**西安电子科技大学**

**电子商务安全实验课程 实验报告**

**实验名称 PKI证书配置实验**

经济与管理学院 2106011 班

成 绩

姓名 赵红玉 学号 21069100225

同作者

实验日期 2023 年12 月 20日

|  |
| --- |
| 指导教师评语：  指导教师：  年月日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

## 一、实验目的：

**1、深入理解公钥基础设施PKI的工作原理**

**2、熟悉CA证书的发放流程**

**3、学习VMware虚拟机的安装与使用**

**4、掌握windows server操作系统环境下，CA中心的配置**

**5、练习CA证书的申请与安装**

## 二、实验所用仪器（或实验环境）

**1、VMware虚拟机**

**2、windows server 2003操作系统**

## 三、实验要求

**1、安装VMware虚拟机**

**2、在虚拟机中安装windows server 2003操作系统**

**3、在windows server 2003中安装IIS服务**

**4、安装独立根CA**

**5、完成一个证书的申请、审批发放、下载安装的全过程**

## 实验步骤及实验数据记录

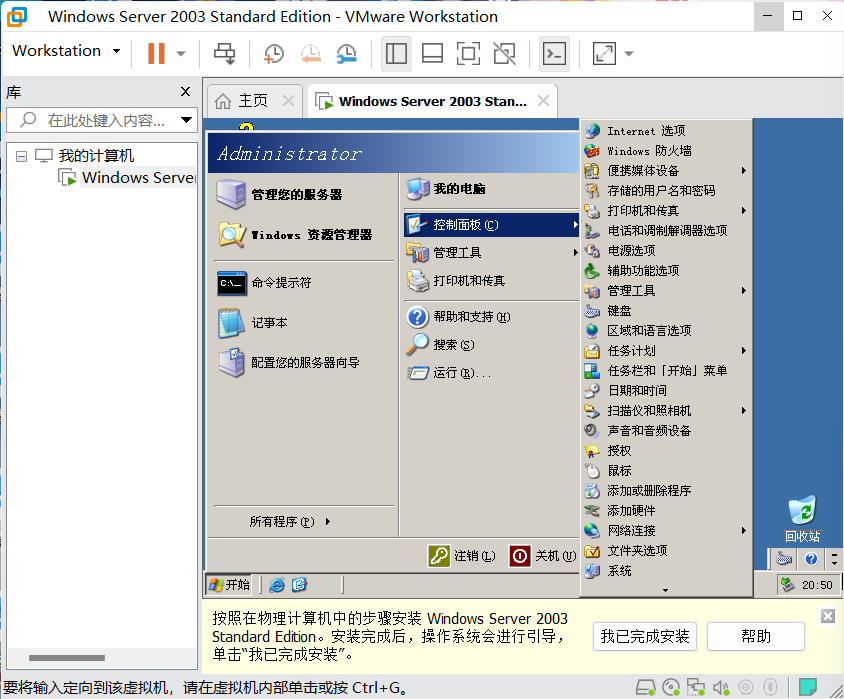
### 1、安装VMware虚拟机

### 2、在虚拟机中安装windows server 2003操作系统

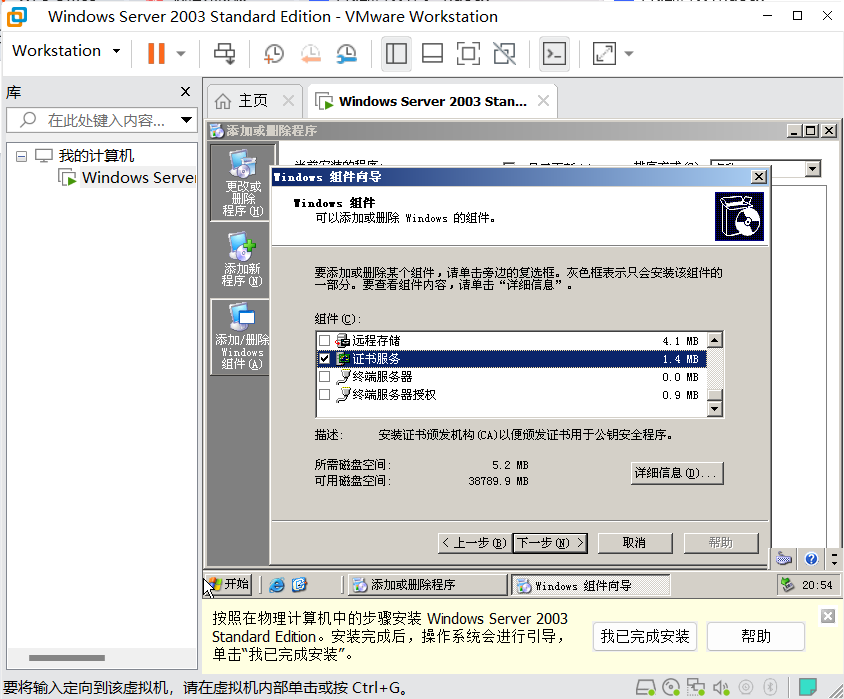
### 3、在windows server 2003中安装IIS服务

### 4、安装独立根CA

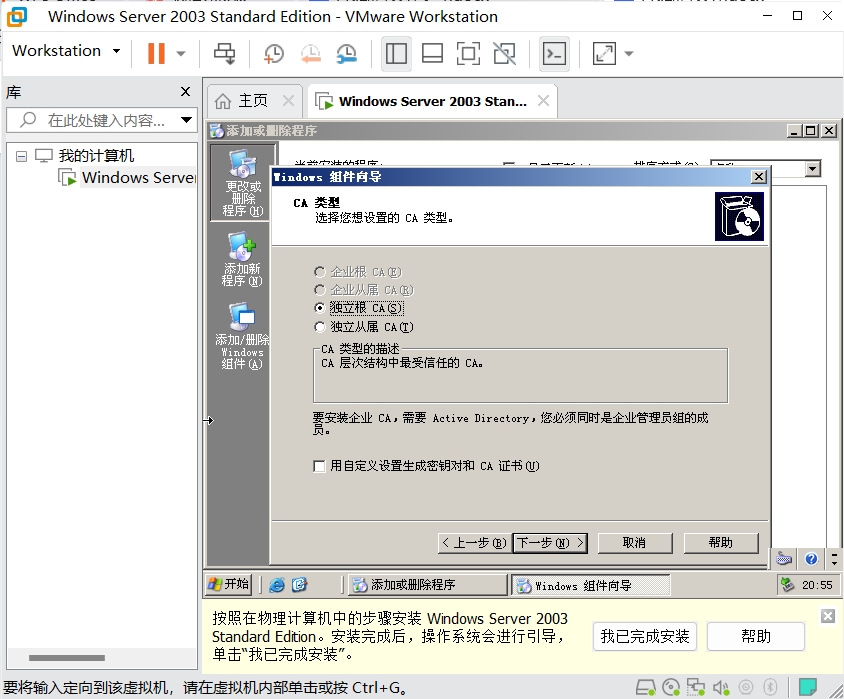
**在Windows server 2003中，选择【开始】->【控制面板】->【添加和删除程序】命令。**

****

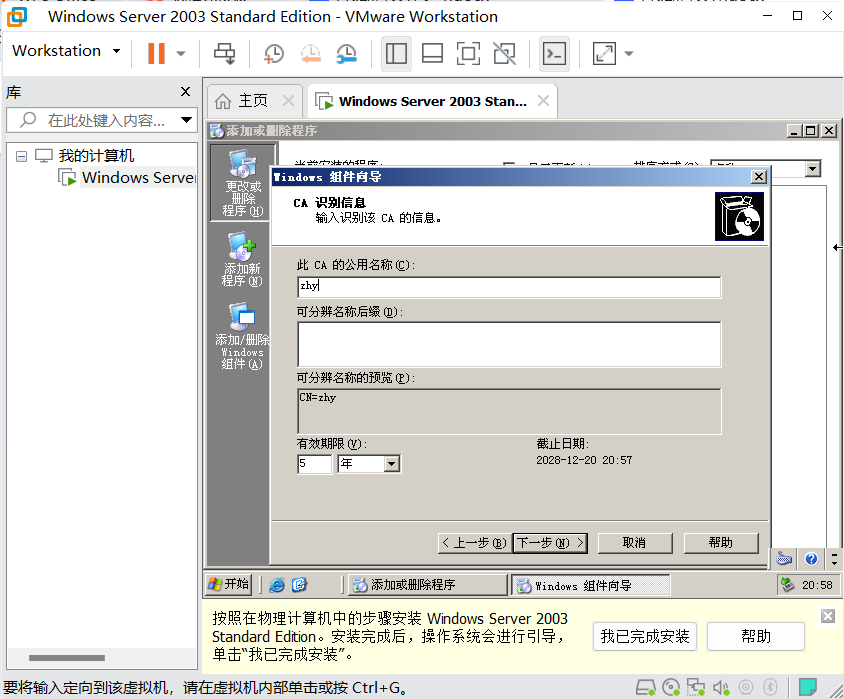
**在弹出的菜单中选择【添加和删除Windows组件】,在组件列表中选择【证书服务】，再单击【下一步】。**

****

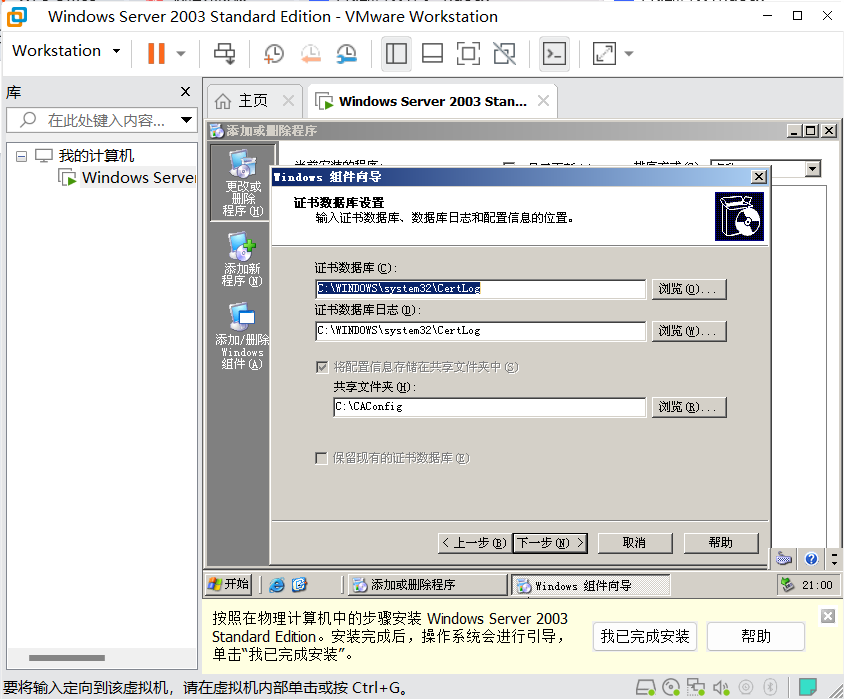
**在弹出的窗口中，选择【独立根CA】，单击【下一步】。**

****

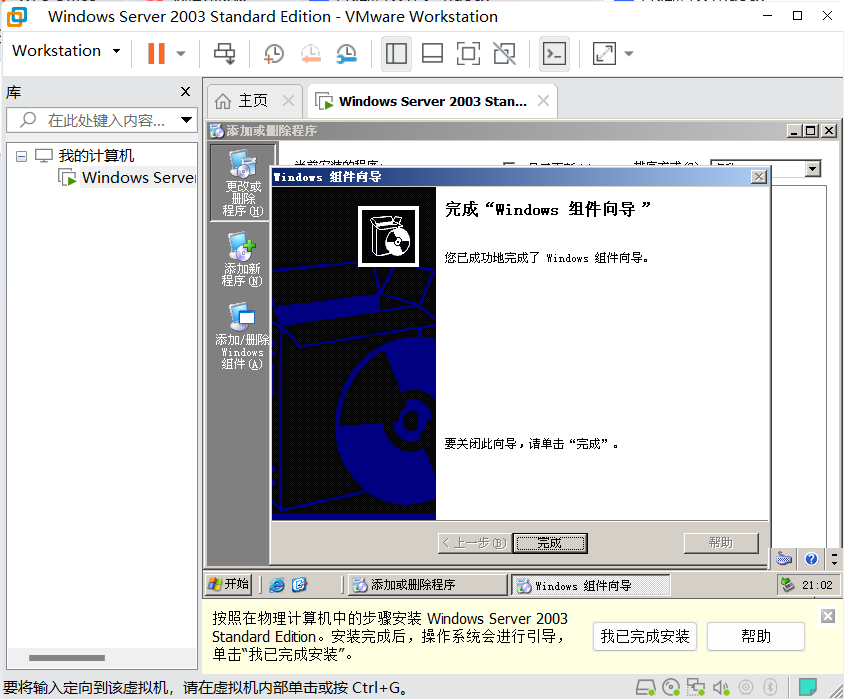
**在弹出的窗口中按要求填写信息，信息为本人名字缩写zhy，填写完成后，点击【下一步】。**

****

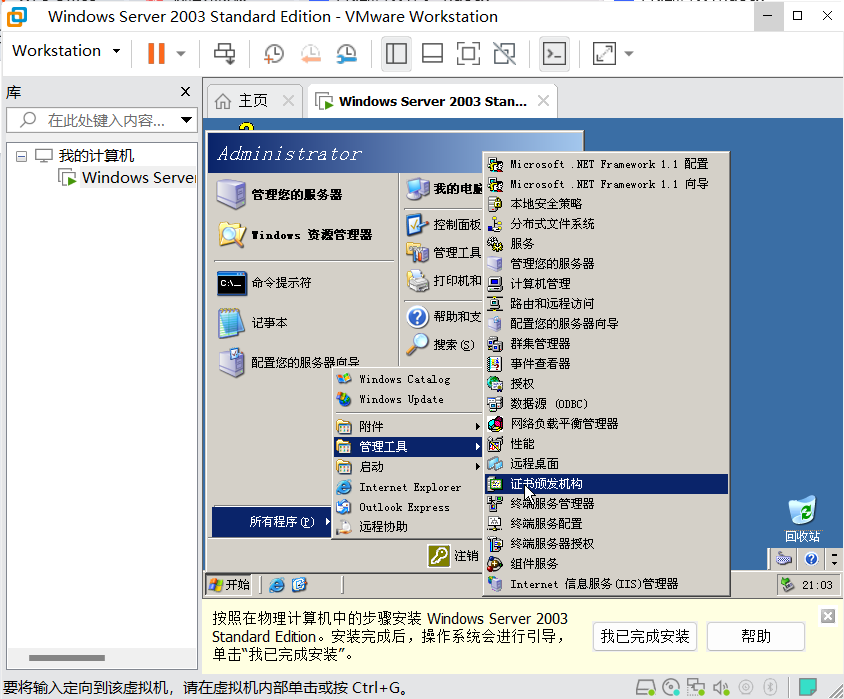
**选择【证书数据库】、【证书数据库日志】和配置信息的存放路径，填完后，单击【下一步】。**

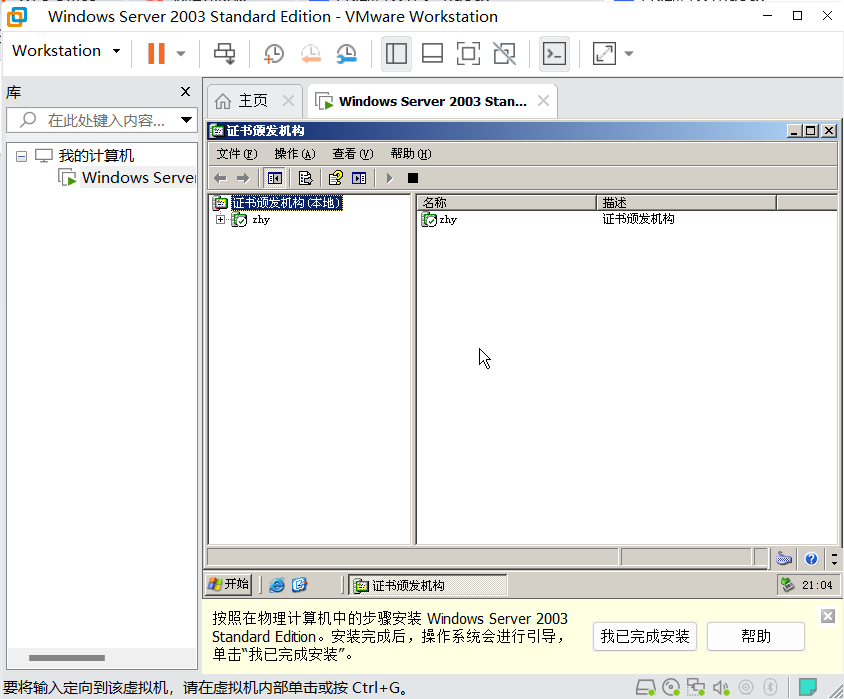
****

**完成安装。**

****

**选择【开始】->【程序】->【管理工具】，若可以找到【证书颁发机构】，则说明安装成功。**

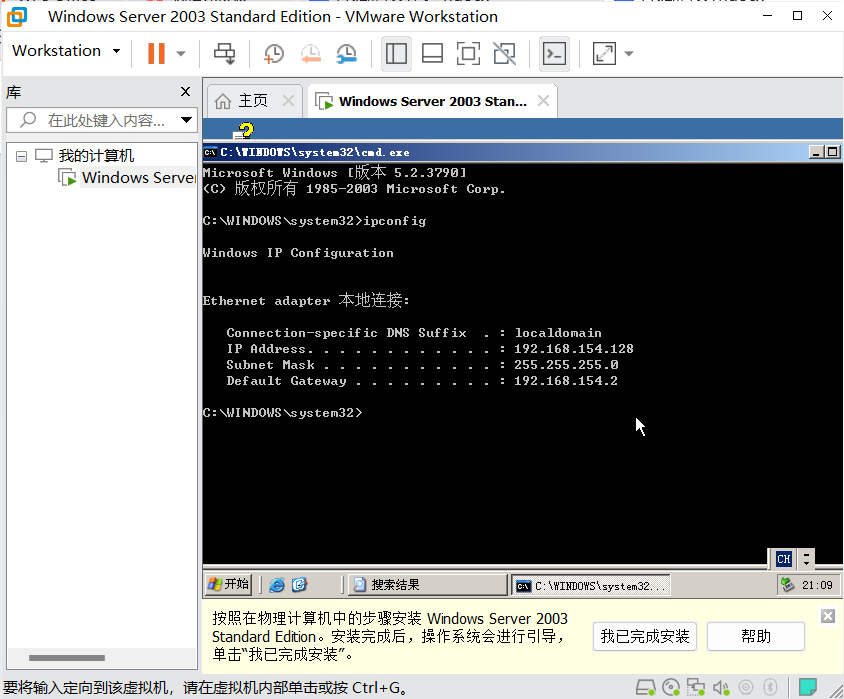
****

****

### 5、完成一个证书的申请、审批发放、下载安装的全过程

#### 通过Web页面申请证书

**先查看本机ip。**

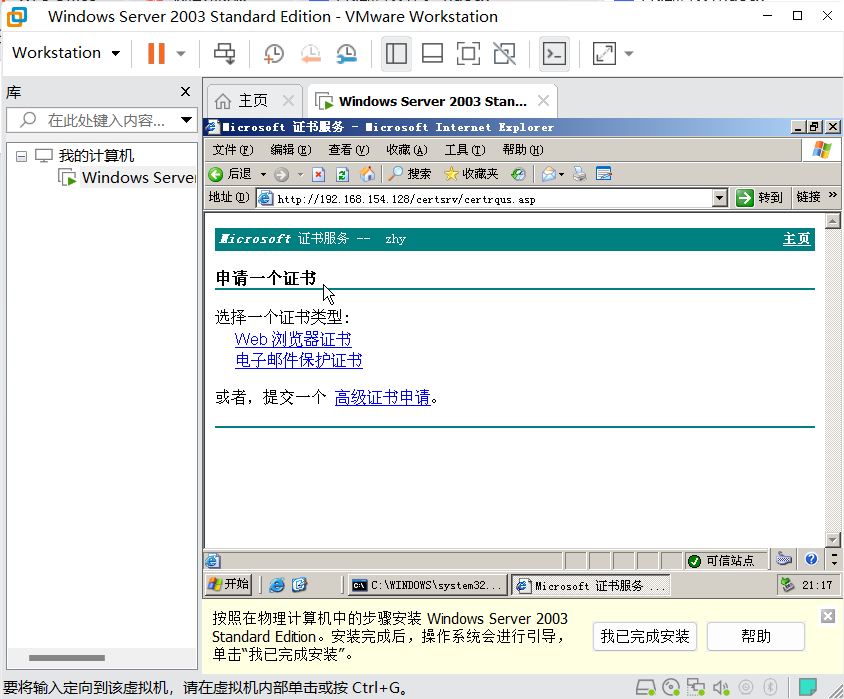
****

**在客户机中申请证书，这里以Windows XP作为客户机申请证书，在Windows XP中打开IE浏览器，输入<http://192.168.154.128/certsrv>**

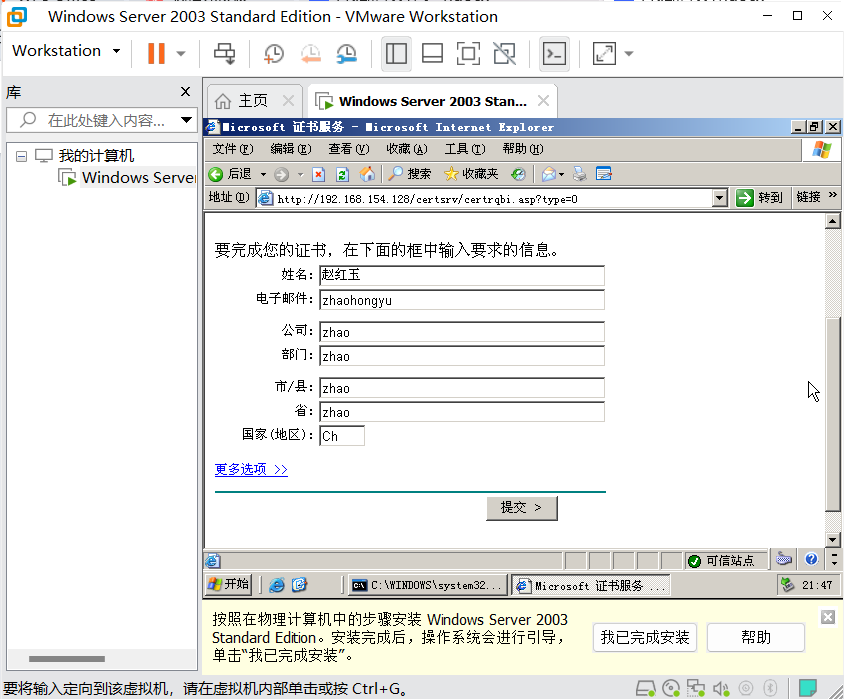
**出现如下界面。**

****

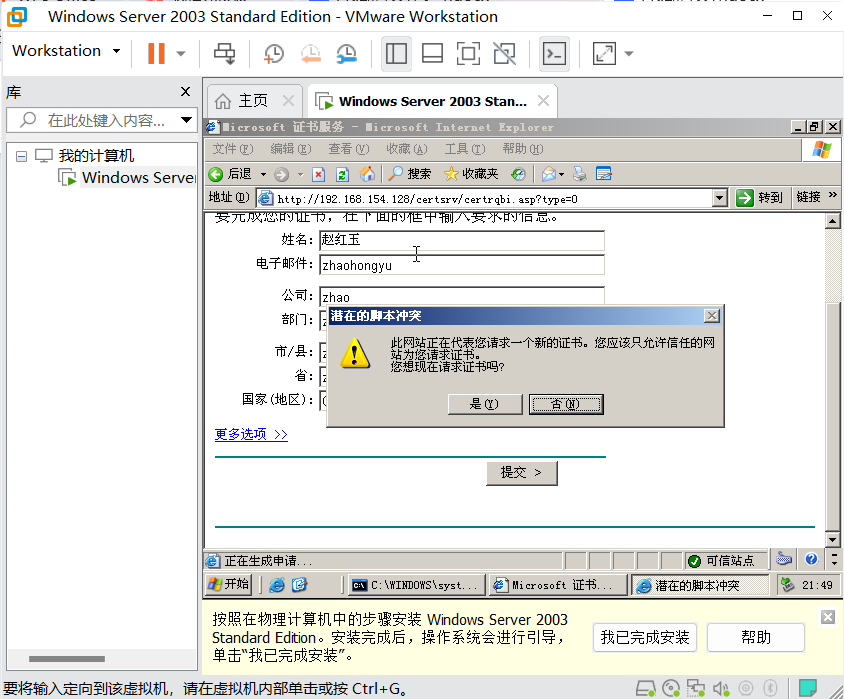
**在此界面选择 申请一个证书选项，在弹出的页面中选择【web浏览器证书】。**

****

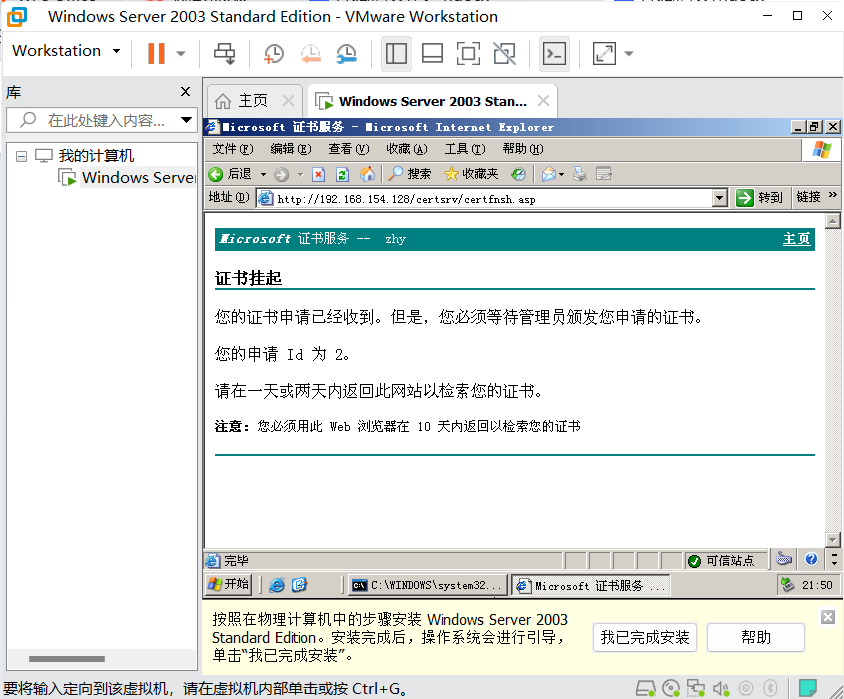
**在弹出的页面中填写相关信息，完成后提交。此时IE浏览器采用默认的加密算法生成公钥对，私钥保存在本地计算机中，公钥和用户信息发给CA服务器。**

****

**提交后，弹出提示框，单击【是】。**

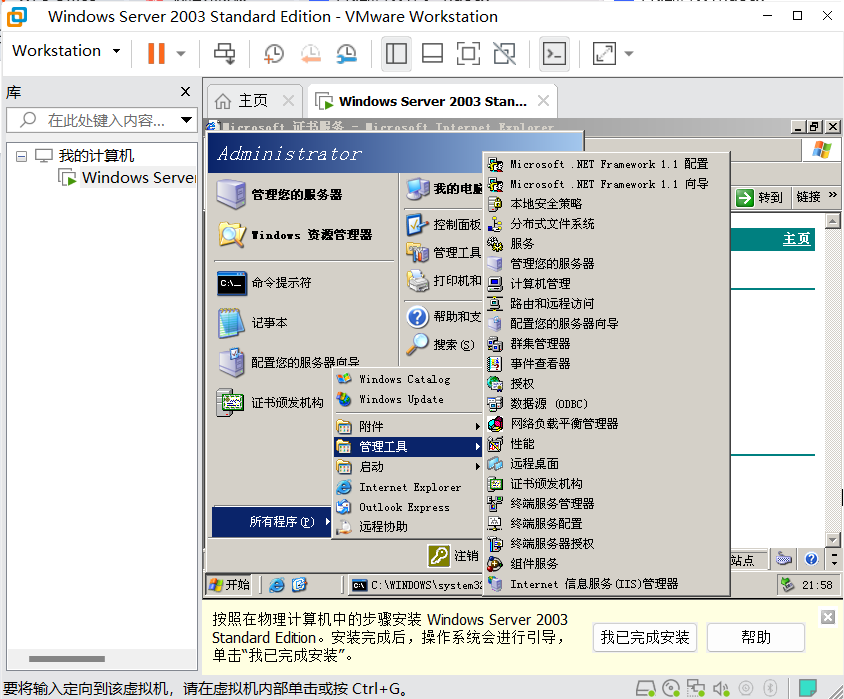
****

**客户端证书申请完成，等待CA服务器管理员颁发申请的证书。**

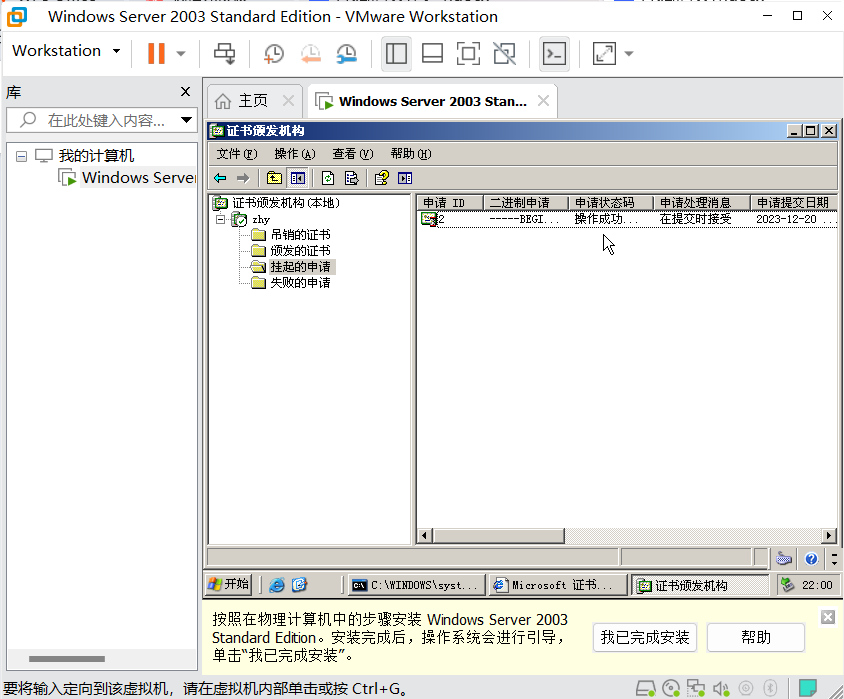
****

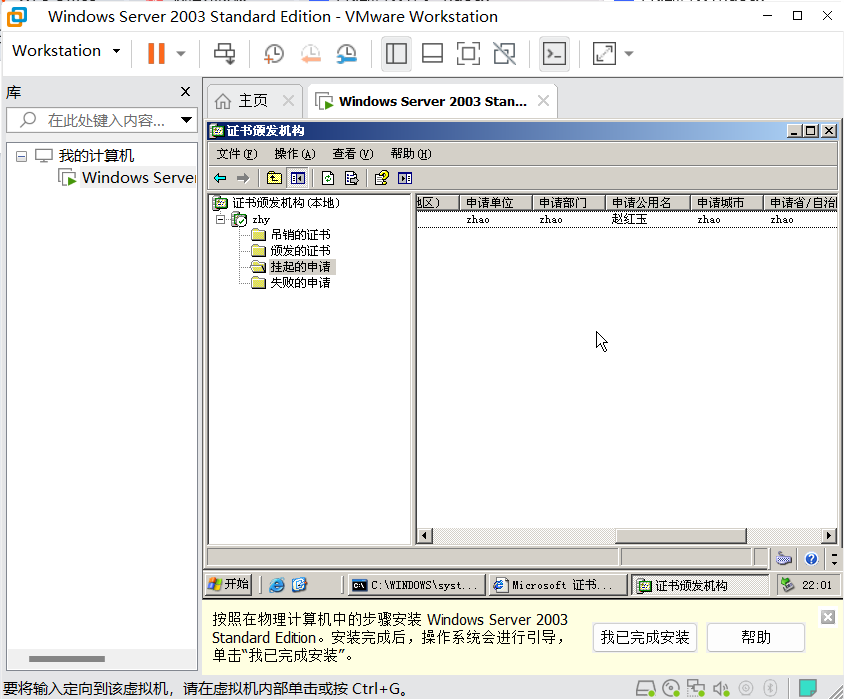
#### 证书发布

**在根CA服务器（Windows server 2003）上，选择【开始】->【程序】->【管理工具】->【证书颁发机构】。**

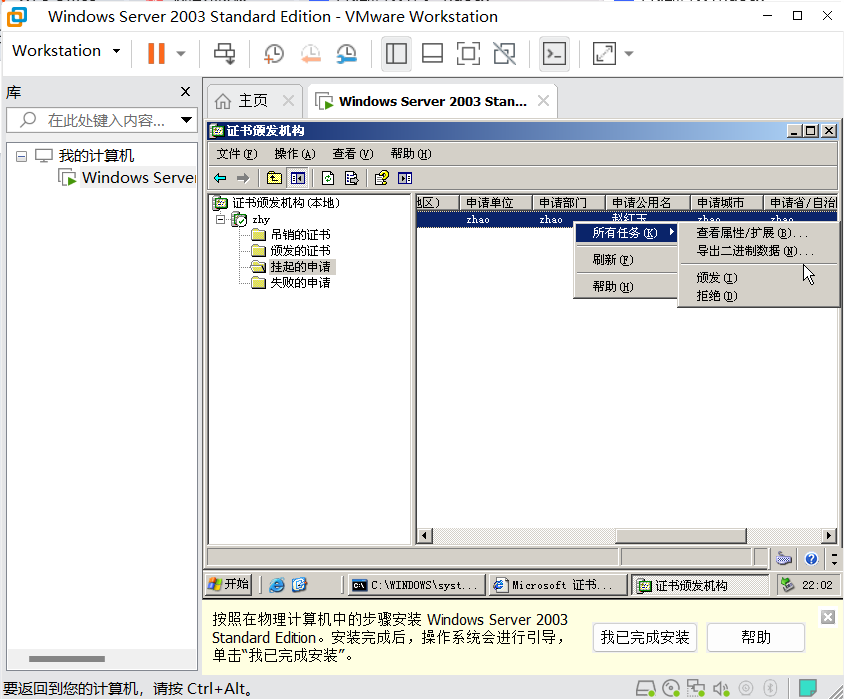
****

**在打开的窗口中选择【挂起的申请】，客户端申请的证书便会出现在窗口的右侧。**

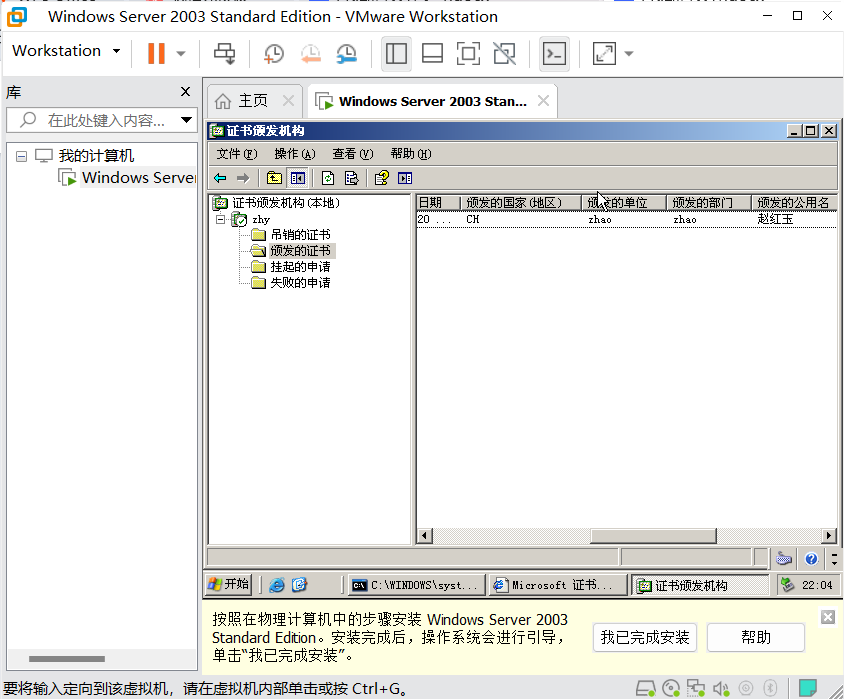
****

****

**右击刚才在客户端申请的证书，选择【所有任务】->【颁发】，进行证书的颁发。**

****

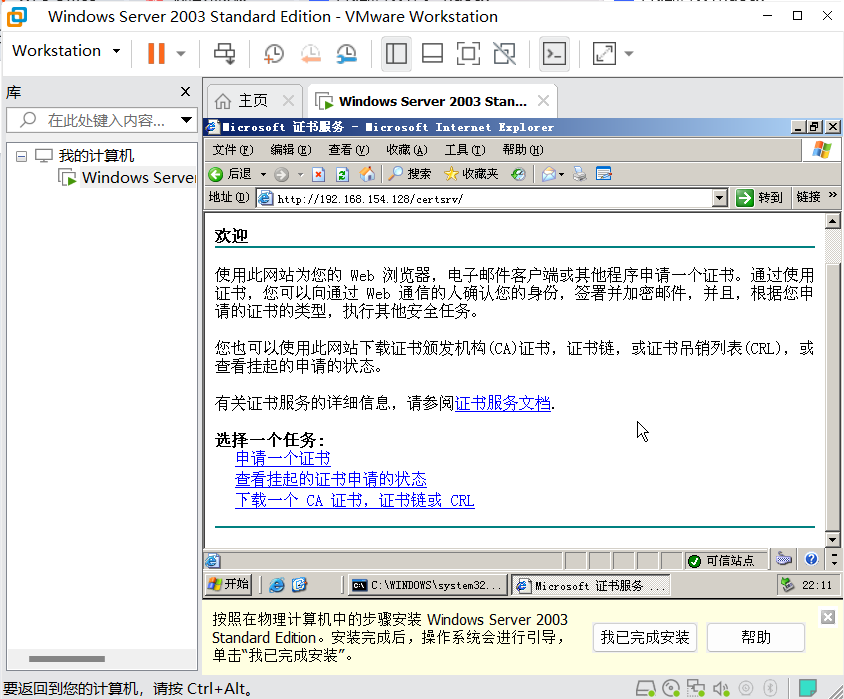
**颁发完成后，证书将转到【颁发的证书】文件夹中。**

****

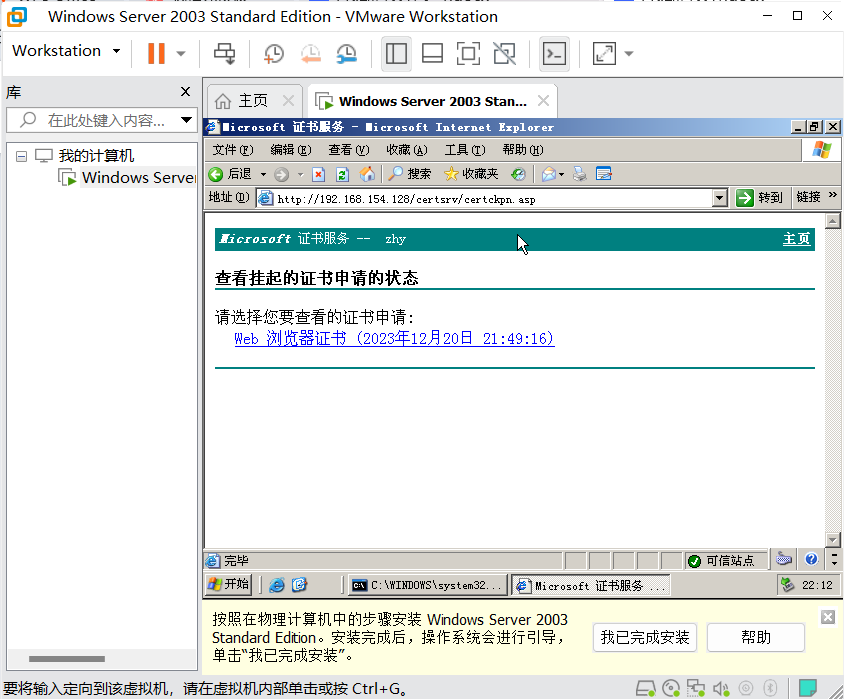
#### 证书的下载和安装

**在客户端（Windows XP）打开IE浏览器，输入<http://192.168.154.128/certsrv>**

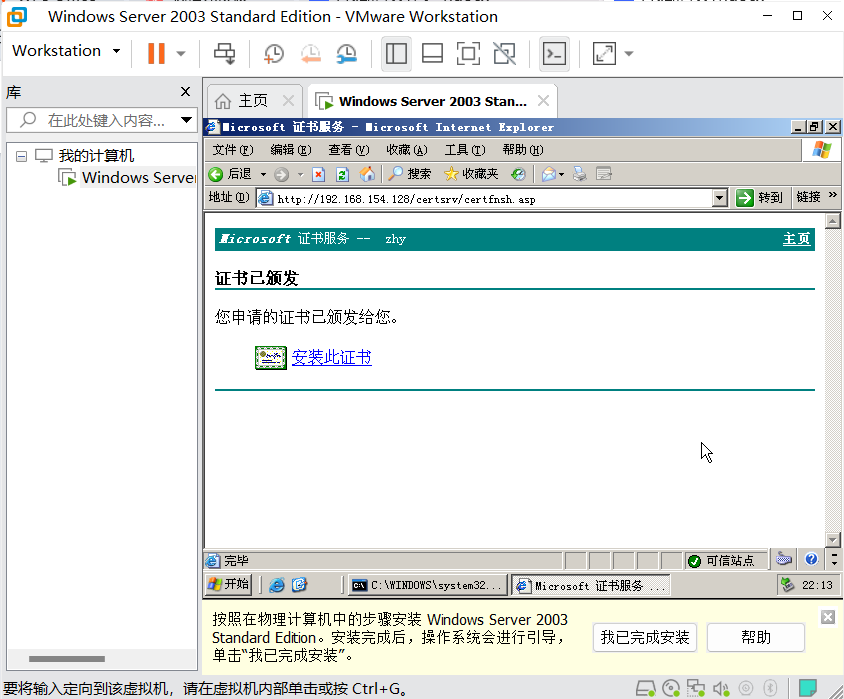
**进入证书申请界面。点击【查看挂起的证书申请状态】。**

****

**在弹出的页面中选择申请的证书**

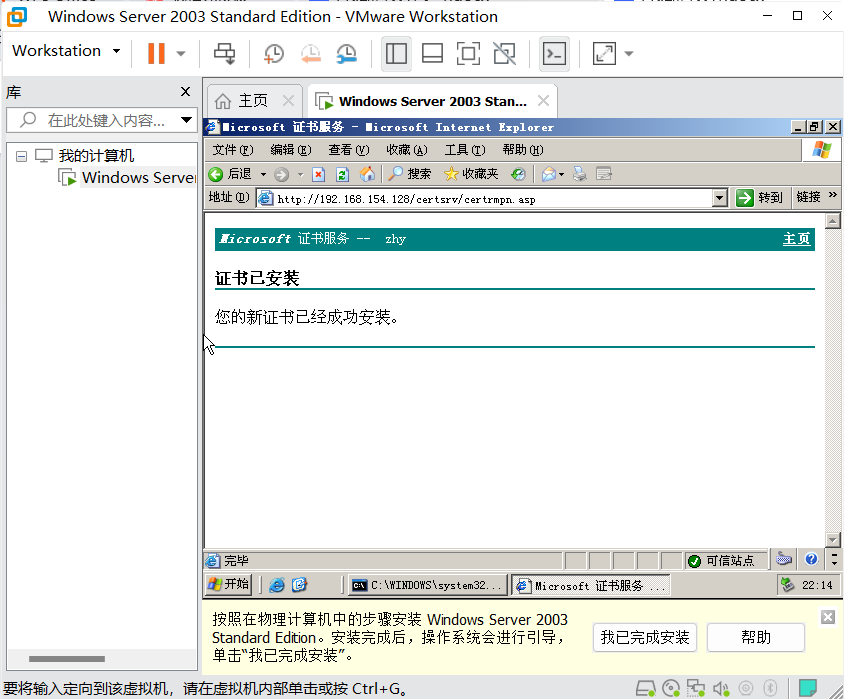
****

**如果CA服务器端证书颁发机构已颁发证书，则会弹出如下界面。**

****

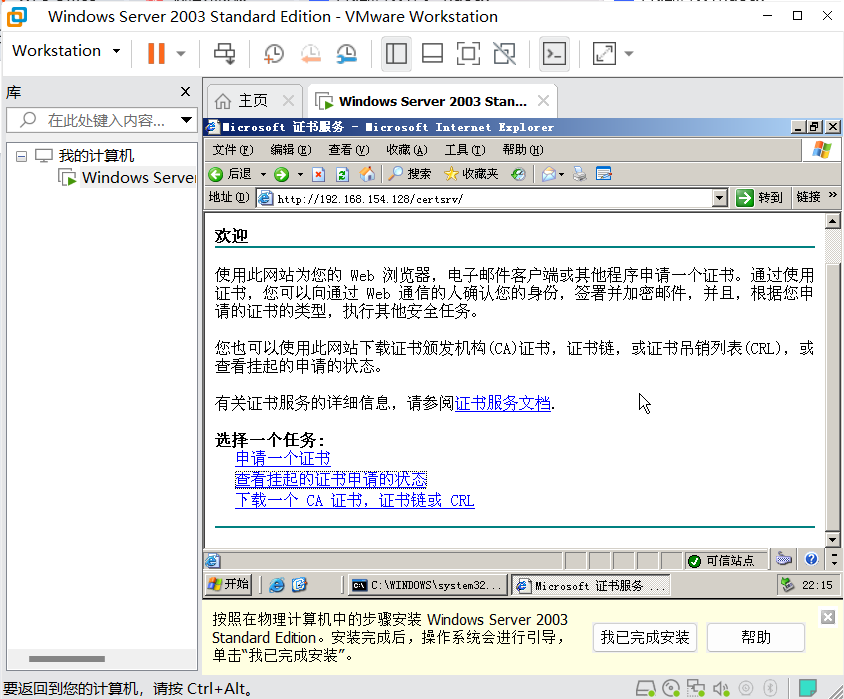
**单击【安装此证书】，系统弹出提示框，单击【是】**

**证书安装完成。**

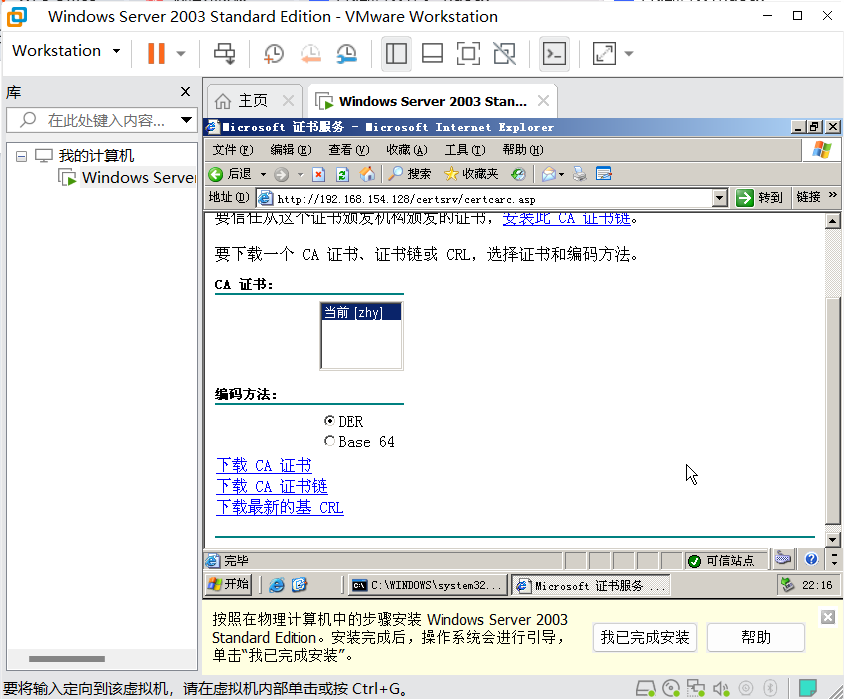
****

**接下来验证此CA颁发的证书是否可信任，为此需要安装CA系统的根证书，在IE浏览器中输入<http://192.168.154.128/certsrv>**

**点击【下载一个证书】。**

****

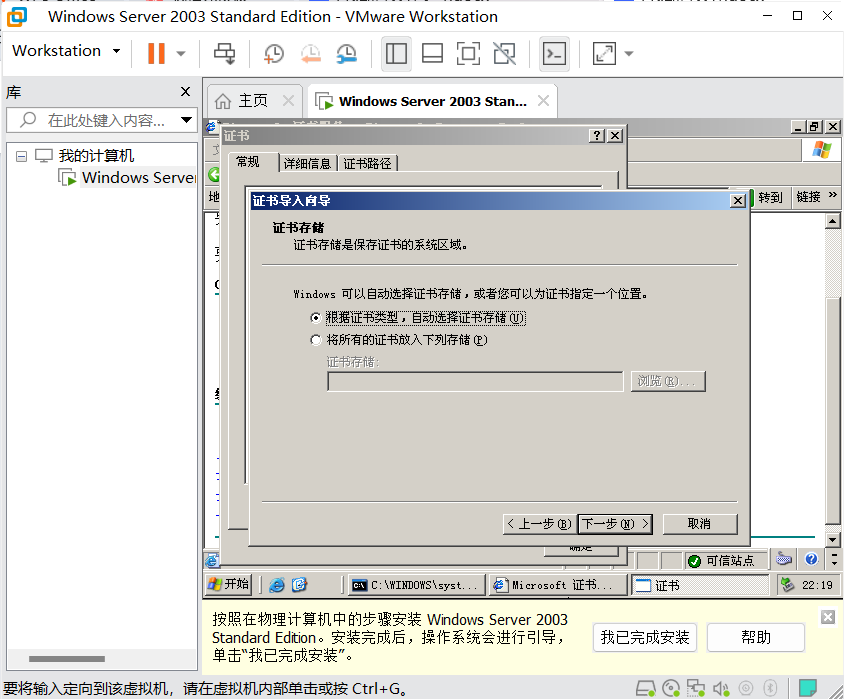
**选择当前的CA证书下载，并保存到合适的路径。**

****

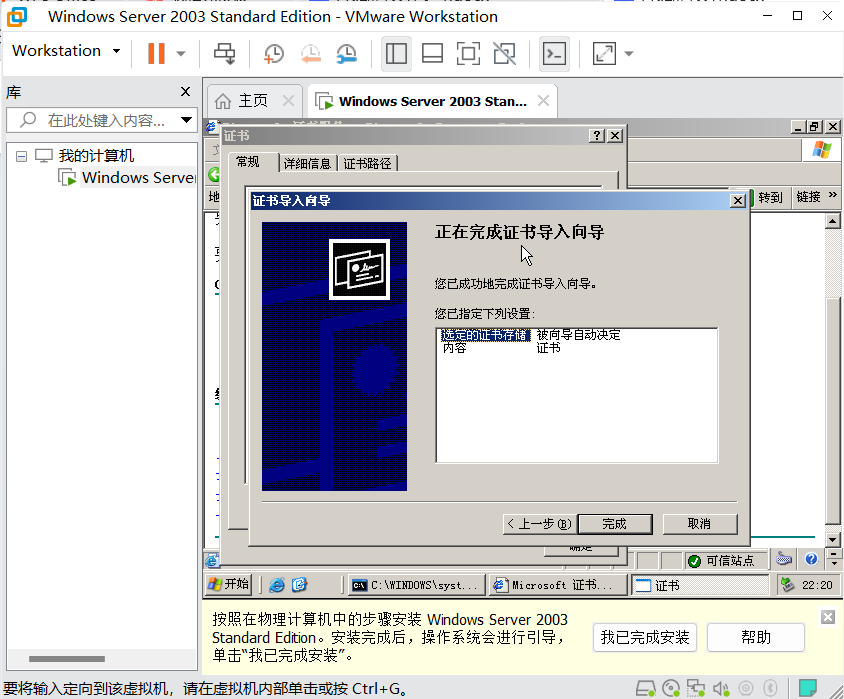
**下载完成后，在保存目录中查看证书信息，然后单击【安装证书】，进行证书导入，单击【下一步】。**

****

**选择证书存储位置，这里选择自动选择，单击【下一步】。**

****

**点击【完成 】，证书导入成功。**

****

****

## 五、实验结果分析及实验总结与体会

### 实验结果分析：

**1. 深入理解公钥基础设施（PKI）的工作原理：通过学习PKI的工作原理，对公钥加密、数字签名、证书颁发机构（CA）等概念有更深入的理解。能够解释PKI中的公钥和私钥的作用，以及如何使用证书和数字签名来实现身份验证和安全通信。**

**2. 熟悉CA证书的发放流程：在实验中，学习了CA证书的发放流程，包括创建和配置证书颁发机构、生成证书请求、证书审批和签名、证书下载和安装等步骤。了解证书的各个组成部分，并知道如何使用CA来确保证书的可信性和安全性。**

**3. 学习VMware虚拟机的安装与使用：通过安装和使用VMware虚拟机，熟悉了虚拟化技术的基本概念和操作。能够创建和管理虚拟机、安装操作系统、配置虚拟网络等。**

**4. 掌握Windows Server操作系统环境下CA中心的配置：在实验中，已经学会了在Windows Server操作系统环境下配置证书颁发机构（CA）。了解如何安装和配置CA服务、设置证书策略、管理证书撤销列表（CRL）等。**

**5. 练习CA证书的申请与安装：通过实验，已经练习了CA证书的申请、审批发放和下载安装的全过程。知道如何生成证书请求、提交请求给CA、审批和签名证书、下载证书并在相应的系统中安装证书。**

### 实验总结与体会：

**通过完成上述实验，获得了对公钥基础设施（PKI）和CA证书发放流程的深入理解。学会了使用VMware虚拟机搭建实验环境并安装Windows Server 2003操作系统。还掌握了在Windows Server 2003中配置证书颁发机构（CA）和IIS服务的技能。**

**在实验过程中，不仅学习了理论知识，还获得了实际操作的经验。了解了CA证书的申请、审批和安装过程，以及如何确保证书的安全性和可信性。这些知识和技能对于建立安全的网络通信和保护敏感数据至关重要。**

**通过实验，还发现了一些挑战和问题，例如配置CA服务时的复杂性、证书请求的生成和管理、证书的撤销和更新等。这些问题可以帮助进一步加深对PKI和CA的理解，并为未来的实际应用提供宝贵的经验。**

**总之，完成这个实验对PKI、CA和证书颁发流程有了更深入的理解，并获得了在Windows Server操作系统环境下配置和管理CA的实际技能。这些知识和技能对于网络安全和身份验证的相关工作非常重要。**