第23章 机房建设

《证书认证系统密码及其相关安全技术规范》规定了证书认证中心和密钥管理中心建设的基本要求。

23.1 业务系统

业务系统主要包括 CA 系统和 KMC 系统。CA 系统部署在证书认证中心，KMC 系统部署在密钥管理中心。

23.1.1 证书认证中心

1. 功能要求

CA 系统提供的服务功能主要有：

① 提供各种证书在其生命周期中的管理服务。

② 提供 RA 的多种建设方式，RA 可以全部托管在 CA 系统；也可以部分托管在 CA，部分建在远端。

③ 提供人工审核或自动审核两种审核模式。

④ 支持多级 CA 认证。

⑤ 提供证书查询、证书状态查询、证书作废列表下载、目录服务等功能。

2. 性能要求

CA 系统的性能应满足如下要求：

① 系统对用户接口采用标准的 HTTP、HTTPS 和 LDAP 协议，确保各种用户都能够使用本系统服务。

② 系统各模块的状态信息保存在配置文件和数据库内部，保证系统的部署方便性和配置方便性，当系统需改变配置时无须中断系统的服务。

③ 各模块的功能可以通过配置文件进行控制，系统可以根据不同的需求进行设置。

④ 系统某一功能模块可有多个实例，并且多个实例可运行在一台或多台计算机上。

⑤ 系统应有冗余设计，保证系统的不间断运行。

3. 管理员配置要求

CA 应设置下列管理和操作人员：超级管理员、审计管理员、业务管理员、业务操作员。其中，“超级管理员”负责 CA 系统的策略设置，设置各子系统的业务管理员并对其管理的业务范围进行授权。“业务管理员”负责 CA 系统的某个子系统的业务管理，设置本子系统的业务操作员并对其操作的权限进行授权。“业务操作员”按其权限进行具体的业务操作。“审计管理员”负责对涉及系统安全的事件和各类管理和操作人员的行为进行

审计和监督。

上述各类人员使用证书进行登录，其中“超级管理员”和“审计管理员”的证书应在 CA 系统进行初始化时同时产生。

另外，CA 应设置安全管理员，全面负责系统的安全工作。

4．网络划分

CA 系统的计算机网络需要合理分段，原则上要求整个网络划分为 4 部分。

① 公共部分（区）：CA 用户所在的网络，所有用户将通过该网络访问 CA。

② 服务部分（区）：为外部用户提供域名解析功能，并负责内部系统对外邮件的收发功能。包括系统的各种 Web 服务器和从目录服务器，是外部用户访问内部功能的接口，为用户提供访问界面。

③ 管理部分（区）：仅供 CA 的工作人员使用的网络。

④ 核心部分（区）：包括各种核心应用、数据库和密码设备等在内的实现系统功能的安全网络。

当 RA 采用客户机/服务器（C/S）模式时，应该按照上述方式划分网络，如图 23-1 所示。

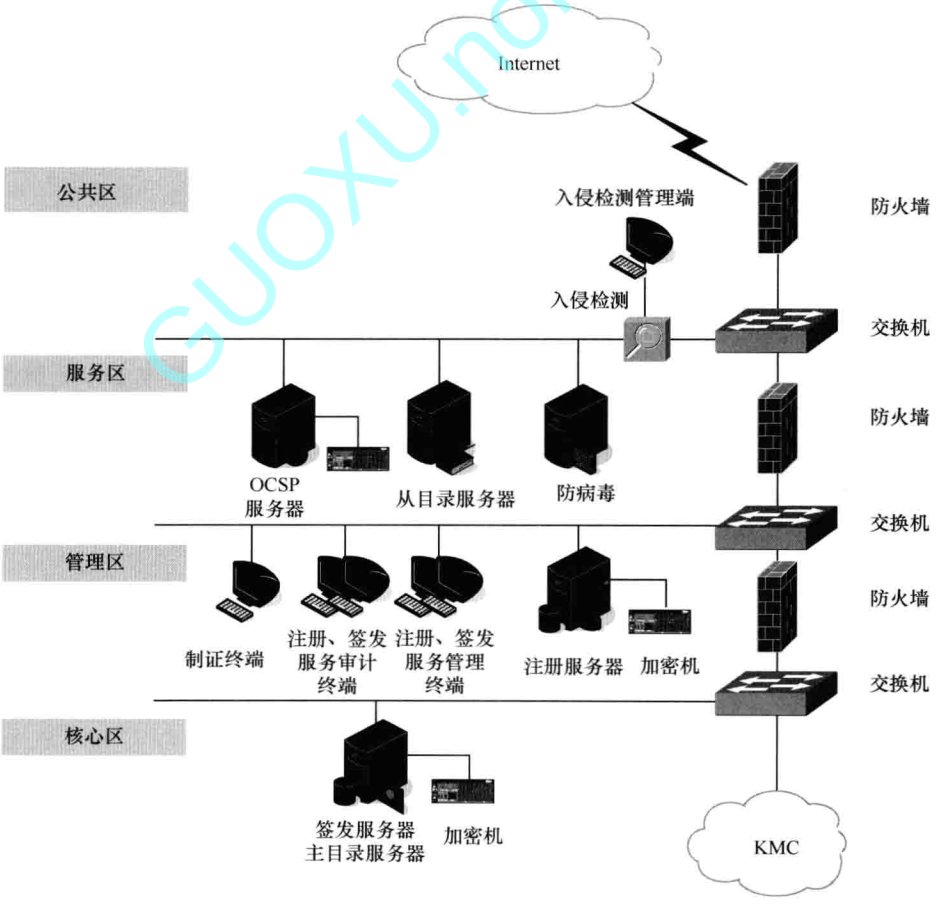

图 23-1　RA 采用 C/S 模式时 CA 的网络结构示意图

当 RA 采取浏览器/服务器（B/S）模式时，可将服务区与管理区网络放在同一网段，如图 23-2 所示。

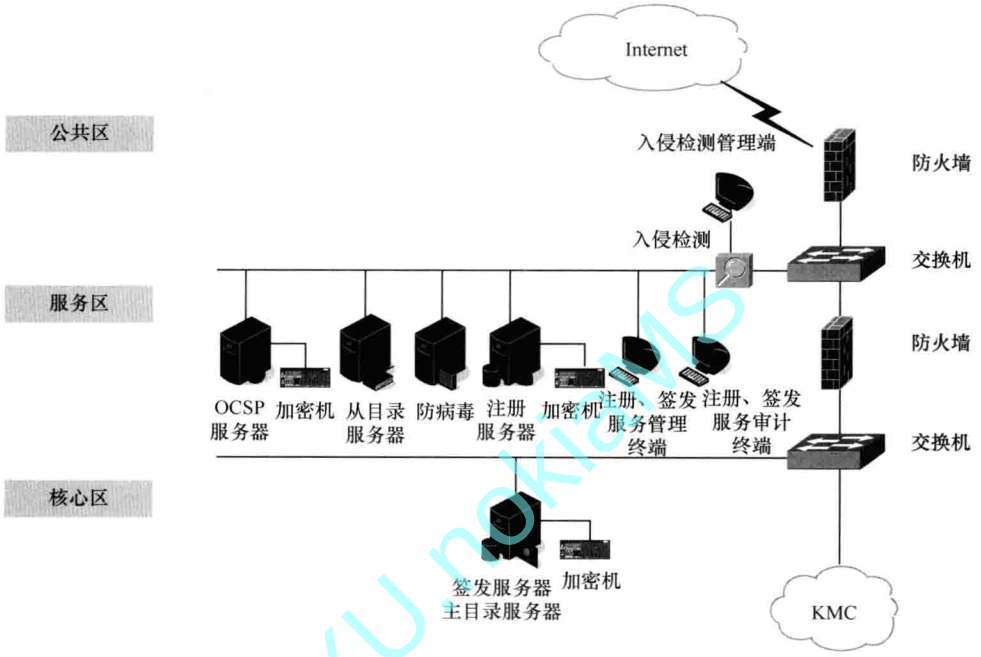

图 23-2　RA 采用 B/S 模式时 CA 的网络结构示意图

5. 初始化要求

CA 的初始化过程必须完成下列工作：

① 产生本 CA 的机构密钥并进行安全备份。

② 若本 CA 为根 CA，则使用根 CA 的签名密钥进行自签名；若本 CA 从属于某一根 CA，则将产生的签名公钥提交根 CA 签发本 CA 的证书。

③ 由 CA 签发 CA 服务器证书。

④ 由 CA 签发 RA 服务器证书（可选）。

⑤ 由 CA 签发超级管理员和审计管理员证书。

⑥ 由 CA 签发其他管理员和操作员证书。

23.1.2　密钥管理中心

密钥管理中心的工程建设按照与 CA 统一规划、有机结合、独立设置、分别管理的原则进行。

1. 功能要求

密钥管理中心应提供下列服务功能：

① 为 CA 提供密钥生成服务；

② 为司法机关提供密钥恢复服务；

③ 为用户提供密钥更新、密钥恢复、密钥作废服务。

2. 性能要求

密钥管理中心的性能应满足如下要求：

① 密钥的保存期应大于10年。

② 系统应支持多并发服务请求。

③ 系统各模块的状态信息保存在配置文件和数据库内部，保证系统的部署方便性和配置方便性，当系统需改变配置时无须中断系统的服务。

④ 各模块的功能可以通过配置文件进行控制，系统可以根据不同的需求进行设置。

⑤ 系统应有冗余设计，保证系统的不间断运行。

3. 管理员配置要求

KMC应设置下列管理和操作人员：超级管理员、审计管理员、业务管理员、业务操作员。其中，“超级管理员”负责KMC系统的策略设置，设置各子系统的业务管理员并对其管理的业务范围进行授权。“业务管理员”负责KMC系统的某个子系统的业务管理，设置本子系统的业务操作员并对其操作的权限进行授权。“业务操作员”按其权限进行具体的业务操作。“审计管理员”负责对涉及系统安全的事件和各类管理与操作人员的行为进行审计和监督。

上述各类人员使用证书进行登录，其中“超级管理员”和“审计管理员”的证书应在KMC系统进行初始化时同时产生。

另外，KMC应设置安全管理员，全面负责系统的安全工作。

4. 初始化要求

KMC的初始化过程必须完成下列工作：

① 生成KMC的机构密钥并进行安全备份。

② 由授权的CA签发KMC服务器证书。

③ 由授权的CA签发超级管理员和审计管理员证书。

④ 由授权的CA签发业务管理员和业务操作员证书。

23.2 应用安全

CA与KMC系统的应用安全包括系统安全、通信安全、密钥安全、证书管理安全、安全审计等各方面的安全。

1. 系统安全

系统安全的主要目标是保障网络、主机系统、应用系统及数据库运行的安全，应采取防火墙、病毒防治、漏洞扫描、入侵监测、数据备份、灾难恢复等安全防护措施。

2. 通信安全

通信安全的主要目标是保障CA系统各子系统之间、CA与KMC之间、CA与RA之间的安全通信，应采取通信加密、安全通信协议等安全措施。

3. 密钥安全

密钥安全的主要目标是保障 CA 系统中所使用的密钥，在其生成、存储、使用、更新、废除、归档、销毁、备份和恢复等整个生命周期中的安全，应采取硬件密码设备、密钥管理安全协议、密钥存取访问控制、密钥管理操作审计等多种安全措施。

（1）基本要求

密钥安全的基本要求是：

① 密钥的生成和使用必须在硬件密码设备中完成。

② 密钥的生成和使用必须有安全可靠的管理机制。

③ 存在于硬件密码设备之外的所有密钥必须加密。

④ 密钥必须有安全可靠的备份恢复机制。

⑤ 对密码设备操作必须由多个操作员实施。

（2）根 CA 密钥

根 CA 密钥的安全性除了满足基本要求外，还应满足下列要求：

① 根 CA 密钥的产生。

CA 系统的根密钥由硬件密码设备生成并存放在该密码设备中，应采用密钥分割或秘密共享机制进行备份。保存分割后的根密钥的人员称为分管者。

生成根 CA 密钥时，应先选定分管者，数量可以限定为 3 个或 5 个。选定的分管者应分别用自己输入的口令保护分管的密钥，分管的密钥应存放在智能 IC 卡或智能密码钥匙中。智能 IC 卡或智能密码钥匙也应备份，并安全存放。

根 CA 密钥的产生过程必须进行记录。

② 根 CA 密钥的恢复。

恢复根 CA 密钥时，要有满足根 CA 密钥恢复所必需的分管者人数。各个分管者输入各自的口令和分管的密钥成分在密码设备中恢复。

③ 根 CA 密钥的更新。

更新根 CA 密钥时，需重新生成根 CA 密钥，其过程同根 CA 密钥的产生。

④ 根 CA 密钥的废除。

根 CA 密钥的废除应与根 CA 密钥的更新同步。

⑤ 根 CA 密钥的销毁。

根 CA 密钥应与备份的根 CA 密钥一同销毁。由密码主管部门授权的机构实施。

（3）非根 CA 密钥

非根 CA 密钥的安全性要求与根 CA 密钥的安全性要求一致。

（4）管理员证书密钥

管理员包括超级管理员、审计管理员、业务管理员和业务操作员等。管理员证书密钥应由证书载体来产生和存储。

管理员证书密钥的安全性应满足下列要求：

① 管理员证书密钥的产生和使用必须在证书载体中完成。

② 密钥的生成和使用必须有安全可靠的管理机制。

③ 管理员的口令长度为 8 个字符以上。