17.2　企业级 CA

企业级 CA 应该可以根据模块进行灵活部署，通常分为几种模式：双层标准模式、双层简化模式、单层单机模式和纯硬件模式。企业级 CA 模块组成可参考图 15-3。

17.2.1　双层标准模式

该模式是企业级 CA 的标准部署结构，将核心层模块和服务层模块分别部署在 2 个不同的安全域中，安全域之间采用防火墙和 VLAN 分隔保护。根 CA 签名模块只签发 CA 证书，为保证安全性，通过脱机方式实现。加密机通过硬件保护 CA 密钥对的安全性，保证了证书签发的安全性。

RA 受理点的管理员和操作员通过互联网访问部署在中心机房的 RA 服务器；证书用户通过互联网访问部署在中心机房的用户服务器。

CA 管理员、RA 管理员、RA 操作员、证书用户等，无需配置特殊设备，只采用普通 PC 就可以访问 CA 系统。

该模式下，网络部署结构如图 17-5 所示。

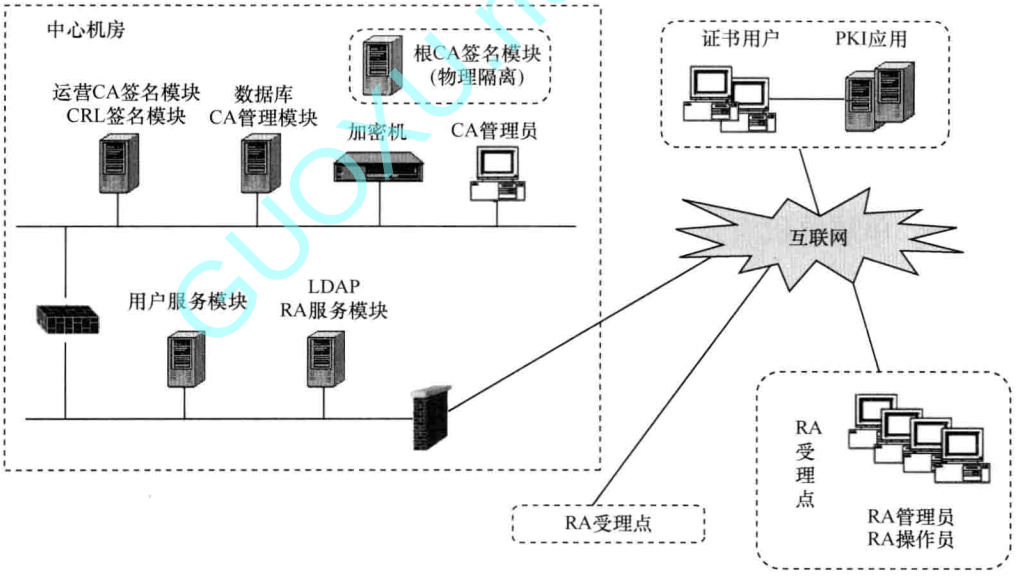

图 17-5　企业级 CA 双层标准模式网络部署结构

17.2.2　双层简化模式

该模式是企业级 CA 标准部署结构的简化模式，将核心层模块和服务层模块分别部署在 2 个不同的安全域中，安全域之间采用防火墙和 VLAN 分隔保护。根 CA 签名模块只签发 CA 证书，为保证安全性，通过脱机方式实现。加密机通过硬件保护 CA 密钥对的安全性，保证了证书签发的安全性。为降低部署硬件成本，核心层所有模块和服务层所有模块分别安装在单台硬件服务器上。

RA 受理点的管理员和操作员以及证书用户均通过互联网访问部署在中心机房的 RA/用户服务器。

CA 管理员、RA 管理员、RA 操作员、证书用户等，无需配置特殊设备，只采用普通 PC 就可以访问 CA 系统。

该模式下，网络部署结构如图 17-6 所示。

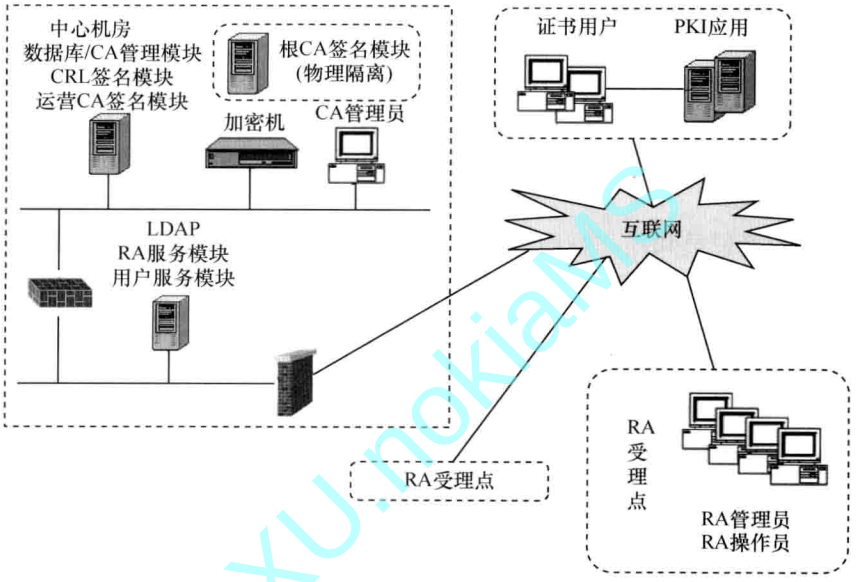

图 17-6　企业级 CA 双层简化模式网络部署结构

17.2.3　单层单机模式

该模式是企业级 CA 最简单的部署结构，为进一步降低硬件成本，不再划分安全域，将核心层和服务层所有模块均部署在同一台硬件服务器上。加密机通过硬件保护 CA 密钥对的安全性，保证了证书签发的安全性。

RA 受理点的管理员和操作员以及证书用户均通过互联网访问部署在中心机房的 RA/用户服务器。

CA 管理员、RA 管理员、RA 操作员、证书用户等，无需配置特殊设备，只采用普通 PC 就可以访问 CA 系统。

该模式下，网络部署结构如图 17-7 所示。

17.2.4　纯硬件模式

该模式属于“交钥匙”部署模式，无需用户提供任何设备，只需安装证书服务器设备即可，采用内置式加密卡保护关键密钥的安全性。核心层和服务层所有模块均部署在该证书服务器设备中。

RA 受理点的管理员和操作员以及证书用户均通过互联网访问部署在中心机房的证书服务器。

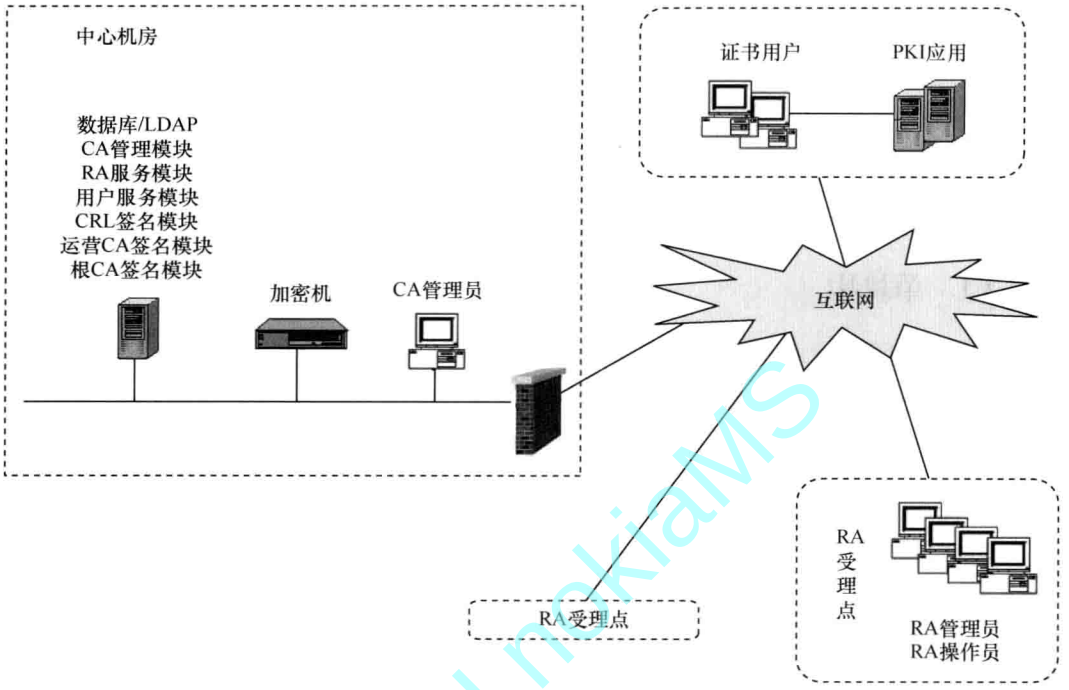

图 17-7　企业级 CA 单层单机模式网络部署结构

CA 管理员、RA 管理员、RA 操作员、证书用户等，无需配置特殊设备，只采用普通 PC 就可以访问 CA 系统。

该模式下，网络部署结构如图 17-8 所示。

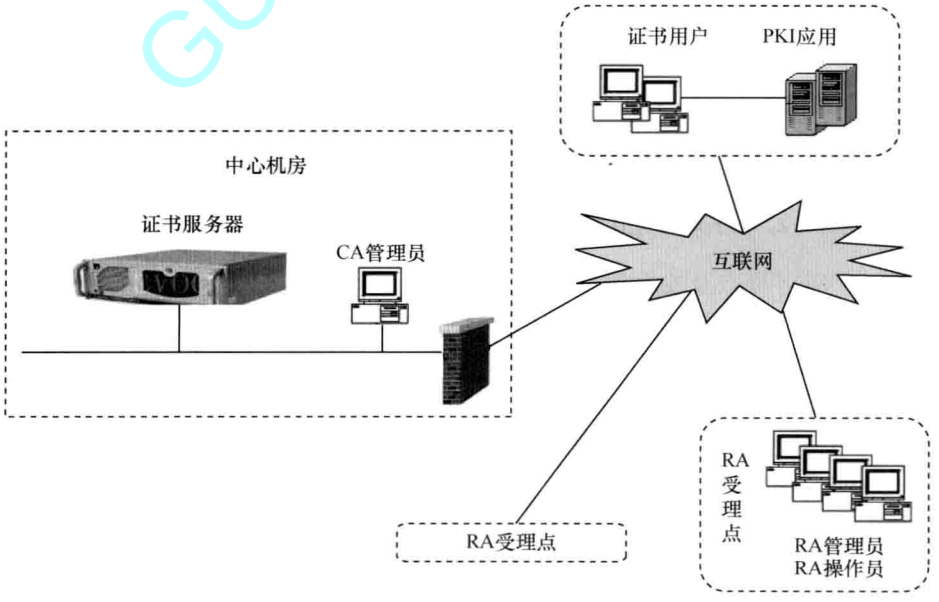

图 17-8　企业级 CA 纯硬件模式网络部署结构

17.3 按企业管理模式部署 CA

企业级 CA 应该可以根据企业管理模式进行灵活部署，通常分为几种模式：单机构、集团公司+集中部署+集中发证、集团公司+集中部署+分布发证、集团公司+两级部署+分布发证。

为了方便说明，本节将企业级 CA 所有功能模块及其网络部署结构抽象成证书服务器，具体部署结构需要根据实际需要选择 17.2 节中的合适模式。

17.3.1 单机构

该模式下，应用特点及安全需求主要包括：

① 没有独立的二级机构。

② 应用系统集中部署。

数字证书部署要点主要包括：

① 部署一套证书服务器。

② 由证书服务器为员工签发个人证书，数字证书及私钥保存在 USB Key 中。

③ 由证书服务器为应用系统签发设备/服务器证书。

④ 基于数字证书技术，保证了员工访问应用系统的安全性。

该模式下，网络部署结构如图 17-9 所示。

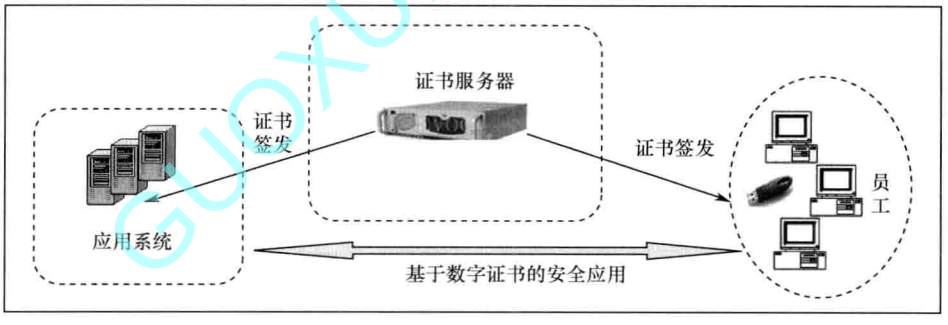

图 17-9 企业级 CA 单机构模式网络部署结构

17.3.2 集团公司+集中部署+集中发证

该模式下，应用特点及安全需求主要包括：

① 组织结构分为 2 级：集团总公司和分/子公司。

② 应用系统部分集中部署，部分分布部署。

③ 数字证书系统要求集中部署。

④ 数字证书发证业务要求集中发证。

数字证书部署要点主要包括：

① 在总公司部署一套证书服务器。

② 由证书服务器为总公司员工签发个人证书，数字证书及私钥保存在 USB Key 中。

③ 由证书服务器为总公司应用系统签发设备/服务器证书。

④ 基于数字证书技术，保证了总公司员工访问总公司应用系统的安全性。

⑤ 由证书服务器为分/子公司员工签发个人证书，数字证书及私钥保存在 USB Key 中。

⑥ 由证书服务器为分/子公司应用系统签发设备/服务器证书。

⑦ 基于数字证书技术，保证了分/子公司员工访问总公司应用系统和分/子公司应用系统的安全性。

该模式下，网络部署结构如图 17-10 所示。

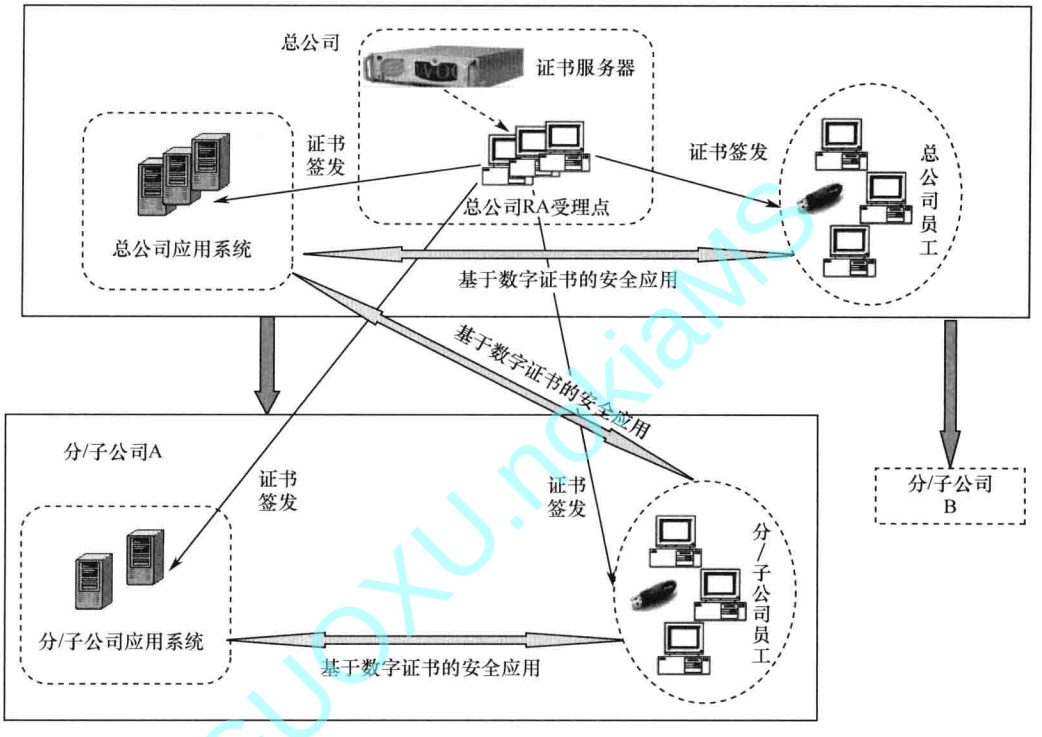

图 17-10　企业级 CA 集团模式 I 网络部署结构

17.3.3　集团公司+集中部署+分布发证

该模式下，应用特点及安全需求主要包括：

① 组织结构分为 2 级：集团总公司和分/子公司。

② 应用系统部分集中部署，部分分布部署。

③ 数字证书系统要求集中部署。

④ 数字证书发证业务要求分布发证。

数字证书部署要点主要包括：

① 在总公司部署一套证书服务器，并支持多个 RA 受理点。

② 由总公司 RA 受理点为总公司员工签发个人证书，数字证书及私钥保存在 USB Key 中。

③ 由总公司 RA 受理点为总公司应用系统签发设备/服务器证书。

④ 基于数字证书技术，保证了总公司员工访问总公司应用系统的安全性。

⑤ 由分/子公司 RA 受理点为分/子公司员工签发个人证书，数字证书及私钥保存在 USB Key 中。

⑥ 由分/子公司 RA 受理点为分/子公司应用系统签发设备/服务器证书。