⑤ 证书签发者 CA 决定作废该证书等。

如发生上述前三项原因，证书持有者应主动发出证书作废申请。

1. 提出申请

用户（证书作废申请者）如实填写“证书作废申请表”，并认真阅读“数字证书服务协议”，按要求在申请表和服务协议上签名或盖章（个人证书作废申请应签名，机构证书作废申请应加盖公章）。证书作废申请书中需要注明作废理由。个人和机构数字证书作废申请表样例分别参见表 25-1 和表 25-2，数字证书服务协议样例参见表 25-3。

按要求准备相关资料后，向 CA 中心提交证书申请。提交的资料与证书申请类似。

2. 受理申请并审核

CA 中心录入员负责内容检查和信息录入。如果检查不合格，则提示申请人补充完善；如果检查合格，则将作废申请信息录入 RA 系统。检查内容与证书申请类似。

CA 中心审核员负责信息审核。如果审核不合格，则在 RA 系统中标记审核不通过、记录不通过理由，并告知申请人原因、返还申请资料；如果审核合格，则在 RA 系统中标记审核通过。审核内容与证书申请类似。

CA 中心也可以提供 Web 服务，允许用户通过互联网进行证书作废申请，录入相关信息后，携带资料到现场进行业务办理。

3. 收费

CA 中心收费员负责费用收取。按计费规定收取费用后，给申请人出具收费票据，并在 RA 系统中记录收费情况。

CA 中心也可以提供 Web 服务，允许用户通过网上支付方式付费。

4. 生效

审核通过并按要求交费后，CA 中心将及时把该证书状态修改为作废，并通过 CRL 定期发布出去。通过 OCSP 可以实时查询到该证书状态已经处于作废状态。

25.2.2.2 证书冻结与证书解冻

证书冻结、证书解冻业务流程与证书作废流程基本相同，这里不再赘述。

25.2.3 证书查询类

25.2.3.1 证书查询

主要用于查询并下载 CA 证书（链）和用户证书，通常采用 HTTP 或 LDAP 方式。

1. HTTP 方式

由于 CA 证书（链）数量很少，通常以文件形式存在，通过 Web 方式就可以直接下载，无需查询。图 25-15 给出了 HTTP 方式下 CA 证书（链）的查询下载界面示例图。

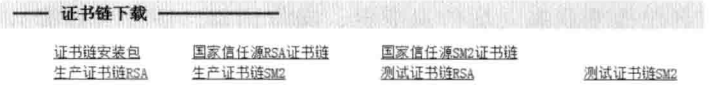

图 25-15 HTTP 方式下 CA 证书（链）的查询下载界面示例

由于用户证书数量很多，通常保存在数据库中，需要通过 Web 方式查询后才能下载。图 25-16 给出了 HTTP 方式用户证书的查询下载界面示例图。

图 25-16　HTTP 方式下用户证书的查询下载界面示例

2．LDAP 方式

LDAP 方式下，CA 证书（链）和用户证书的存储方式相同，均以条目形式存在。需要采用专用的 LDAP 软件工具或 API 方式，才能对证书进行查询和下载。图 25-17 给出了 Foxmail 6.5 中使用 LDAP 方式进行证书查询的界面示例。

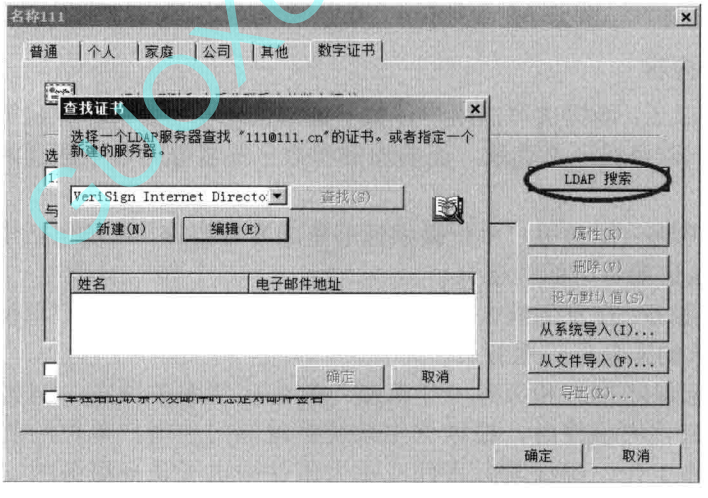

图 25-17　Foxmail 6.5 中 LDAP 证书查询界面

25.2.3.2　证书状态查询

证书状态查询主要采用 OCSP、CRL 等方式。

OCSP 方式下，需要专用的 OCSP 查询工具或 API 方式才能进行证书状态查询。

CRL 方式下，可通过 HTTP 或 LDAP 方式获得。采用 HTTP 方式时，CRL 以文件形式存在，通过 Web 方式就可以直接下载，无需查询。采用 LDAP 方式时，CRL 以条目形式存在，需要采用专用的 LDAP 软件工具或 API 方式，才能对 CRL 进行查询和下载。

25.3 客户服务

鉴于数字证书领域的专业性，在用户使用数字证书过程中可能会涉及多种多样的业务问题和技术问题，需要配置专门的坐席并基于知识库对用户提供全方位客户服务。客户服务与发证点和用户之间的关系如图 25-18 所示。

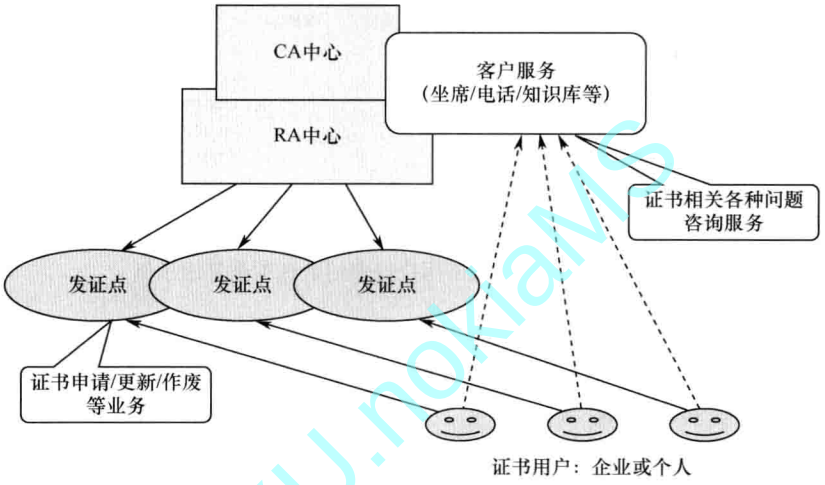

图 25-18 客户服务与发证点和用户之间的关系

1. 客户服务内容

① 使用帮助服务：能提供解决用户在数字证书的申请、更新和解锁等环节中遇到的各类业务办理问题，以及在证书登录、证书加密和数字签名等环节中遇到的各类证书应用问题的帮助服务。

② 咨询培训服务：能对用户单位提供证书集成方案咨询，以及包括电子认证服务相关政策法规、技术认证服务方面的培训。

③ 应急保障服务：在发生重大事件或特殊应急事件时，根据用户单位的要求而临时提供的超越常规要求的应急保障服务。

应该建立应急保障措施和应急工作机制，制定应急服务预案。例如，在卫生信息系统出现紧急事件或重大事件时，根据卫生系统管理部门和用户单位的要求，及时提供现场方式的应急保障工作，确保紧急事件或重大事件中电子认证服务的安全性、可靠性和有效性。

④ 应用集成支持服务：能提供针对各行业信息系统的电子认证安全需求分析、电子认证法律法规、技术体系的咨询，设计满足业务要求的电子认证及电子签名服务方案；应提供面向多种应用环境的证书应用接口程序供应用系统集成和调用。

2. 客户服务分级

客户服务应该分级管理，通常可分为 3 级：

① 紧急服务：直接影响应用系统关键任务运行，并导致业务工作停顿的故障所需要的维修服务。

② 常规服务：系统自身发生故障，影响到安全系统正常运行，但对业务系统影响较小，所需要的维修服务。

③ 计划服务：定期检修服务。

不同客户服务级别，所要求的服务时间、响应时间、解决时限等也不同。表25-4给出了一个实例。

表25-4 客户服务级别要求实例

服务级别	服务时间	响应时间	解决时限	需求程度
紧急服务	7×24小时	2小时	24小时	非常关键、紧急
常规服务	工作日	4小时	1～3个工作日	重要但不紧急
计划服务	工作日	一周	1～7个工作日	重要但可延缓数日

第26章 资质申请

26.1 电子认证服务使用密码许可证

26.1.1 政策法规要点

1.《电子签名法》（2004年版）

《电子签名法》（2004年版）规定：

第十六条 电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。

第十七条 提供电子认证服务，应当具备下列条件：

（一）具有与提供电子认证服务相适应的专业技术人员和管理人员；

（二）具有与提供电子认证服务相适应的资金和经营场所；

（三）具有符合国家安全标准的技术和设备；

（四）具有国家密码管理机构同意使用密码的证明文件；

（五）法律、行政法规规定的其他条件。

2.《电子认证服务密码管理办法》（2009年版）

《电子认证服务密码管理办法》（2009年版，国家密码管理局公告第17号）规定：

第二条 国家密码管理局对电子认证服务提供者使用密码的行为实施监督管理。

省、自治区、直辖市密码管理机构依据本办法承担有关监督管理工作。

第三条 提供电子认证服务，应当依据本办法申请《电子认证服务使用密码许可证》。

第四条 采用密码技术为社会公众提供第三方电子认证服务的系统（以下称电子认证服务系统）使用商用密码。

电子认证服务系统应当由具有商用密码产品生产资质的单位承建。

第七条 申请《电子认证服务使用密码许可证》应当在电子认证服务系统建设完成后，向所在地的省、自治区、直辖市密码管理机构提交下列材料：

（一）《电子认证服务使用密码许可证申请表》；

（二）企业法人营业执照或者企业名称预先核准通知书的复印件；

（三）电子认证服务系统安全性审查相关技术材料，包括建设工作总结报告、技术工作总结报告、安全性设计报告、安全管理策略和规范报告、用户手册和测试说明；

（四）电子认证服务系统互联互通测试相关技术材料；

（五）电子认证服务系统物理环境符合电磁屏蔽、消防安全有关要求的证明文件；

（六）电子认证服务系统使用的信息安全产品符合有关法律规定的证明文件。