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 17-11 所示。

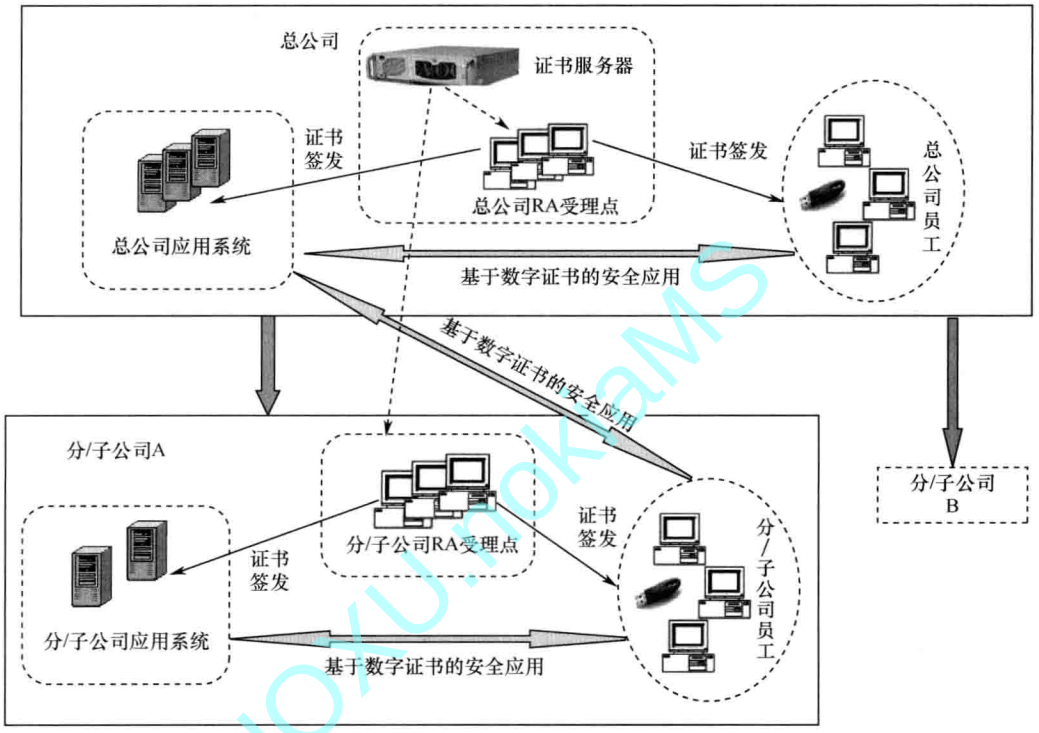

图 17-11　企业级 CA 集团模式 II 网络部署结构

17.3.4　集团公司+两级部署+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 数字证书系统要求分布部署。

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 在总公司部署一套根证书服务器。

② 在总公司部署一套证书服务器。

③ 由总公司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。

④ 由总公司证书服务器为总公司应用系统签发设备/服务器证书。

⑤ 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。

⑥ 在分/子公司部署一套证书服务器。

⑦ 由分/子公司证书服务器为分/子公司员工签发个人证书，数字证书及私钥保存在

USB Key 中。

⑧ 由分/子公司证书服务器为分/子公司应用系统签发设备/服务器证书。

⑨ 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 17-12 所示。

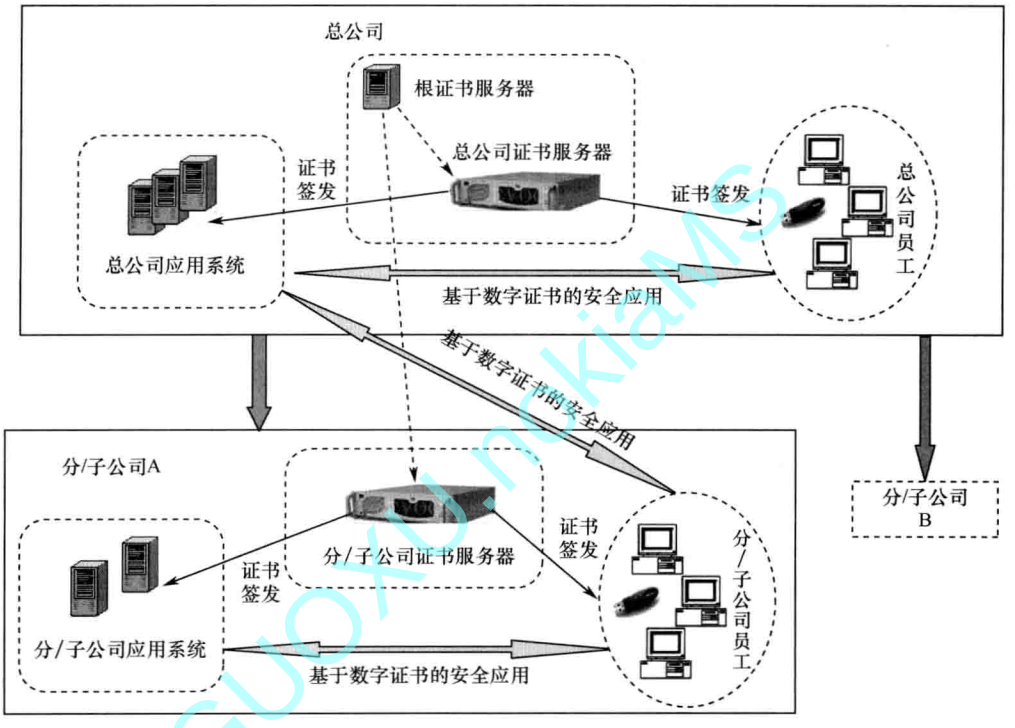

图 17-12　企业级 CA 集团模式 III 网络部署结构

第18章 实 验 三

18.1 OpenSSL CA 示例

18.1.1 简介

OpenSSL 是一个功能丰富的开源安全工具箱，它提供的主要功能有：多种软件算法（对称/非对称/摘要）、大数运算、非对称算法密钥生成、ASN.1 编解码库、时间戳、证书请求（PKCS10）编解码、数字证书/CRL 编解码、OCSP 协议、数字证书验证、PKCS7 标准实现、PKCS12 个人数字证书格式实现、SSL 协议实现（包括 SSLv2、SSLv3 和 TLSv1）等。OpenSSL 官方网址为 http://www.openssl.org。本章只涉及 OpenSSL 中的 CA 功能。

OpenSSL 采用 C 语言作为开发语言，这使得它具有优秀的跨平台性能，支持 Linux、UNIX、windows、Mac 等平台。

18.1.2 安装配置

本节以 32 位 Windows 7 操作系统环境为例进行安装配置说明，其他操作系统环境类似。从 Shining Light 网站 http://slproweb.com/products/Win32OpenSSL.html 下载编译好的安装软件包，如果读者感兴趣，可以下载源代码进行编译。在下载页面有多个版本的 OpenSSL，分别是 1.0.1g、1.0.0L、0.9.8y，每个版本号下对应 32 位和 64 位版本，根据自己的操作系统环境可以选择下载对应的版本。这里以 1.0.1g 的 32 位版本进行说明，下载链接说明如表 18-1 所示。

表 18-1 下载链接说明

文件	类型	说明
Win32 OpenSSL v1.0.1g Light	1MB 安装包	建议使用版本 OpenSSL v1.0.1g，按缺省条件编译
Visual C++ 2008 Redistributables	1.7MB 安装包	支持库，适合 Windows 2000 以后系统
Visual C++ 2008 Redistributables for Windows 9x/NT4	4.6MB 压缩包	支持 Windows 95/98/Me/NT4 操作系统

1. 安装 Visual C++ 2008 Redistributables

单击表 18-1 中的运行库“Visual C++ 2008 Redistributables”，浏览器会导航到微软网站，见图 18-1，单击“Download”进行下载。

下载完成后，双击该安装包。当出现安全警告对话框（因从网络下载，系统产生安全警告），提示“无法验证发布者，您确定要运行此软件吗？”时，单击“运行”按钮。当出现许可条款对话框时，勾选“我已阅读并接受许可条款”，单击“安装”按钮。其他安装界面按照提示选择缺省按钮即可完成安装。

安装完成后，会出现如图 18-2 所示画面，单击“完成”按钮，结束安装。

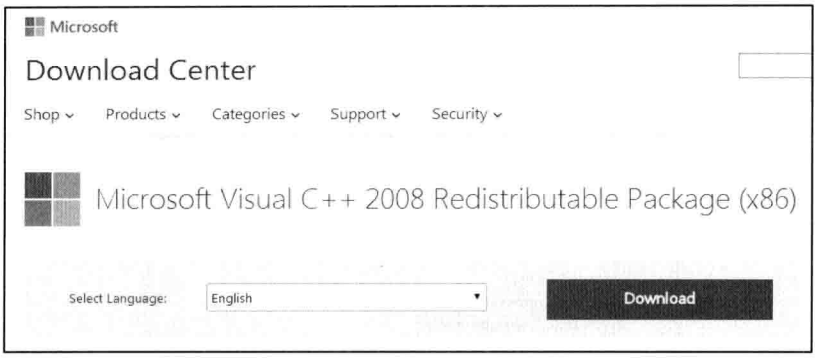

图 18-1　运行库支持包下载页

图 18-2　运行库安装完成界面

安装完成后，请重新启动操作系统。

2．安装 Win32 OpenSSL v1.0.1g Light

单击表 18-1 中链接下载“Win32 OpenSSL v1.0.1g Light”软件包，下载完成后，双击安装包 Win32OpenSSL_Light-1_0_1g.exe。当出现安全警告对话框，提示“无法验证发布者，您确定要运行此软件吗？”时，单击“运行”按钮，进入安装过程。

当出现如图 18-3 所示画面时，表示系统缺少 Visual C++ 2008 Redistributables 运行库或该运行库安装不正确，请重新安装。

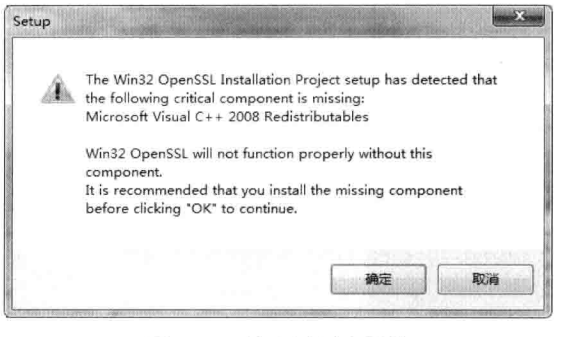

图 18-3　缺少运行库警告

当出现“License Agreement”对话框时，选择“I accept the agreement”，单击“Next”

按钮。

当出现如图 18-4 所示画面时，选择“The OpenSSL binaries (/bin) directory”，表示把 OpenSSL 动态库复制到 OpenSSL 的安装目录的 bin 目录下。

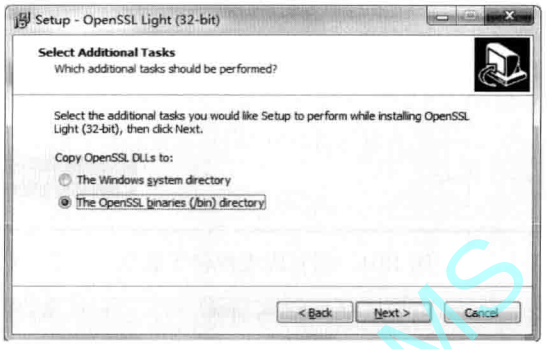

图 18-4　选择复制 OpenSSL 动态库位置

当出现如图 18-5 所示画面时，要求选择安装路径，本例使用“D:\var\OpenSSL-Win32”。

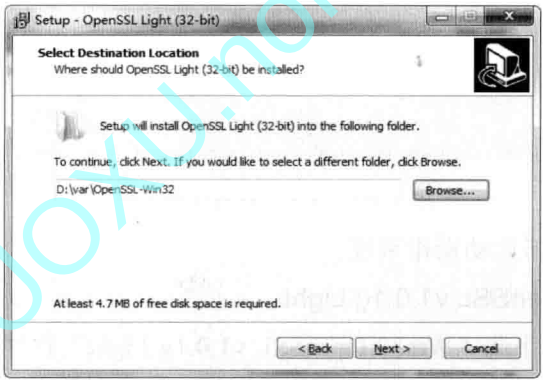

图 18-5　安装路径选择

安装完成后，会出现如图 18-6 所示画面，单击“Finish”按钮，结束安装。

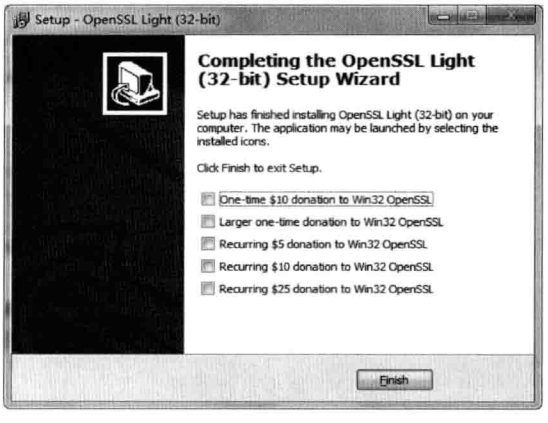

图 18-6　安装结束界面