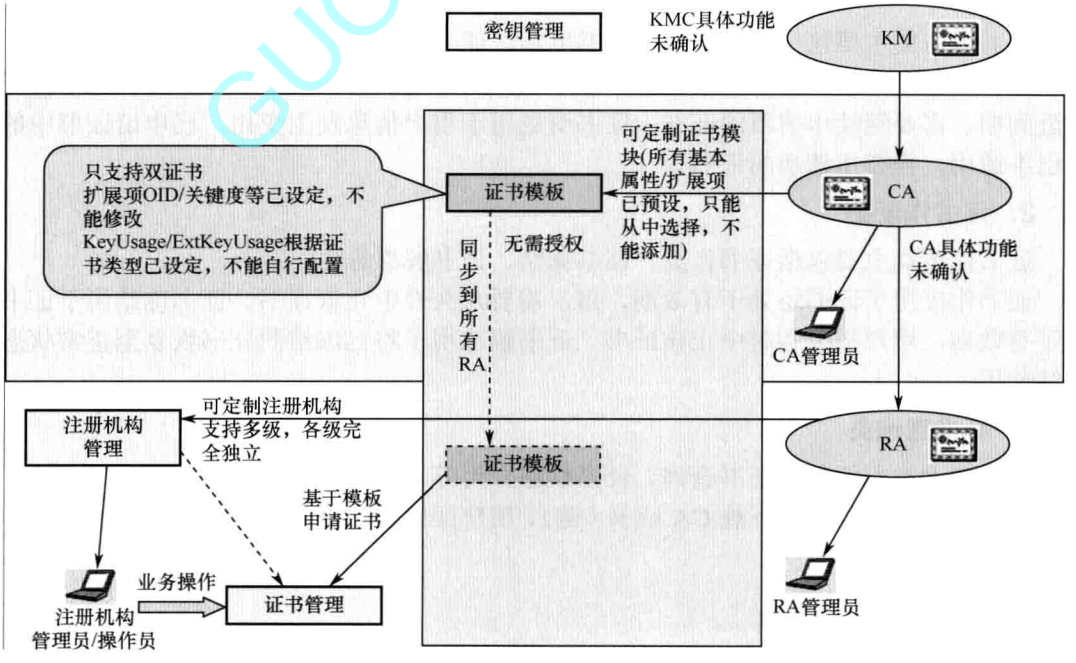

图 25-11　管理模式示例 B

3．示例 C

图 25-12 给出了一种档案管理的实现形式，其中同时支持项目管理、档案管理、收费管理等。

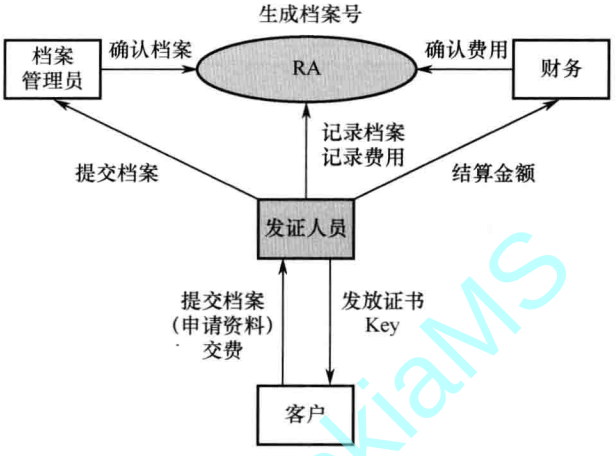

图 25-12 档案管理示例

25.2 主要业务流程

CA 中心面向用户（证书申请者）提供的业务办理类型可分为三大类。

1．证书申请类

证书申请类主要包括证书申请、证书更新、证书变更等。

证书申请用于用户首次申请证书。证书更新用于用户信息没有发生变化，已申请证书临近到期，需要继续申请新的证书。证书变更用于用户信息发生变化，已申请证书中的内容已不适用，需要申请新的证书。

2．证书作废类

证书作废类主要包括证书作废、证书冻结、证书解冻等。

证书作废用于证书还处于有效期，用户需要永久性中止该证书。证书冻结用于证书还处于有效期，用户需要临时中止该证书。证书解冻用于将已冻结的证书恢复至正常状态，继续使用。

3．证书查询类

证书查询类主要包括证书查询、证书状态查询等。

证书查询用于查询并下载 CA 证书（链）、用户证书等。证书状态查询主要采用 OCSP、CRL 等方式。

25.2.1 证书申请类

证书申请类的业务流程如图 25-13 所示。