# 第 13 章　公钥基础结构

公钥加密是用于电子商务、Intranet（企业内部网）、Extranet（企业外部网）和其他网络应用程序的核心技术。但是，要想充分利用公钥加密带来的好处，就还需要基础结构的支持。Windows 2000 系统本身包括了一个公钥基础结构（Public Key Infrastructure, PKI），它完全是利用 Windows 2000 的安全验证体系而设计的。

本章介绍了公钥基础结构的基本原理，包括它们所提供的优点以及实现它们所需要的组件。同时也介绍了 Windows 2000 的 PKI 组件在提供互操作性、安全性、灵活性和易用性时是如何传递所需的服务的。

## 13.1　PKI 基础

### 13.1.1　公钥加密算法

加密技术是一门保护数据的科学。加密算法从数学上将输入的“ 明文 ”数据与“ 加密密钥 ”结合起来生成加密数据（密文）。

在传统的对称加密算法中，用于加密的密钥与用于解密的密钥是相同的。对于想要使用密钥加密进行通信的双方，只有安全地交换加密和解密密钥后，才能相互交换加密数据。而公钥加密算法（也叫做非对称加密算法）的基本属性则是：加密和解密使用不同的密钥。用公钥加密密钥进行的加密是“ 单向 ”的，明文虽然可以很容易地转变为密文，但加密密钥却与解密过程无关。要将密文转回到明文，则必须要用解密密钥（与加密密钥有关，但不相同）。因此，对于公钥加密来说，每个用户都有一对密钥，由一个“ 公钥 ”和一个“ 私钥 ”组成。在知道对方公钥的情况下，可以使用该公钥对一段数据进行加密，然后发送给对方，那么该密文就只能由对方的私钥解密。

使用公钥加密算法，能够完成以下一些功能。

**1. 数字签名**

数字签名是一种确保数据完整性和原始性的方法。由于数据被签名并确认了对数据签名的人或实体的身份，因此数字签名提供有力的证据。数字签名启用“ 完整性 ”和“ 认可 ”这两项重要安全功能，这是实施安全电子商务的基本要求。

当数据以明文或未加密形式分发时，通常使用数字签名。因为在分布式计算环境中，网络上的任何人使用适当的访问都可能读取或改变明文文本而无论是否授权。在这些情况下，当消息本身的敏感度不能保证加密时，将强制数字签名以确保数据保持原始形式并且没有被冒名者发送。

**2. 认证**

身份验证对于安全通信十分重要。用户必须在与另一方通信时有能力证实双方的身份。网络上的身份验证很复杂，因为通信各方在通信时实际上没有接触，这会为攻击者截获消息或冒充另一个人或实体提供了可乘之机。

数字证书是提供身份验证的常用保密措施。证书使用加密技术解决物理上缺乏联系的通信问题。使用这些技术限制攻击者截获、篡改或伪造消息的可能性。这些加密技术使证书难以修改。因此，实体要冒充他人很困难。

证书中的数据包括来自证书主题的公钥和私钥对的公用加密密钥。对于带有发送方私钥签名的消息，消息接收方可以使用发送方公钥确认其真实性。公钥可以在发送方证书的副本上找到。使用证书公钥验证签名可以证实签名是使用证书主题私钥创建的。如果发送方小心

并保持私钥机密性，接收方就可以确信消息发送方的身份。

用来提供身份验证的一些证书方法有：

- 通过传输层安全（TLS）或安全套接字层（SSL）协议，用户到安全 Web 站点上的身份验证。
- 通过 TLS，服务器到用户的身份验证。
- 登录到 Windows 2000 域。

**3. 安全密钥协议**

网络（例如 Internet）上的通信容易受到未知的，可能还是有恶意的用户的监视。公用网络对于未加密的敏感信息来说是危险的，因为任何人都可以访问网络并且对在两点间传输的数据进行分析。即便专用局域网（LAN）也容易被有意图的入侵者从物理上进入网络。因此，如果在任何类型的网络上的计算设备间传输敏感信息，用户几乎肯定会使用一些加密方法来保证数据的隐秘性。

公钥加密不用于加密大量数据。实际上，数据通常由密钥加密来保护，而密钥则由数据接收方公钥加密。加密的密钥和自身的加密数据接着被传输到接收方，接收方将使用私钥解密密钥，然后将使用密钥解密消息本身。

证书使用大量不同的方法保证传输数据的机密性。使用证书的常用保密协议有：

- 安全的多用途网际邮件扩充协议（S/MIME）
- 传输层安全（TLS）
- IP 安全（IPSec）

**4. 数据加密**

在计算机上，以电子邮件形式存在的敏感数据、磁盘上的文件和网络上传输的文件都可以使用密钥加密。通常，公钥加密不用于加密大量数据。但是，公钥加密确实提供了有效的方法：向某些用户发送密钥，当大量数据执行了对称加密操作时，这些用户可以使用密钥。

举一个例子：假设 B 要向 A 发送大量加密文件。由于操作原因，B 将使用对称密钥算法加密数据，例如数据加密标准（DES），为了发送加密的数据和安全加密数据所需的 DES 密钥，B 将用从 A 的证书处获得的公钥加密密钥。因为 A 的公钥被用来加密密钥，具有私钥的 A 就是惟一能够解密 DES 密钥从而解密 DES 加密数据的人。

### 13.1.2 公钥基础结构

使用公钥加密算法能够大幅度提高在网络上的安全性，而公钥基础结构（PKI）就是便于使用公钥加密的一套操作系统和应用程序服务。PKI 一般来说应该具有以下一些功能。

- 管理密钥：PKI 方便了颁发新密钥、检查或吊销现有密钥、以及管理不同颁发者发行的密钥的信任程度。
- 发行密钥：PKI 为客户端明确定义了定位和获得公钥，以及查看某公钥是否有效的途径。如果不能获得公钥和知道它的有效性，用户就不能利用公钥服务。
- 使用密钥：PKI 为用户提供了便于使用密钥的途径。它不仅将密钥置于用户需要的地方，而且还提供了执行公钥加密的便于使用的应用程序，使之能保障电子邮件、电子商务和网络的安全。

那些需要公钥加密功能的应用程序需要有安全、便于使用、灵活的方式来管理、发行和使用公钥，这正是需要公钥基础结构的原因。

**1. 数字证书**

数字证书是 PKI 的基础。证书主要是证明证书持有人的身份颁发机构所颁发的数字声明。证书将公钥与拥有相应私钥的个人、计算机或服务绑在一起。证书提供了一种机制，用于确立对公钥和拥有相应私钥的实体之间关系的信任。数字证书由各种公钥安全服务和提供身份验证的应用程序、数据完整性和通过网络（例如 Internet）的安全通信使用。

证书是一种特殊类型的数字签名式的声明：证书的主题则是一个特殊的“主题公钥”，该证书是由身份颁发机构签名的。通常，证书也含有与主题公钥有关的其他信息，如有相应私钥的实体标识信息。因此，当颁发一个证书时，颁发者就证明了主题公钥和主题标识信息之间绑定关系的有效性。

**2. 公钥基础结构的组件**

在公钥基础结构（PKI）中，有以下五个组件创建、传输并使用了 PKI 赖以生存的数字证书并使之生效。

- 证书颁发机构（CA）：证书颁发机构的大小差别可能很大。大的机构一般为商业证书颁发机构，它们向数百万用户颁发证书；小的机构一般为公司部门内的证书颁发机构，它们只向少数几个用户颁发证书。这些较小的证书颁发机构可能是“中级证书颁发机构”，它们的证书由单位内级别较高的证书颁发机构签署，而高级别机构的证书又来自更高级别，以此类推，直到根级证书颁发机构。每个证书颁发机构都有责任决定证书中应包括什么属性，以及在颁发证书前用什么机制来验证这些属性。证书颁发机构还颁布“颁发证书吊销列表”（CRL）。当某证书被吊销后（不论是因为所有人的私钥泄露还是因为持有人已经与颁发者脱离关系），证书颁发机构会将它添加到 CRL，然后公布 CRL，以便客户端检查。这种方法就像信用卡发行商公布的失窃的信用卡列表一样，任何授权请求都必须先清除此列表，然后才能获准。
- 证书发行点：证书发行点使证书和 CRL 可以在单位内或单位外公开发布。它还使支持整个 PKI 所需的重要材料能够得到更广泛的使用。具体地讲，好的证书发行者允许客户端自动获得证书，包括根级证书和所要证书之间的所有证书。发行者可使用各种目录服务，包括 X.500、轻量型目录访问协议（LDAP）或因操作系统而异的目录，还可在网页上发行证书和公布 CRL，或者通过智能卡、磁盘或 CD-ROM 来传播。在这些所有的途径中，LDAP 的协作性最好，灵活性最强。
- 密钥和证书管理工具：如果希望应用 PKI 来满足一些管理要求。例如，站点必须记录颁发了哪些证书、颁发时间、持有人；旧证书需要归档，以便即使证书不再起作用后也能阅读加密的电子邮件。同时，还必须有某些途径来控制和监视证书颁发机构和证书发行者发行和公布证书及 CRL 的情况；这正是为什么有用的 PKI 必须有一个组件是管理和审计工具的原因。
- 能使用公钥的应用程序：PKI 能够颁发、发行和控制证书后，下一步就是部署能够使用证书的应用程序。与 PKI 其余部分紧密结合的好的应用程序应能全面利用公钥加密技术，同时对用户又几乎是透明的。用户无须知道如何加密、证书的保存位置以及任何其他细节，而只须简单地表明想干什么，然后把事情交给应用程序和 PKI 去完成就可以了。应用程序可利用数字证书来推广公钥加密带来的好处，而且能结合加密技术的功能（如数字签名和加密），实现电子商务、网络的安全访问和其他有吸引力的服务。
- 硬件支持：要求实施 PKI 的需求日益强烈，刺激了硬件供应商开发出加密硬件，包括能进行本机加密处理的智能卡、PC 卡和 PCI 卡。这些硬件设备提供了众多能

力，在低端，智能卡可进行有限的加密处理和密钥的安全存储；在高端，多处理器加密加速器能提供大容量的网络数据保护服务，摆脱了软件加密模块造成的瓶颈。PKI 硬件设备的最优处在于它是可选的，如果应用程序需要其他性能或安全性，可以按照需要通过添加硬件来实现。

**3. 证书颁发机构的层次结构**

证书颁发机构的层次结构是一种信任模型。在这种模型中，通过在 CA 之间建立父/子关系，创建了认证路径。构成证书颁发机构层次结构的成分包括：根 CA，已经被根 CA 鉴定过的下级 CA 和已经被其它下级 CA 鉴定过的下级 CA。

根 CA（Root CA）是一个机构的 PKI 中最可信任的 CA 类型。通常情况下，根 CA 的物理安全性和证书发放策略比下层 CA 更严格。如果根 CA 受到危害，或者向某个未经授权的实体发放了证书，那么在你的网络架构中，所有基于证书的安全性都突然成为脆弱的。虽然对于发送安全电子邮件之类的任务，也可以利用根 CA 为终端用户发放证书，但是在大多数机构中，只将根 CA 用于向其他 CA，即下级 CA 发放证书。

下级 CA（Subordinate CA）是已经被另一个 CA 鉴定过的 CA。通常，下级 CA 针对特定的用途发放证书，例如安全电子邮件、基于 Web 的身份验证，或者智能卡身份验证。下级 CA 也可以向其他的，更下级的 CA 发放证书。

## 13.2 Windows 2000 中的 PKI

Windows 2000 操作系统为 Windows 平台引进了一个全面的公钥基础结构（PKI）。这个基础结构扩展了以前 Windows 系统中基于 Windows 公共密钥（PK）的加密服务，它提供了一个服务和管理工具，例如创建、配置和管理基于 PKI 的应用程序的集成化集合。

Microsoft 将公钥服务集成在 Windows 2000 中的主要动机是为未来的电子商务提供平台。即提供基于诸如 Kerberos v5、安全套接字层（SSL）、传输层安全（TLS）和 IP 安全等 Internet 标准协议的分布式验证服务。公钥服务集成到 Windows 2000 也意味着它利用了活动目录服务和操作系统所提供的安全基础结构的优势，从而保持成本下降的趋势，使 PKI 的管理尽可能透明。同样，实现既定的 Internet 标准是获得同其他标准的 PKI 产品互操作性的一个重要的必要条件。

Windows 2000 用来支持 PKI 的特性包括：

- 证书。Windows 2000 中基于证书的进程所使用的标准证书格式是 X.509 v3。X.509 证书包括接受证书的个人或实体的有关信息、证书的有关信息以及有关证书颁发机构的可选信息。主题信息可能包括实体名称、公钥、公钥算法以及可选择的惟一主题标识。X.509 v3 证书的标准扩展部分则包含与密钥标识、密码用法、证书策略、候选名称和属性、证书路径约束相关的信息，以及用于吊销证书的增强部分，其中包括吊销的原因和由 CA 更新的 CRL 部分。
- Windows 2000 Server 上的证书服务。证书服务是 Windows 2000 用来创建和管理证书颁发机构（CA）的组件。CA 负责建立和确定证件持有者的身份。如果证书不再有效，CA 会吊销证书并公布由证书核对者使用的证书吊销列表（CRL）。最简单的 PKI 设计只有一个根 CA。然而实际上，部署 PKI 的大部分组织会使用多个 CA，这些 CA 被组织成称为证书层次结构的信任组。证书服务的个别组件是 CA Web 注册页面。这些 Web 页是在安装 CA 时默认安装的，并允许证书申请者使用 Web 浏览器递交证书申请。另外，也可以在未安装证书颁发机构的 Windows 2000 服务器上安装 CA Web 页面。在这种情况下，系统使用 Web 页直接将证书申请递交给 CA，

而不管是什么原因，都不希望申请者直接访问。用户可以使用证书颁发机构的 MMC 控制台管理证书服务。

- 智能卡支持。Windows 2000 支持通过智能卡上的证书登录，以及使用智能卡存储用于 Web 身份验证、安全的电子邮件以及与公钥加密相关的其他活动的证书。
- 公钥策略。在 Windows 2000 中可以使用组策略自动给计算机指派证书、建立证书信任表和公用的信任证书颁发机构，以及为 EFS（文件加密系统）管理恢复策略。

Windows 2000 PKI 的组成结构如图 13-1 所示。

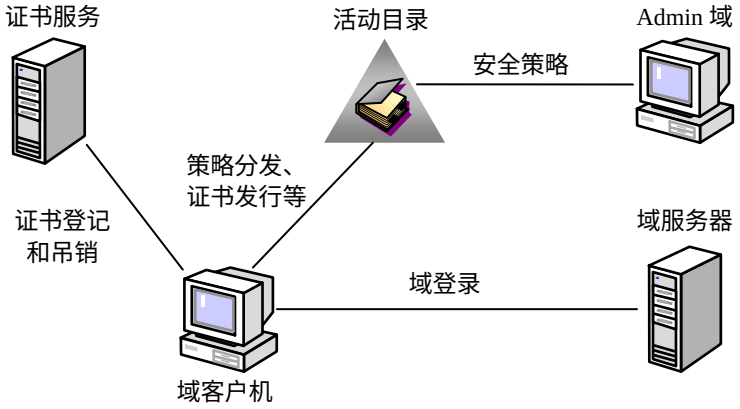


图 13-1 Windows 2000 PKI 结构组件图

## 13.3 使用 Windows 2000 中的 PKI

### 13.3.1 创建证书颁发机构

创建证书颁发机构（CA）的方法是在 Windows 2000 系统上安装证书服务。在安装证书服务之前，应该首先规划单位中证书颁发机构和公钥基础结构的配置。

#### 1. 安装证书服务

如果要在 Windows 2000 Server 上安装证书服务，则会有许多可能需要安装 CA 的情况。若要在已安装 Windows 2000 Server 的服务器上安装证书服务，可通过“控制面板”中的“添加/删除程序”→“添加/删除 Windows 组件”中选择安装证书服务。尽管证书服务是一种 Windows 2000 的服务并且随 Windows 2000 Server 一同提供，但它并不是作为最初安装过程的一部分默认安装的。若要在 Windows 2000 Server 最初的基本安装过程中安装证书服务，必须在安装期间从显示的可选组件列表中选取该组件。只有在 Windows 2000 安装完成后登录到服务器时证书服务安装才真正完成。

#### 2. 安装选项和信息

在安装证书服务的时候，需要提供以下信息。

（1）证书颁发机构的类型选择

在证书服务安装期间，可以选择安装任意类型的证书颁发机构（CA），其界面如图 13-2 所示。

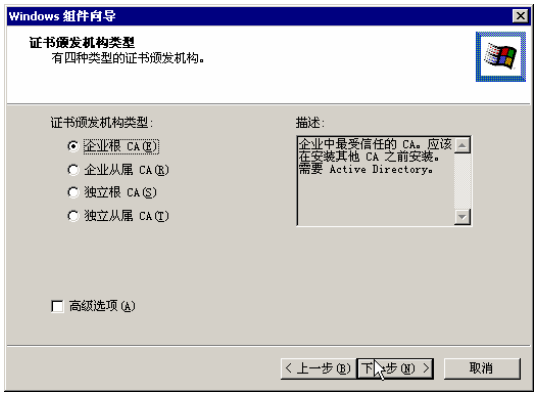


图 13-2 证书颁发机构类型

- 企业根 CA：企业根 CA 是证书层次结构中的最高级 CA。企业根 CA 需要 Active Directory。它自我签发自己的 CA 证书并将该证书发布至域中所有 Windows 2000 服务器和工作站的受信任的根证书颁发机构的存储区中。
- 企业下级 CA：企业下级 CA 必须从另一 CA 获得它的 CA 证书。企业下级 CA 要求 Active Directory。若想使用 Active Directory、证书模板和智能卡登录到 Windows 2000 计算机时，应使用企业下级 CA。
- 独立根 CA：独立根 CA 是证书层次结构中的最高级 CA。独立根 CA 既可以是域的成员也可以不是，因此它不需要 Active Directory。然而，如果 Active Directory 存在的话，独立根 CA 将会使用 Active Directory。由于独立根 CA 不需要 Active Directory，因此可以很容易地将它从网络上断开并安置在安全的区域，这在决定创建安全的脱机根 CA 时非常有用。
- 独立下级 CA：独立下级 CA 必须从另一 CA 获得它的 CA 证书。独立下级 CA 可以是域的成员也可以不是，因此它不需要 Active Directory。然而，如果 Active Directory 存在，它将会使用 Active Directory。独立下级 CA 必须从另一 CA 获取它的 CA 证书。

图 13-3 则说明了证书颁发机构的层次关系，其中包含了根 CA、中级 CA 和颁发 CA 之间的关系。

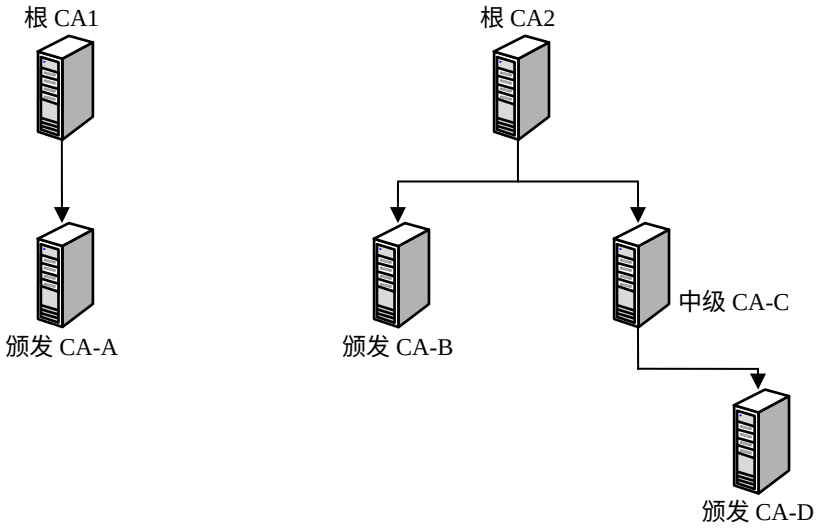


图 13-3 证书颁发机构的层次关系

如果在选择要安装的 CA 类型时启用“高级选项”，那么还可以选择使用加密服务提供程序（CSP）。CSP 生成公钥和私钥对并代表 CA 执行加密操作。

在高级选项中，还可以为 CA 用来签发证书的公钥加密密钥设置密钥长度。一般来说，密钥越长越安全。但在安装期间较长的密钥需要花更长的时间才能生成。

此外，在高级选项中还可以选择 CA 使用的消息散列算法，以及指定使用现有的加密密钥，而不是生成新密钥，如图 13-4 所示。

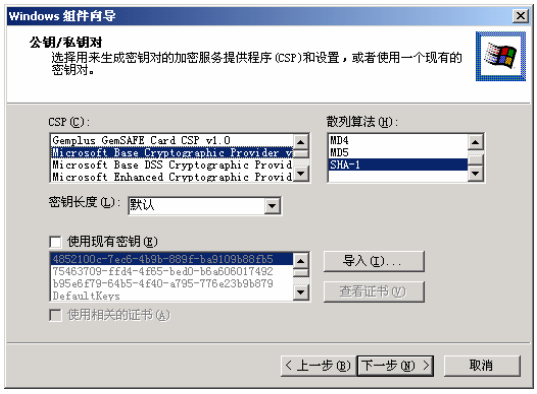


图 13-4　证书服务安装的高级选项

（2）证书颁发机构标识信息

表 13-1 列出了在证书服务安装过程中完成 CA 标识信息及其说明。

表 13-1　CA 标识信息说明

| 字　　段 | 说　　明 |
|---|---|
| CA 名称 | 要提供给 CA 的名称。可以使用几乎所有字符来输入字符串。CA 的名称也是 Active Directory 中 CA 可分辨名称的公用名。当 CA 名称中存在特殊字符时，对于不能使用未修改 CA 名称的操作须用“净化的”CA 名称。“净化过的”CA 名称是 CA 特有的名称，其中的所有特殊字符都经过编码，以便能用于文件名、CryptoAPI（CAPI）密钥容器名称和 Active Directory 对象名称。特殊字符是指那些不能在上述名称中使用的一个或多个字符，包括所有的非 ASCII 字符和许多 ASCII 标点符号。此外，根据 LDAP 标准，Active Directory 对象名须限制在最多 64 个字符 |
| 单位 | 在合适的国家（地区）或省市政府机构注册的单位合法名称 |
| 组织单位 | 可用来区分单位内不同的部门，例如 Internet 安全单位或人事部门 |
| 地点 | 单位所在的城市 |
| 州或省 | 单位的物理位置 |
| 国家（地区） | X.500 命名架构标准所要求的双字符国家（地区）代码。例如，美国的代码为 US，加拿大为 CA |

（3）数据库和配置存储

证书服务对数据库、配置数据、备份数据和记录数据使用本地存储设备。可以在 CA 安装期间指定数据库和记录的位置，如图 13-5 所示。

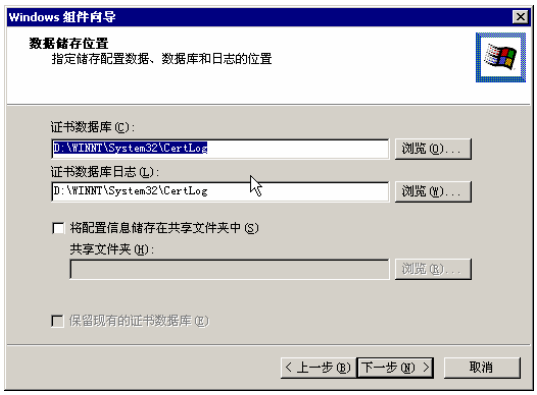


图 13-5 证书服务的数据库和存储配置

默认情况下，CA 所颁发的证书存储位置是%SYSTEMROOT%\system32\certlog。也可以在安装 CA 时指定共享文件夹。共享文件夹是计算机用户查找证书颁发机构相关信息的位置。只有在安装了独立的 CA 但没有 Active Directory 时，该选项才有效。

如果证书服务的主机是域的成员，那么有关 CA 的信息会自动发布到 Active Directory。然而，Active Directory 不作为证书服务的数据库。该功能在本地计算机上保留。

### 13.3.2 为用户分发证书

#### 1. 申请证书

证书申请必须由有权访问与公钥相关联的私钥的用户、计算机或服务产生，该公钥和私钥对将成为证书的一部分。根据系统管理员建立的公钥策略，计算机和服务可以自动申请证书而不受用户干涉。此外，通过使用注册代理证书，管理员还可以申请智能卡用户证书和智能卡证书以便代表其他用户登录到系统。

在 Windows 2000 中，有两个主要方法可明确地申请证书：

（1）使用证书申请向导申请证书

当从 Windows 2000 企业证书颁发机构申请证书时，可以使用位于“证书”管理单元中的证书申请向导，如图 13-6 所示。

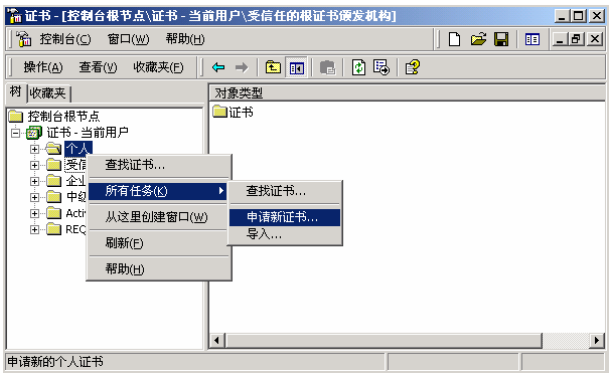


图 13-6 使用证书申请向导申请证书

- 选择要向其提交申请的证书颁发机构。只有在 Windows 域中可用的企业证书颁发机构才可以使用证书申请向导颁发证书。
- 对于新证书，选择适当的证书模板，如图 13-7 所示。证书模板为证书申请预定义了许多常用配置。证书模板描述所申请的证书的使用目的。对可用的证书模板列表由证书颁发机构所配置颁发的证书类型，以及系统管理员是否授予用户对证书模板的访问权限来决定。

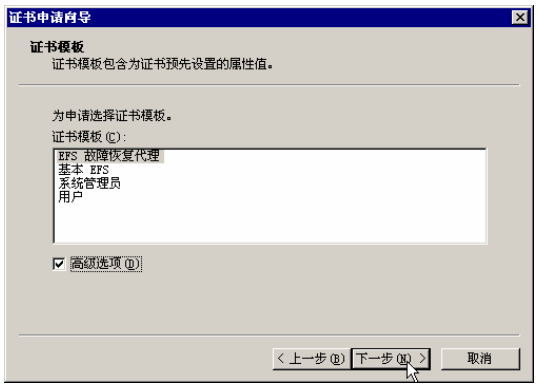


图 13-7 选择证书模板

- 使用“ 高级选项 ”来选择为与证书申请相关的密钥对选择加密服务提供程序 (CSP)。这是可选的。

当使用证书申请向导时，只有基本 EFS（加密文件系统）和 EFS 故障恢复代理证书才有标记为可导出的相关私钥。如果要申请其他类型的证书，并想使其私钥可导出到 PKCS #12 文件，则需要使用 Windows 2000 证书服务 Web 页上的 “ 高级申请 ” 页。

（2）使用 Windows 2000 证书服务 Web 页申请证书

安装在 Windows 2000 服务器上的每个证书颁发机构都有用户可以提交基本和高级证书申请的 Web 页。默认情况下，这些页位于 http://servername/certsrv，其中 servername 是宿主 CA 主机的 Windows 2000 服务器的名称。

从 Windows 2000 独立证书颁发机构申请证书时，可使用证书服务 Web 页，如图 13-8 所示。如果要设置在证书申请向导中不可用的可选申请功能，例如将密钥标记为可导出、设置密钥长度、选择散列算法或将申请保存到 PKCS #10 文件，可以使用 Web 页从 Windows 2000 企业证书颁发机构申请证书。

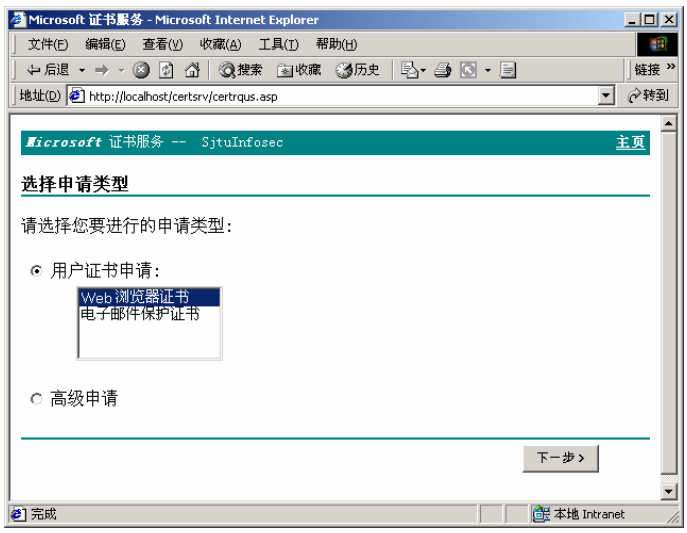


图 13-8 使用 Web 页申请证书

**2. 处理证书申请**

在将证书申请提交到 Windows 2000 企业证书颁发机构时，它将被立即处理，而不是被设置为 “ 未决 ”。证书申请将立即失败或授予。如果被授予，将颁发证书，并且系统将提示申请证书的用户安装证书。

而在将证书申请提交到 Windows 2000 独立证书颁发机构时，申请将被立即处理。或者

在默认情况下，在证书颁发机构管理员批准或拒绝申请之前，该申请将先被“ 待定 ”(挂起)。可在证书颁发机构所在的服务器上查看到该待定的证书申请，如图 13-9 所示。在待定申请的情况下，证书申请者将必须使用证书服务 Web 页以检查未决证书的状态。

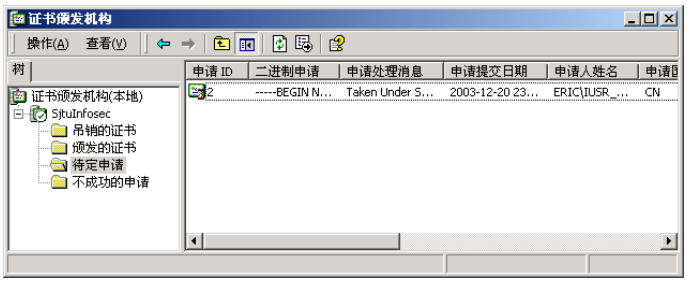


图 13-9　在证书颁发机构中查看待定申请

在处理证书申请时，Windows 2000 的证书颁发机构（CA）执行下列操作：

（1）接收申请。证书申请由客户应用程序（如证书管理单元中的证书申请向导）发送，它将证书申请处理为 PKCS #10 格式的申请报告并提交给 CA。

（2）申请已被批准。CA 服务器引擎调用查询申请属性的 CA 策略模块，确定此申请是否已获得授权，并设置可选的证书属性。

（3）证书形成。如果此申请被批准，CA 服务器引擎取出该申请以及由策略模块申请的任何属性，并建立一份完整的证书。

（4）证书发布。CA 服务器引擎将完整的证书存储在它的证书数据库中，并将申请状态通知给中间应用程序。如果退出模块已向它发出了申请，则服务器引擎会向它通知证书颁发事件。它允许退出模块执行进一步的操作，比如向 Active Directory 发布证书。其间，客户应用程序从证书数据库获得发布的证书，并将它保存在自己的本地证书存储区中。

### 13.3.3　证书和密钥的导出

证书管理单元提供管理工具以导出和导入证书。如果需要，还可以包括证书路径和私钥。可以将证书导出到这些文件，也可以从这些文件导入证书：PKCS #12 文件、PKCS #7 文件和二进制编码的 X.509 证书文件。

#### 1. 导入证书

导入证书一般用于以下情况：

- 安装由另一用户、计算机或证书颁发机构发送来的文件中的证书。
- 还原受损或丢失的以前备份的证书。
- 从证书持有者以前使用的计算机上安装证书及其相应的私钥。

导入证书时，应将证书从使用标准证书存储格式的文件复制到本地的用户账户或计算机账户的证书存储区中。

#### 2. 导出证书

导出证书用来备份证书及其相关私钥，可用于以下情况。

- 复制证书以在另一台计算机上使用。
- 从证书持有者当前的计算机上删除证书及相关私钥，以在另一台计算机上安装。

当导出证书时，即将证书从证书存储复制到使用标准证书存储格式的文件。

#### 3. 标准证书文件格式

可以按以下格式导入和导出证书。

- 个人信息交换（PKCS #12）。个人信息交换格式（PFX，也称为 PKCS #12）允许证书及相关私钥从一台计算机传输到另一台计算机或可移动媒体。PKCS #12 是业界格式，适用于证书及相关私钥的传输、备份和还原，可以在相同或不同的供应商的产品间进行。要使用 PKCS #12 格式，加密服务提供程序（CSP）必须认定证书和密钥可以导出。如果证书由 Windows 2000 证书颁发机构颁发，则只有在以下任一条件为真时才可以导出证书私钥：
  - 证书用于 EFS（加密文件系统）或 EFS 故障恢复。
  - 通过 Web 页向证书颁发机构申请证书时，在“高级证书申请”中选中“标记密钥为可导出”复选框。

  因为导出私钥可能使私钥暴露给无关一方，所以 PKCS #12 格式是 Windows 2000 中支持的导出证书及相关私钥的惟一格式。
- 加密消息语法标准（PKCS #7）。PKCS #7 格式允许将证书及证书路径中的所有证书从一台计算机传输到另一台计算机或可移动媒体。PKCS #7 文件通常使用.p7b 扩展名。
- DER 编码的二进制 X.509。该格式可由不在 Windows 2000 服务器上的证书颁发机构使用，因此它支持互操作性。DER 证书文件使用.cer 扩展名。
- Base64 编码的 X.509。该格式可由不在 Windows 2000 服务器上的证书颁发机构使用，因此它支持互操作性。Base64 证书文件使用.cer 扩展名。

### 13.3.4 证书的更新

每个证书都有一个有效期。在有效期结束之后，证书不再被认为是可接受或可使用的凭证。“证书”管理单元允许在有效期结束前后使用“证书续订向导”续订 Windows 2000 企业证书颁发机构所颁发的证书，如图 13-10 所示。可以使用以前使用的密钥集续订证书，也可以使用新的密钥集续订证书。

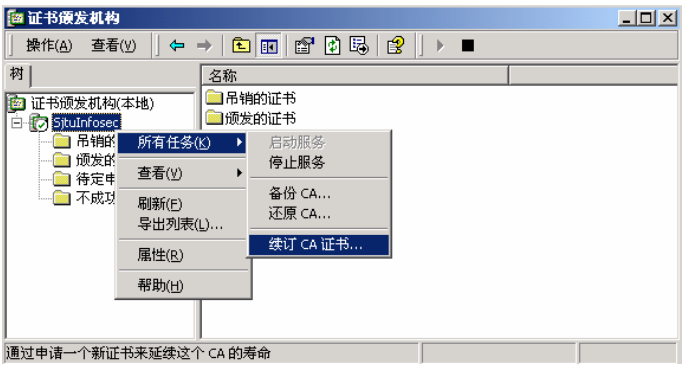


图 13-10 续订证书

此外，可以向证书服务 Web 页传递 PKCS #7 文件的内容，从 Windows 2000 企业证书颁发机构和 Windows 2000 独立证书颁发机构续订颁发的证书。

### 13.3.5 证书的撤销

可以使用证书颁发机构管理单元来吊销证书、管理证书吊销列表（CRL）的发布，以及指定在证书颁发机构（CA）所颁发的每份证书中发布的 CRL 分发点（CDP）。

#### 1. 吊销证书

为了帮助维护单位公钥基础机构（PKI）的完整性，如果证书的受领人离开单位，或者证书受领人的私钥已泄露，或者其他一些与安全相关的事件规定它不再需要将证书视为“有

效”，那么 CA 的管理员必须吊销证书。当证书被 CA 吊销时，它将被添加到该 CA 的证书吊销列表中。

**2. 安排 CRL 的发布**

证书服务的其中一项功能是在 CA 管理员指定了时间间隔后每个 CA 都自动发布更新的 CRL。这个时间间隔被称做 CRL 的发布期。在初次安装 CA 之后，CRL 发布期被设置为一周（基于本地计算机时间，从 CA 首次安装的日期开始计算）。管理员可以使用安排证书吊销列表的发布日程过程来更改证书颁发机构的 CRL 发行间隔。

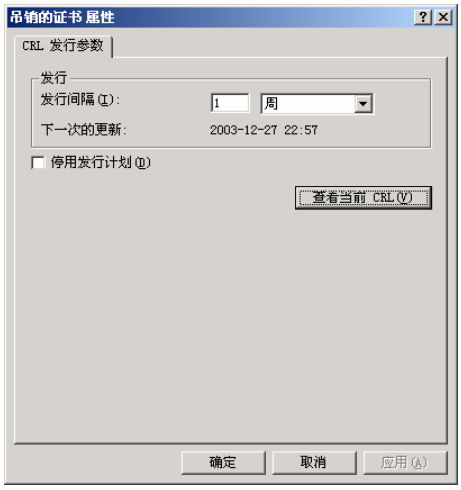


图 13-11 更改 CRL 的发行间隔

而 CRL 的有效期则是证书验证者将 CRL 视为权威的时间段。只要证书验证者在其本地缓存中具有有效的 CRL，它就不会尝试从发布它的 CA 检索另一个 CRL。

CRL 的发布期是由 CA 管理员建立的。但是，CRL 的有效期是从发布期延伸而来的，期间允许进行 Active Directory 复制。默认情况下，证书服务将发布期延长 10%（最多可加上 12 个小时）以建立有效期。因此，如果 CA 每 24 小时发布一次 CRL，那么有效期将被设置为 26.4 小时。

此外，由于还存在时钟偏差，因此考虑到计算机时钟设置中的偏差，CRL 将在其发布期开始前 10 分钟有效。

除了自动发布 CRL 之外，管理员也可以通过使用 CRL 发布向导根据需要发布 CRL。通过使用 CRL 发布向导选择的发布参数不会修改预定的发布期。换句话说，如果在预定的发布期内手动发布 CRL，那么 CRL 将在当前发布期结束时自动重新发布。

即使是已经发布了新的 CRL，具有以前发布的 CRL 之缓存副本的客户仍可以继续使用直到其有效期满，这一点非常重要。手动发布 CRL 不影响仍然有效 CRL 的缓存副本，它只为没有有效 CRL 缓存副本的系统提供新的 CRL。

**3. CRL 分发点和 CRL 文件名**

由 Windows 2000 证书颁发机构颁发的每一份证书将 CRL 分发点作为其内容的一部分。CRL 分发点向证书验证者提供网络位置，可在这里检索 CRL 的当前副本。

默认情况下，CRL 文件在证书颁发机构所在服务器上的以下位置发布：%Systemroot%\System32\Certsrv\Certenroll。

CRL 文件名的格式是 CA 的“净化名称”并附带 CA 的“关键 ID”（如果 CA 证书已使用新的密钥续订）和.crl 扩展名。

### 13.3.6 备份和恢复证书服务

备份和还原操作的目的是保护证书颁发机构（CA）及其可操作数据，以免因硬件或存储媒体出现故障而导致数据丢失。建议采用的 CA 备份方法是使用 Windows 2000 备份程序来备份整个文件服务器。

通过使用“证书颁发机构”管理单元也可以备份和还原 CA（如图 13-12 所示），但是这种备份方法只有在不想备份安装了 CA 的整个服务器的特殊情况下使用。

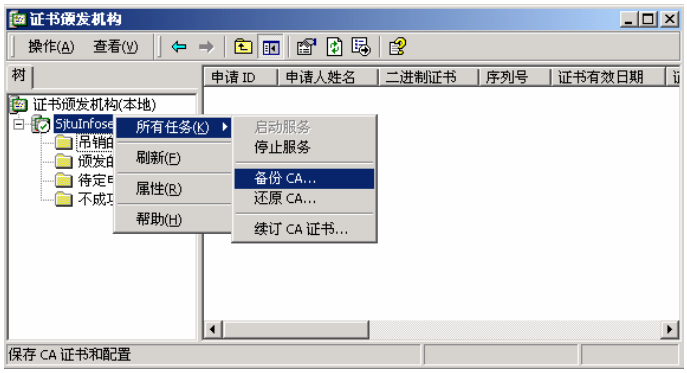


图 13-12 备份和还原证书颁发机构

通过使用“证书颁发机构”管理单元，可以备份和还原以下类型的信息：

- 公钥、私钥和 CA 证书。公钥和私钥使用 PKCS #12 的 PFX 格式备份或还原。
- 证书数据库。

备份向导会要求在备份公钥和私钥及 CA 证书时提供密码。系统需要该密码来存储 CA。

在第一次完成 CA 的完全备份后，以后就可以进行增量备份了。而在还原证书颁发机构时，就需要首先还原完全备份，然后以创建备份的顺序逐个还原每个增量备份。

在还原 CA 的时候，如果该数据库日志在进行还原之前没有手动删除，则该 CA 将还原为进行还原时的状态，数据库日志将重新显示，而且自上次备份之后所进行的改动将应用到该数据库中（数据库日志的默认位置是%systemroot%\system32\certlog）。如果数据库日志在还原之前手动删除了，则该 CA 将还原到执行备份时的状态。