③ 执行 LDAP 条目添加操作并返回执行结果。ldap_add()和 ldap_add_s()用来添加 LDAP 目录条目。

④ 关闭 LDAP Server 连接。由 ldap_unbind()调用实现。

16.3.2 访问 LDAP 获取数字证书

1. 通过软件工具访问

向对方发送安全邮件时，使用对方的数字证书对邮件内容进行加密，因此邮件发送前需要获得对方的数字证书，很多电子邮件软件已经支持通过访问 LDAP 获得数字证书。

以 Foxmail 6.5 为例，对于每个联系人，可以通过其电子邮箱从 LDAP 查询并获得其数字证书。

进入“地址簿”→“每个卡片”→“属性”→“数字证书”界面后，单击“LDAP 搜索”按钮即可进行搜索，如图 16-2 所示。

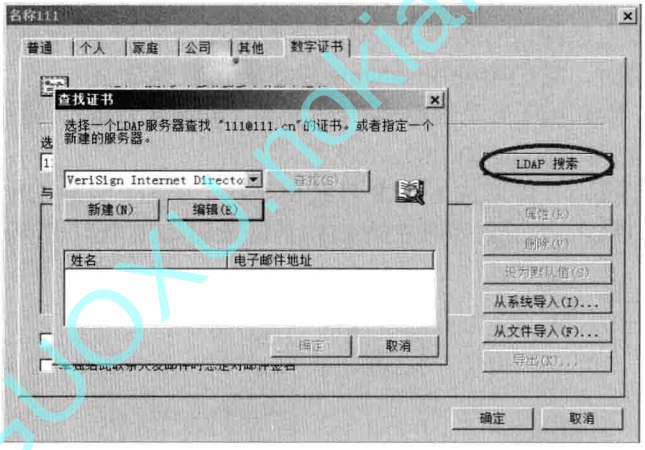

图 16-2 Foxmail 6.5 中 LDAP 搜索界面

通过“新增”或“编辑”按钮可对 LDAP 进行新增或修改，如图 16-3 所示。

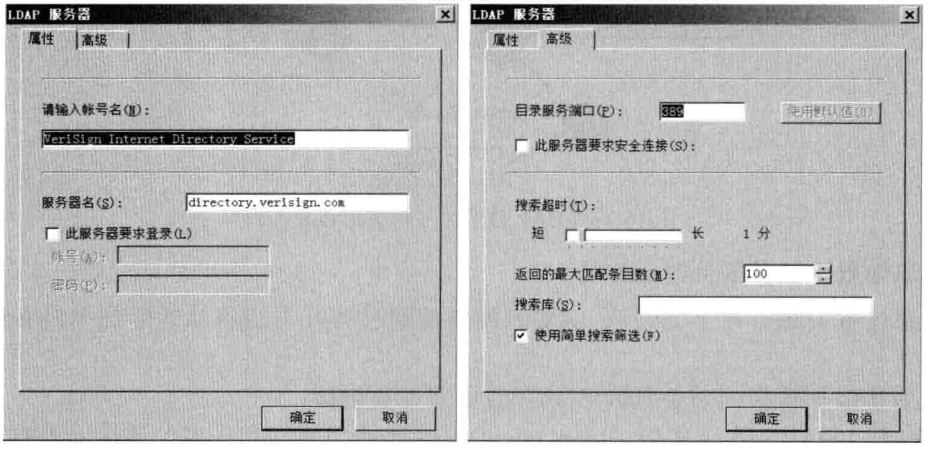

图 16-3 Foxmail 6.5 中 LDAP 设置界面

2．通过 API 方式访问

应用程序通过 API 方式访问 LDAP 需要进行以下 4 个步骤：

① 打开 LDAP Server 连接。ldap_open()返回连接句柄，允许多个连接同时打开。

② 同 LDAP Server 进行身份认证。ldap_bind()及相关函数支持多种不同的认证方法。

③ 根据条件执行 LDAP 查询操作并获得查询结果。ldap_search()及相关函数可执行 ldap 查询操作并获取结果；返回结果可以由 ldap_result2error()、ldap_first_entry()、ldap_next_entry()解析。ldap 操作支持同步或异步执行。

④ 关闭 LDAP Server 连接。由 ldap_unbind()调用实现。

第 17 章　网络部署结构

17.1　运营型 CA

根据运营型 CA 的安全要求，CA 中心需要划分不同安全级别的安全域，并将不同的模块部署在不同的安全域内。按照安全级别的高低，CA 中心的安全域主要包括：

① KM 区：部署密钥管理系统。

② 核心区：部署证书/CRL 签发系统、主 LDAP 系统、主 OCSP 系统等。

③ 管理区：部署证书管理系统。

④ 服务区：部署从 LDAP 系统、从 OCSP 系统、RA 系统等。

CA 中心网络部署结构如图 17-1 所示。

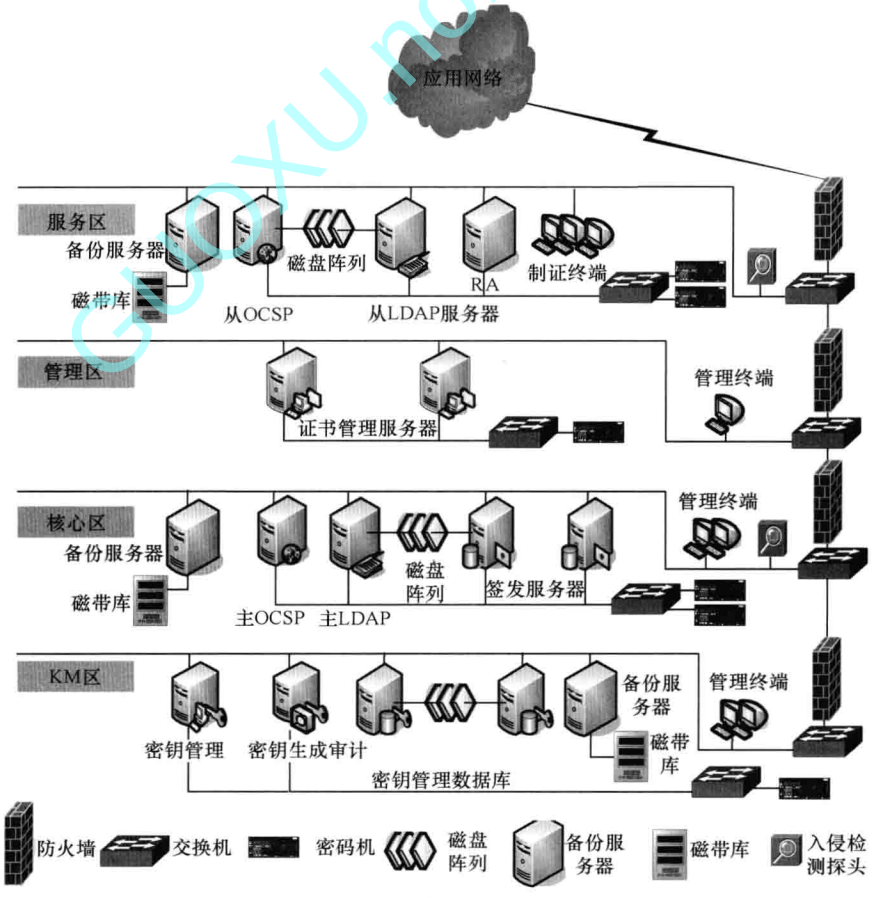

图 17-1　CA 中心网络部署结构

图中，KM 区内，密钥管理系统只接收来自核心区的证书/CRL 签发系统的服务请求。核心区内，证书/CRL 签发系统只接收来自管理区证书管理系统的请求；主 LDAP 系统和主 OCSP 系统都是单向通信，只定期将数据同步到服务区内的从 LDAP 系统和从 OCSP 系统。管理区内，证书管理系统只接收来自服务区 RA 系统的各种业务请求。服务区内，RA 系统负责面向直接用户，提供证书申请、身份审核和证书下载等业务服务。

各安全域之间通过防火墙进行边界保护，并部署 IDS、漏洞扫描、防病毒等安全系统进行网络安全和主机安全防护。

为确保业务的连续性，尽量降低或避免单点故障对运营服务的营销，可配置双网络链路、核心服务器双机热备、磁盘阵列等。为保证业务服务性能，从 LDAP 系统和从 OCSP 系统的硬件服务器性能要优于其他服务器。

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，网络部署结构可参考图 17-2。

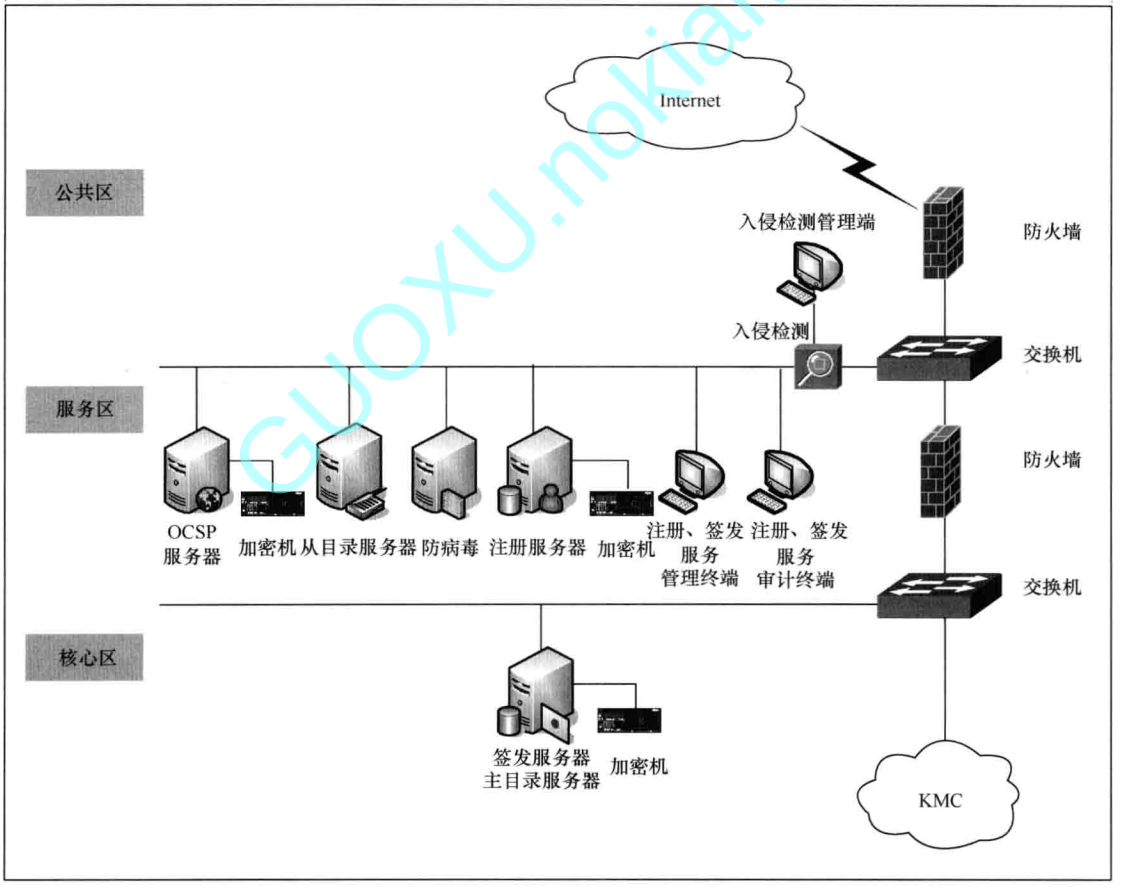

图 17-2　RA 采用 B/S 模式时 CA 的网络结构示意图

CA 与远程 RA 的连接时，网络部署结构可参考图 17-3。

KMC 与多个 CA 的网络连接时，网络部署结构可参考图 17-4。

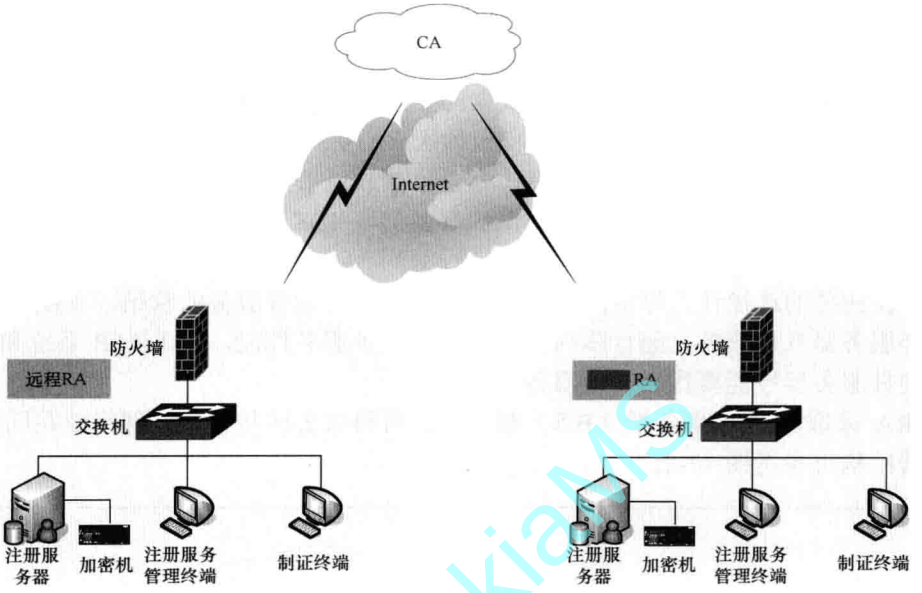

图 17-3　CA 与远程 RA 的连接示意图

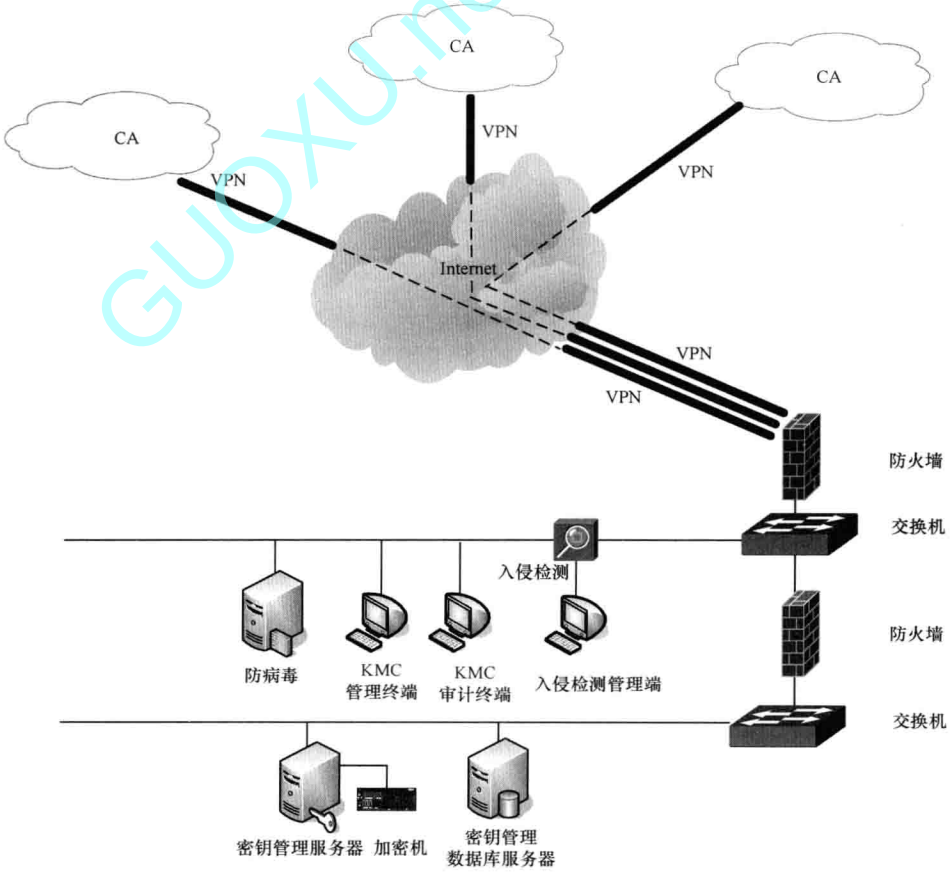

图 17-4　KMC 与多个 CA 的网络连接示意图