④ 管理员的账号要和普通用户账号严格分类管理。

4. 证书管理安全

证书的管理安全应满足下列要求：

① 验证证书申请者的身份。

② 防止非法签发和越权签发证书，通过审批的证书申请必须提交给CA，由CA签发与申请者身份相符的证书。

③ 保证证书管理的可审计性，对于证书的任何处理都需要做日志记录。通过对日志文件的分析，可以对证书事件进行审计和跟踪。

5. 安全审计

CA 系统在运行过程中涉及大量功能模块之间的相互调用，以及各种管理员的操作，对这些调用和操作需要以日志的形式进行记载，以便用于系统错误分析、风险分析和安全审计等工作。

（1）功能模块调用日志

系统内的各功能模块在运行过程中会调用其他功能模块或被其他功能模块所调用，对于这些相互之间的功能调用，各模块应该记录如下数据：

① 调用请求的接收时间。

② 调用请求来自的网络地址。

③ 调用请求发起者的身份。

④ 调用请求的内容。

⑤ 调用请求的处理过程。

⑥ 处理结果等。

（2）CA 系统管理员审计

CA 系统管理员的下列操作应被记录：

① 根 CA 证书加载。

② CA 证书加载。

③ 证书作废列表加载。

④ 证书作废列表更新等。

⑤ 系统配置。

⑥ 权限分配。

（3）CA 业务操作员审计

CA 业务操作员的下列操作应被记录：

① 证书请求批准。

② 证书请求拒绝。

③ 证书请求分配。

④ 证书作废。

（4）RA 业务操作员审计

RA 业务操作员的下列操作应被记录：

① 证书请求批准。

② 证书请求拒绝。
③ 证书请求分配。
④ 证书作废。

23.3 数据备份

数据备份的目的是确保 CA 与 KMC 的关键业务数据在发生灾难性破坏时，系统能够及时和尽可能完整地恢复被破坏的数据。应选择适当的存储备份系统对重要数据进行实时备份、定期备份、增量备份、归档检索与恢复。

不同的应用环境可以有不同的备份方案，但应满足以下基本要求：

① 备份要在不中断数据库使用的前提下实施。
② 备份方案应符合国家有关信息数据备份的标准要求。
③ 备份方案应提供人工和自动备份功能。
④ 备份方案应提供实时和定期备份功能。
⑤ 备份方案应提供增量备份功能。
⑥ 备份方案应提供日志记录功能。

23.4 系统可靠性

CA 与 KMC 必须提供 7×24 小时服务，对影响系统可靠性的主要因素（如网络故障、主机故障、数据库故障和电源故障等）需要采取冗余配置等措施。

1. 网络链路冗余

为保证 CA 的服务，CA 网络对外接口应根据具体情况，可有两条物理上独立的链路，同时考虑交换机、路由器、防火墙的冗余配置。

2. 主机冗余

CA 系统中与关键业务相关的主机、在服务网段和核心网段中的服务器应采用双机热备份或双机备份措施。

3. 数据库冗余

CA 系统的数据库应采用磁盘阵列、磁盘镜像等措施，具备容错和备份能力。

4. 电源冗余

CA 系统应采用高可靠的电源解决方案，并应采用 UPS 为系统提供不间断电源。

23.5 物理安全

1. 物理环境建设

CA 的建筑物及机房建设应按照国家密码管理相关政策要求，并遵照下列标准实施：

① GB 9361—88：《计算站场地安全要求》。

② GB 2887—89：《计算站场地技术条件》。

③ GB 6650—86：《计算机机房用活动地板技术条件》。

④ GB 50174—93：《电子计算机机房设计规范》。

2. 对CA的分层访问

CA系统按功能分为4个区域，由外到里分别是：公共区、服务区、管理区和核心区。

（1）公共区

入口之外的区域为公共区。

（2）服务区

所有进入此区的人员使用身份识别卡刷卡进入。该区的每扇窗户都应安装玻璃破碎报警器。

（3）管理区

所有进入此区的人员需要同时使用身份识别卡和人体特征鉴别才可以进入，人员进出管理区要有日志记录。所有的房间不应安装窗户，所有的墙体应采用高强度防护墙。

（4）核心区

所有进入此区的人员需要同时使用身份识别卡和人体特征鉴别才可以进入，人员进出该区要有日志记录。

核心区应为屏蔽机房，应加装高强度的钢制防盗门。所有进出屏蔽室的线路都要采取防电磁泄漏措施。屏蔽效果应符合国家密码管理相关政策要求并达到国家相关标准要求。

（5）安全监控和配电消防

CA应设置安全监控室、系统监控室、配电室和消防器材室。

安全监控室是安全管理人员值班的地方，可对整个CA的进出人员实行监控，处理日常的安全事件。只有安全管理人员同时使用身份识别卡和人体特征鉴别才可以进入，刷卡离开。

系统监控室是网络管理人员工作的地方，需要同时使用身份识别卡和人体特征鉴别才可以进入，刷卡离开。

配电室是放置所有供电设备的房间，只有相应的授权人员同时使用身份识别卡和人体特征鉴别才可以进入，刷卡离开。

消防器材室是存放消防设备的房间，建议使用身份识别卡进入消防器材室。

3. 门禁和物理侵入报警系统

CA应设置门禁和物理侵入报警系统。

门禁系统控制各层门的进出。工作人员都需使用身份识别卡或结合人体特征鉴别才能进出，并且进出每一道门都应有时间记录和相关信息提示。

任何非法闯入、非正常手段的开门以及授权人刷卡离开后房内还有非授权的滞留人员，都应触发报警系统。报警系统应明确地指出报警部位。

门禁和物理侵入报警系统应自备有UPS，并应提供至少8小时的供电。

与门禁和物理侵入报警系统配合使用的还应有录像监控系统。对监控区域进行24小时不间断的录像。所有的录像资料要根据需要保留一段时间，以备查询。

23.6 人事管理制度

人事管理制度包括人员的可信度鉴别、岗位设置等。

CA 应制定可信人员策略并据此进行人员的可信度鉴别和聘用。可信人员必须接受并通过广泛的背景调查，才能证明他们有能力进行相应关键操作所必需的信任级别。

CA 对人员的教育水平、从业经历、信用情况等方面进行调查，以评估人员的可信度。进行可信人员背景调查必须遵循国家的有关法律、法规和政策。

第24章 运营文件

24.1 CPS

CPS（Certification Practice Statement，电子认证业务规则）是电子认证服务机构对所提供的认证及相关业务的全面描述。

按照《中华人民共和国电子签名法》第十九条："电子认证服务提供者应当制定、公布符合国家有关规定的电子认证业务规则，并向国务院信息产业主管部门备案。电子认证业务规则应当包括责任范围、作业操作规范、信息安全保障措施等事项。"法律规定，CA必须制定完整的认证业务规则，才能够提供合法的认证业务。缺少CP/CPS的CA，就不是合法的CA。

CP/CPS应以文档的形式发布，在文档中说明证书相关的各种情况，而且要对PKI的依赖方、订户完全公开，使依赖方和订户能够更安全、更有效地使用PKI的服务。

CPS说明了CA/PKI系统的方方面面的信息，即相应CP证书的产生、维护、赔偿、法律责任等信息，让使用者（PKI应用系统）愿意接受其CP，并将其用于合适的场合。

依据工业和信息化部《电子认证业务规则规范（试行）》办法，电子认证业务规则包括责任范围、作业操作规范和信息安全保障措施等内容，主要由以下几部分组成。

① 概括性描述。
② 信息发布与信息管理。
③ 身份标识与鉴别。
④ 证书生命周期操作要求。
⑤ 认证机构设施、管理和操作控制。
⑥ 认证系统技术安全控制。
⑦ 证书、证书作废列表和在线证书状态协议。
⑧ 认证机构审计和其他评估。
⑨ 法律责任和其他业务条款。

在"概括性描述"部分，对电子认证业务规则进行概要性表述，给出文档的名称和标识，指出电子认证活动的参与者及证书应用范围，并说明对电子认证业务规则的管理，最后给出电子认证业务规则中使用的定义和缩写。

在"信息发布与信息管理"部分，描述任何与认证信息发布相关的内容，包括信息库的运营者、运营者的职责、信息发布的频率以及对所发布信息的访问控制等。

在"身份标识与鉴别"部分，描述电子认证服务机构在颁发证书之前，对证书申请者的身份和其他属性进行鉴别的过程，以及标识和鉴别密钥更新请求者和作废请求者的方法。说明命名规则，包括在某些名称中对商标权的承认问题。

在"证书生命周期操作要求"部分，说明在证书生命周期方面对电子认证服务机构及