相关实体的要求，注册机构、订户或其他参与者的要求，在每个子项中可能需要对电子认证服务机构、注册机构、订户或其他参与者予以分别考虑。

在“认证机构设施、管理和操作控制”部分，描述物理环境、操作过程和人员的安全控制。电子认证服务机构使用这些控制手段来安全地实现密钥生成、实体鉴别、证书签发、证书作废、审计和归档等功能。也可定义信息库、注册机构、订户或其他参与者的非技术安全控制。

在“认证系统技术安全控制”部分，阐述电子认证服务机构为保护其密钥和激活数据（如 PIN 码、口令字或手持密钥共享）而采取的安全措施。说明对证书库、订户和其他参与者进行的限制，以保护他们的私钥、私钥激活数据和关键安全参数。描述电子认证服务机构使用的其他技术安全控制手段，用以安全地实现密钥生成、用户鉴别、证书注册、证书作废、审计和归档等功能。技术控制包含生命周期安全控制（包括软件开发环境安全，可信的软件开发方法论）和操作安全控制。

在“证书、证书作废列表和在线证书状态协议”部分，说明证书、证书作废列表和在线证书状态协议的格式，包括描述、版本号和扩展项的使用。

在“认证机构审计和其他评估”部分，说明对电子认证服务机构进行审计或评估相关的内容，包括评估所涵盖的主题、评估频率、评估者的资质、被评估者的资质、对问题所采取的措施以及结果的公告等。

在“法律责任和其他业务条款”部分，涵盖了一般性的业务和法律问题。在业务条款中说明不同服务的费用问题，和各参与方为了保证资源维持运营，针对参与方的诉讼和审判提供支付所需承担的财务责任。法律责任条款则与通用的技术协定标题相近，涉及保密、隐私、知识产权、担保及免责等内容。

24.2 CP

根据 X.509 标准，CP（Certificate Policy，证书策略）作为一组规则，表明了证书在某特定范围内的、和/或某些具有相同安全需求的应用内的适用程度，也就是说明证书能够用于“安全需求为×××”的应用中。

一个 CA 可以支持签发多种不同等级 CP 的证书，不同等级 CP 的证书用于不同的应用，当然，CA 也可以只支持一种 CP，相当于对证书没有分级，只有一种级别。根 CA 的多个子 CA 可以分别支持不同的 CP。

CP 和 CPS 都说明了 PKI 用户（也就是依赖方）对于证书的可信赖程度，CP 给出了证书的可信赖程度、安全等级。CPS 说明，为了达到相应 CP 的安全等级有什么样的措施和要求，既包括对 CA 的要求，也包括对订户的要求。例如，对高级证书，要求订户只能在电磁辐射屏蔽的机房内使用，否则 CA 不赔偿。

CP 证书策略不包含操作细节，以保持 CP 的长期稳定不变，而操作细节随时间而变化。CP 的设计符合基础设施的思想，应用系统只看到其结果，可以不知道具体操作。CP 与密钥用途截然不同，二者没有联系。密钥用途是从密码运算的角度区分证书用途，证书策略是从安全等级的角度区分证书用途。

CP 标识了证书的安全等级，为 PKI 应用系统提供了使用上的指导和根据。在证书扩

展项中，CP 表示为 OID 的形式，不同的 CA 公司，可以定义自己的 OID，来表示不同的级别。证书的可靠程度由 CPS 保证。例如，CP 和 CPS 关系可以通过一个简单示例来说明：CP 定义的高级证书可用于 100 万人民币以下的电子交易，OID 为 1.3.6.1.4.1.21315.5.1；CPS 措施中，对于高级证书，如果出现任何问题，CA 立即无条件赔偿 200 万人民币。

在 CP 的制定上，CA 公司可以不具有自己的 CP，可以是由第三方制定的。CP 都以文档的形式表现并发布，在文档中说明了证书相关的各种情况。例如，如下 CP 设计：

CP1——使用者 DN 允许匿名/假名，512 位 RSA 密钥，CRL 更新周期 10 天。

CP2——使用者 DN 不允许匿名/加密，1024 位 RSA 密钥，CRL 更新周期 3 天。

CP3——使用者 DN 不允许匿名/加密，1024/2048 位 RSA 密钥，CRL 更新周期 1 天。

CP 设计中应该考虑以下问题：

① 安全级别覆盖范围，覆盖从“最简单基本”到“最复杂严格的”安全要求。

② 具有可扩展性，将来可能的各种应用的安全要求应该能够方便地映射到某一级别 CP。

③ 一套 CP 中的各个 CP，其安全等级应有差异，应用系统才能更好地选择合适的 CP。

④ 尽可能只体现安全级别，不体现具体的操作流程和方法（放在 CPS 中，可以随着时间变化而修改）。

24.3 RA 管理

RA（Registration Authority，注册机构）作为电子认证服务机构授权委托的下属机构，负责受理证书申请，包括提交证书申请、审核证书申请、提交作废申请、审核作废申请、提交密钥恢复申请、审核密钥恢复申请、发布审核结果、查询用户、查看用户证书信息、删除用户等功能。

对 RA 的管理应包括系统建设与运维、证书服务等方面，对于外部建设 RA，还应包括业务运营和责任及赔偿。

1. 系统建设与运维方面

必须遵循电子认证服务机构的 CPS（电子认证业务规则）中规定的管理操作要求。采用的 RA 系统（或产品）需要经过密码主管部门的评测与认证。物理环境上，确保 RA 系统位于安全的物理环境，终端电脑需具备必要的系统运行环境和安全防护措施。对运营人员进行可信雇员调查，确保其资格、背景、经历符合运营要求，并保证人员具有适当的知识、技能、素质，通过培训考核后可以进行相关业务操作。RA 系统日常运行维护上，应确保数字证书操作终端设备的稳定运行，并将日常运行情况进行记录，以备后期审查。系统备份上，需定期对系统关键数据进行备份，特别是数据库的自动备份和系统关键数据的自动备份，并具备完善的系统恢复方案，当系统发生异常时，能够快速恢复到正常业务工作状态。

2. 证书服务方面

在接受证书申请和证书更新等各类证书业务时，应严格依据和遵守电子认证服务机构的 CPS，对证书申请者的身份进行鉴证，收取相应的证书申请者鉴证材料和证书申请信息等用户资料，保证证书申请者的身份信息真实、完整和准确，不得在用户资料缺失的情况下随意受理证书业务。在受理点存放的证书用户申请资料和证书生产、服务、管理所需的所有原材

料，应使用独立的安全设备存放，确保防潮、防盗、防火等各项安全措施落实到位。在证书申请发放上，RA 向 CA 中心提交证书请求之前，需确认证书申请者的身份已得到鉴证并与证书申请信息相符，确认申请者已认同由电子认证服务机构制定或认可的订户协议，确认在证书申请过程中已遵循电子认证服务机构对物理环境、人员和信息安全等要求并遵循所有适用的法律。RA 系统需对系统中的各种操作以日志的形式记载，以方便系统错误分析、风险分析、安全审计等工作。记录日志包括系统运行日志、业务运行日志、操作员操作日志等。

3. 外部建设方面

对于外部建设 RA（即由独立第三方机构管理运维），除了系统建设与运维、证书服务要求外，还包括业务运营和责任及赔偿规范。在业务运营方面，需要规范“证书产品交付及结算，数字证书对账，数字证书结算”等方面。在责任及赔偿方面，涉及“鉴证责任，业务审查责任，赔偿范围，赔偿限额”等。外部建设 RA 需要遵循电子认证服务机构的 CPS 开展业务。

针对人员控制，某 CA 中心（简称 XXCA）CPS 定义如下：

5.3 人员控制

5.3.1 资格、经历和无过失要求

所有的员工与 XXCA 签定保密协议。对于充当可信角色或其他重要角色的人员，必须具备一定的资格，具体要求在人事管理制度中规定。XXCA 要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响 CA 运行的其他兼职工作、无同行业重大错误记录、无违法记录等。

5.3.2 背景审查程序

XXCA 与有关的政府部门和调查机构合作，完成对 XXCA 可信任员工的背景调查。

所有目前的可信任员工和申请调入的可信任员工都必须书面同意对其进行背景调查。

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历、职业推荐、教育、社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录、社会关系和社会安全方面的调查。

调查程序包括：

a）人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

b）人事部门通过电话、信函、网络、走访等形式对其提供的材料的真实性进行鉴定。

c）用人部门通过现场考核、日常观察、情景考验等方式对其考察。

d）经考核，人事部门和用人部门联合填写《可信雇员调查表》，报主管领导批准后准予上岗。

5.3.3 培训要求

XXCA 对运营人员按照其岗位和角色安排不同的培训。培训有：系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 中心的运行管理、CA 中心的内部管理、政策和规定及系统备份与恢复等。

对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 XXCA 组织培训。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 XXCA 组织的培训一次。

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

5.3.5 工作轮换周期和顺序

对于可替换角色，XXCA 将根据业务的安排进行工作轮换。轮换的周期和顺序视业务的具体情况而定。

5.3.6 对未授权行为的处罚

当 XXCA 员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用 XXCA 系统或进行越权操作，

XXCA 得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。情节严重的，依法对其追究相应责任。

5.3.7 独立合约人的要求

对不属于 XXCA 内部的工作人员，但从事 XXCA 有关业务的人员等独立签约者（如注册机构的工作人员），XXCA 的统一要求如下：

a）人员档案进行备案管理；

b）具有相关业务的工作经验；

c）必须接受 XXCA 组织的为期一周的岗前培训。

5.3.8 提供给员工的文档

为使系统正常运行，必须提供给具有权限的相关人员各种文档，包括：

a）加密机用户手册；

b）机房设备管理办法；

c）密码信封打印工具用户手册；

d）数字证书运营规范；

e）灾难备份和恢复方案；

f）目录服务器安装配置手册。

第25章 业务管理

25.1 管理模式

25.1.1 总体框架

1. 业务管理模式总体框架

CA 中心作为第三方电子认证服务机构，是独立的法人企业，将为多个行业的多种应用提供服务，具有很强的通用性和独立性，证书规模至少在几十万以上，投资规模也比较大。CA 中心不仅要满足上级主管部门的监管要求，而且需要通过市场化经营实现自身的生存和发展，具有以下特点：

① 需要快速适应市场需求，提供多种产品服务。CA 中心提供的产品就是数字证书，不同用户或行业领域对证书产品的具体要求可能不同，如证书中内容、有效期、密码算法等。不同用户或行业领域提供的产品可能完全独立，不允许互用，如税务领域证书可能不允许用于社保领域。相同用户或行业领域可能包含多种证书产品。

② 应方便计费收费管理。CA 中心计费类型应包括介质费、证书服务费等。应支持多种收费方式，如现场缴费、远程汇款、网上支付等。还应支持优惠促销活动。

③ 应满足主管部门的监管要求。应保存好相关记录，包括业务纸质档案、证书记录、业务申请记录等，且方便查询。

④ 需要为客户提供方便服务。应支持灵活且安全的发证点管理，不同发证点可授权办理不同类型业务。应支持发证点的调整或合并。

CA 中心业务管理模式总体框架如图 25-1 所示。

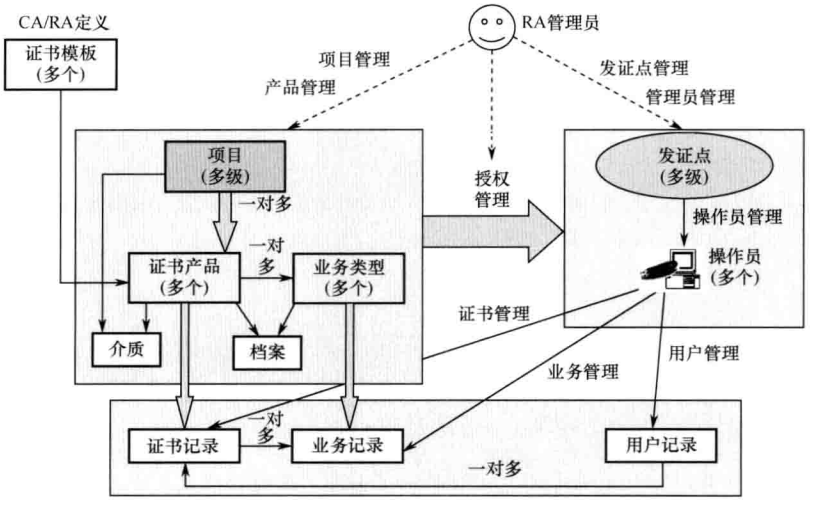

图 25-1 CA 中心业务管理模式总体框架