# CA系统应用实验

**【实验目的】**

(1）通过实验深入理解PKI系统的工作原理，了解数字证书和CA系统的主要功能和工作；

(2)通过运用SSH和SSL进行数据加密实验，使读者理解和掌握SSH和SSL的加密原理同时掌握对应用层协议进行安全传输的技术。

**【实验仪器】**

(1)需要安装Windows 2000 Server操作系统的一台计算机以及与其联网的一台Windows 2000计算机；

(2)SSH、SSL加密试验需要两台安装Windows 2000的计算机，一台作为服务器，一台作为客户端，通过网络连接。

**【实验原理】**

**(1)CA简介**

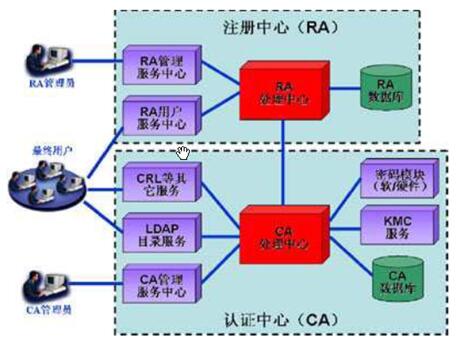
  一个典型的CA系统包括安全服务器、登记中心RA服务器、CA服务器、证书库服务器等。如图12-1所示。  


                  图12-1 CA系统示意图

   安全服务器用于保证用户进行证书申请、浏览、证书撤销列表查询，以及证书下载等过程中信息的安全性。CA服务器是整个CA系统的核心，负责证书的签发。出于安全的考虑，应将CA服务器与其他服务器隔离，确保认证中心的安全。登记中心服务器即RA，负责接收用户的证书申请并转发给CA，另一方面向证书库和用户转发CA颁发的数字证书和证书撤销列表。证书库服务器提供证书的目录浏览服务，其他用户通过访问此服务器就能够得到其他用户的数字证书。

②CA系统的主要功能

   CA系统的主要功能是对证书进行管理，包括颁发证书、废除证书、更新证书、验证证书、管理密钥等。

   对于加密要求不高的用户，密钥可由用户端生成，例如由浏览器或固定的终端应用产生，这样产生的密钥强度较小，不适合应用于比较重要的网络安全交易。对于比较重要的证书，密钥对一般由专用程序或CA之间产生，这样产生的密钥强度大，适合于重要的应用场合。在一个CA系统中，密钥的备份和恢复也是密钥管理中的重要一环。当用户密钥不慎丢失或者被破坏时，CA可以为用户及时恢复密钥。密钥的使用都有一定的期限，密钥到期后自动失效，所以密钥应该定时更新。在密钥泄漏时，也需要及时更新密钥，以保证证书应用过程中的安全性。  
**(2)Windows中CA系统**

   Windows 2000/2003的Server版本或者Enterprise版本，将PKI功能作为操作系统的一项基本服务，避免了购买第三方PKI所带来的额外开销。Windows 2000/2003中支持两种类型的CA：企业CA和独立CA。企业CA一般用于为一个组织机构内部并且属于同一个域的用户和计算机颁发证书，企业CA要求请求证书的用户在Windows 2000/2003活动目录中有配置信息。如果给以Windows 2000/2003域之外的独立用户颁发证书，一般安装独立CA。按照所处级别不同，Windows 2000/2003Server中又将CA分为：根CA和从属CA。根CA在这个组织的PKI中是最高级别的CA，也是最受信任的CA，它一般用于向从属CA颁发证书，从属CA是根CA的下一级CA。

**(3)SSH协议**

   传统的服务程序在传输机制和实现原理上没有在安全机制方面进行太多考虑，这些数据很容易被截获。此外，传统的网络服务业容易受到“中间人”攻击，因而在本质上是不安全的。

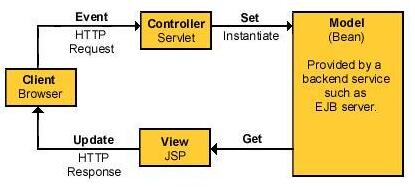
SSH是英文Secure Shell的简写形式，通过使用SSH可以把所有传输的数据进行加密。加密后“中间人”这种攻击方式就不能实现了，同时也能防止DNS欺骗和IP欺骗攻击。SSH协议的框架结构如图12-2所示。  


            图12-2 SSH协议的框架结构

 ①SSH的安全登录原理

 SSH支持两种安全登录认证方式。

a)基于口令的登录认证。

b)登录认证需要依靠密钥进行。

 ②SSH的加密通信原理

SSH的加密通信通过以下五个阶段来实现。

**① 协商SSH版本 ;**

**②  协商产生会话密钥;**

**③登录认证;**

**④处理会话请求;**

**⑤交互会话;**

**(1)SSL协议**

SSL是Secure Sockets Layer（安全套接层）的简写，它是由Netscape公司开发的，用来解决点到点数据安全传输和传输双方身份认证的网络安全传输协议。当访问某些网站时发现使用的是https协议，就是通过SSL协议在浏览器与Web Server之间建立了一个安全的连接。

 SSL协议的连接过程

 SSL协议的执行过程，即建立服务器和客户端之间安全通信的过程，共分6个阶段。

  ①客户端发送ClientHello请求，将它所支持的加密算法列表和一个用作产生密钥的随机数发送给服务器。

  ②服务器发送ServerHello消息，从算法列表中选择一种加密算法，将它发给客户端，同时发送Certificate消息，将包含服务器公用密钥的证书发送给客户端；该证书还包含了用于认证的服务器标识，服务器同时还提供了一个用作产生密钥的随机数。如果希望客户端提供数字证书，服务器向客户端发送CertificateRequest请求。最后，服务器发送ServerHelloDone消息以表示这一握手阶段的完成。

  ③如果服务器请求客户端提供证书，客户端将发送Certificate消息，将数字证书发送给服务器，服务器对客户端的数字证书进行验证，这个步骤是可选的。

  ④服务器证书发给客户端后，客户端对服务器的证书也进行验证，并抽取服务器公钥。客户端再产生一个pre\_master\_secret的随机密码串，并使用服务器的公钥对其进行加密，并将加密后的消息发送给服务器。

  ⑤客户端与服务端根据pre\_master\_secret以及客户端与服务器的随机数值，各自独立计算出会话密钥和MAC密钥。

  ⑥最后客户端和服务器彼此之间交换各自的握手完成信息，客户端向服务器发送类型为client\_finished的消息表示认证完成。服务器向客户端发送类型为service\_finished的消息表示认证完成。

  当上述连接步骤完成后，在服务器和客户端之间就建立起了可靠的会话，保证两者之间数据传输的安全性。

**【实验内容及步骤】**

**4.1实验步骤一：搭建实验环境**

* 实验平台拖出一台Windows2003 Server PC、一台WindowsXP PC以及Cisco Switch,两台PC通过交换机连接，实验拓扑图如下图12-1所示：

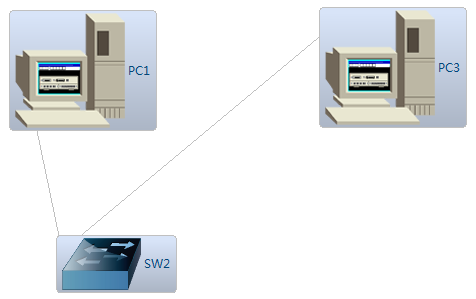


图12-3 实验拓扑图

②启动PC机以及交换机，PC机启动完成后，【网上邻居】->【属性】->【本地连接】->【属性】->【Internet协议（TCP/IP）】,配置IP地址；打开交换机配置界面，配置交换机端口IP地址，相应的IP地址如下表12-1所示：

|  |  |
| --- | --- |
|  | 分配IP地址 |
| Client | 192.168.1.64/24 |
| Server | 192.168.1.111/24 |
| Switch vlan1 | 192.168.1.100 |

* 打开交换机配置界面，配置交换机, Switch1中添加VLAN1，并且将ports3－5 添加到VLAN1中，具体命令如下所示：

Switch1:

enable

configure terminal

vlan database

vlan 1

exit

exit（全部退出再进入Config模式下）

    config terminal

interface range fa1/3  –  5

switchport access vlan 1

no shut

int  vlan 1

ip address 192.168.1.100 255.255.255.0

no shut

配置完成后，ping命令三者之间均可通。

**4.2 Windows环境下独立根CA的安装和使用**

4.2.1独立根CA的安装

单击“开始”按钮，选择“控制面板”→“添加和删除程序”，在弹出的窗口中选择“添加和删除Windows组件”。

在弹出的窗口中，选择“证书服务”，如图12-4所示。如果单击“详细信息”，这里面可以看到Windows所提供的CA和RA两个基本功能模块。单击“下一步”按钮开始安装。

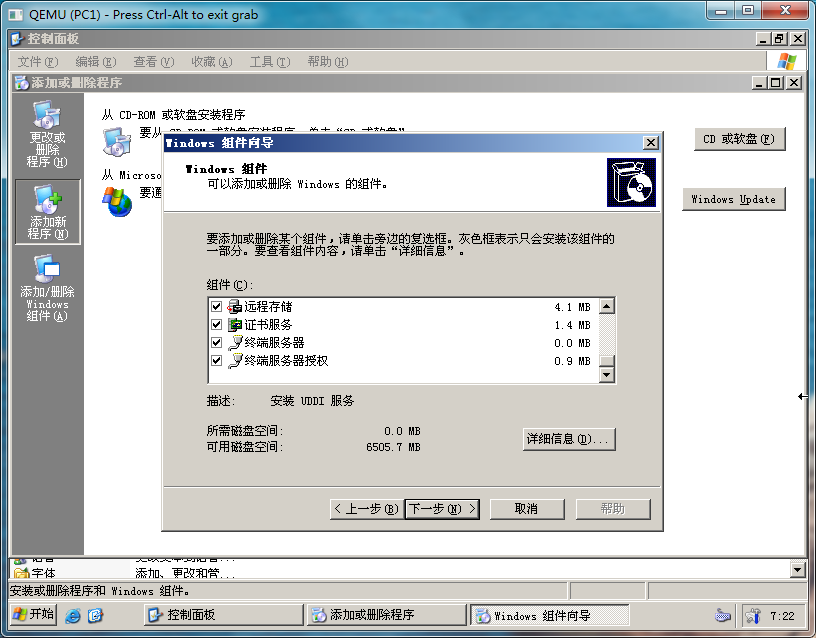


图12-4 安装Windows证书服务

   在弹出的配置窗口中，选择“独立根CA”，并单击“下一步”按钮，如图12-6所示。

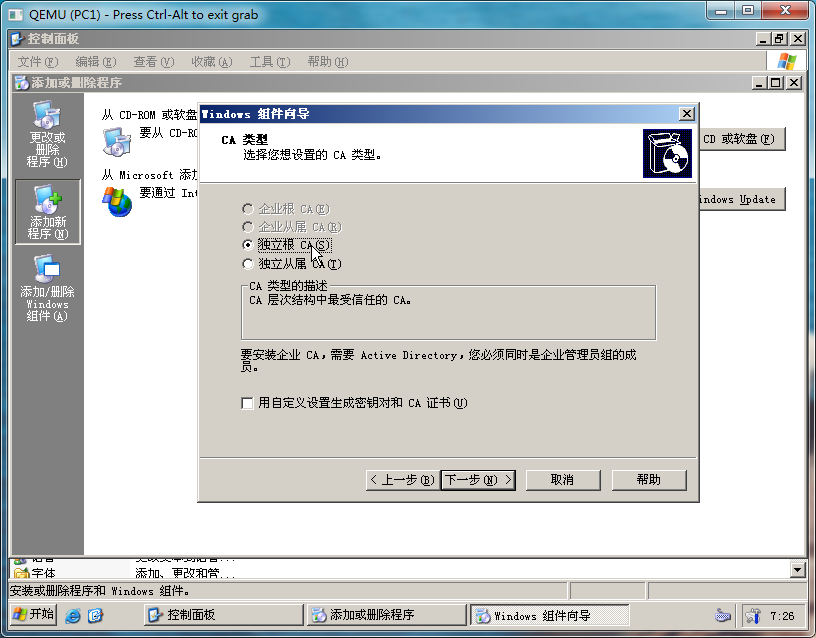


图12-6 独立根CA安装

   按要求依次填入CA的名称、单位、部门、城市、电子邮件、描述、有效期限，单击“下一步”按钮，如图12-7所示。



图12-7 证书服务安装

在弹出的窗口中填入数据的存放位置，单击“下一步”按钮，如图12-8所示。

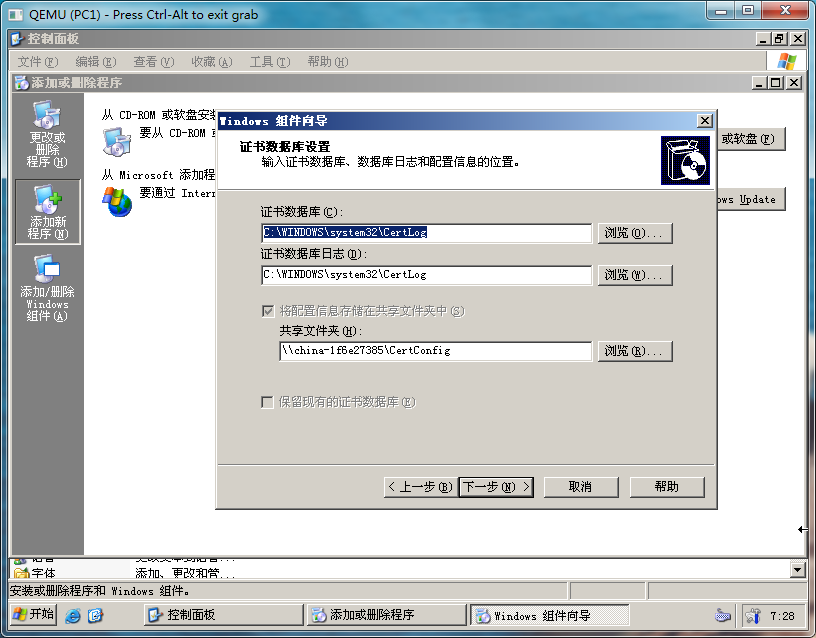
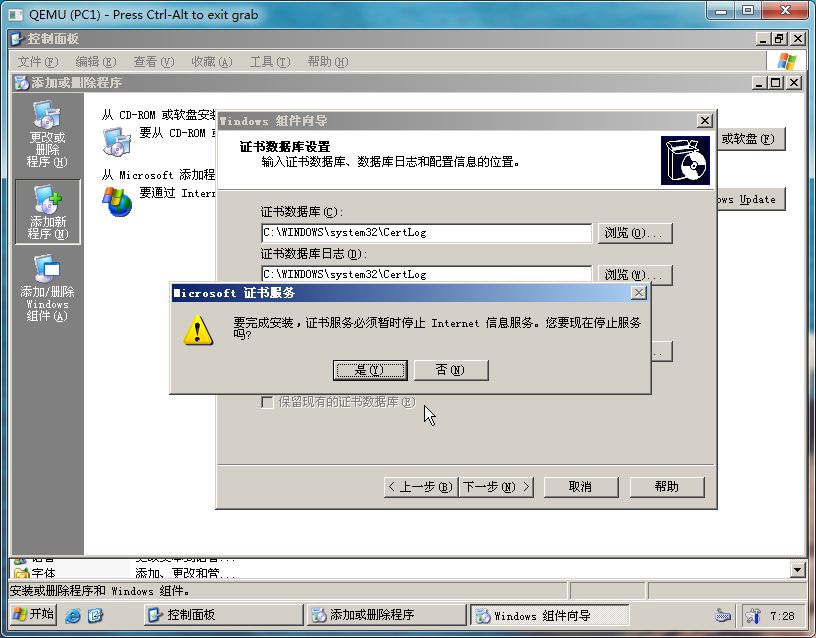


图12-8 “证书服务安装”的证书数据库位置选择

点击“下一步”，出现下图提示框，点击“确定”；出现进度条视图，配置完成后，点击“完成”。



安装完成后，单击“开始”按钮，选择“管理工具”，此时可在该菜单中找到“证书颁发机构”，说明CA的安装已经完成，如图12-9所示。



图12-9 CA安装完成示意图

我们已经为服务器成功配置完公用名为bupt的独立根CA，Web服务器和客户端可以通过访问该服务器的IIS证书申请服务申请相关证书。

 4.2.2 Windows CA 证书服务器配置(二) —— 申请数字证书

* 在客户端PC，首次启动IE浏览器需要配置局域网，配置步骤详见下图示，不再赘述。



图 12.10 Internet连接导向图示一

②申请数字证书

在IE地址栏中输入“http：//根CA的IP地址/certsrv”，正常情况下会出现证书申请页面。选中“申请一个证书”，并单击“下一步”按钮，如图12-14所示。

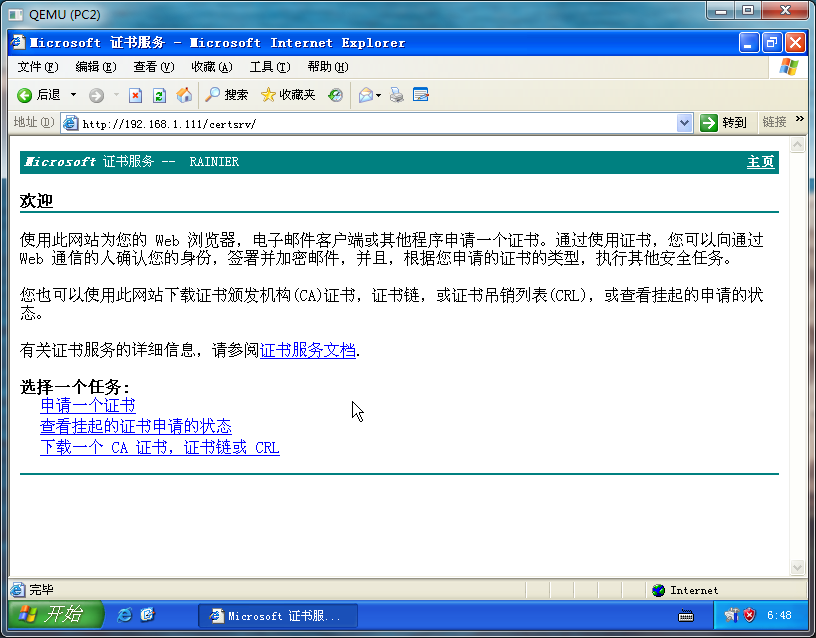


图12-14 Microsoft证书申请

在弹出的页面中选择“用户证书申请”中的某一用途的证书，如果证书用作客户端身份认证，则可点击‘Web浏览器证书’或‘高级证书申请’，一般用户申请‘Web浏览器证书’即可，‘高级证书申请’里有更多选项，也就有很多专业术语，高级用户也可点击进入进行申请。这里我们以点击申请‘Web浏览器证书’为例：

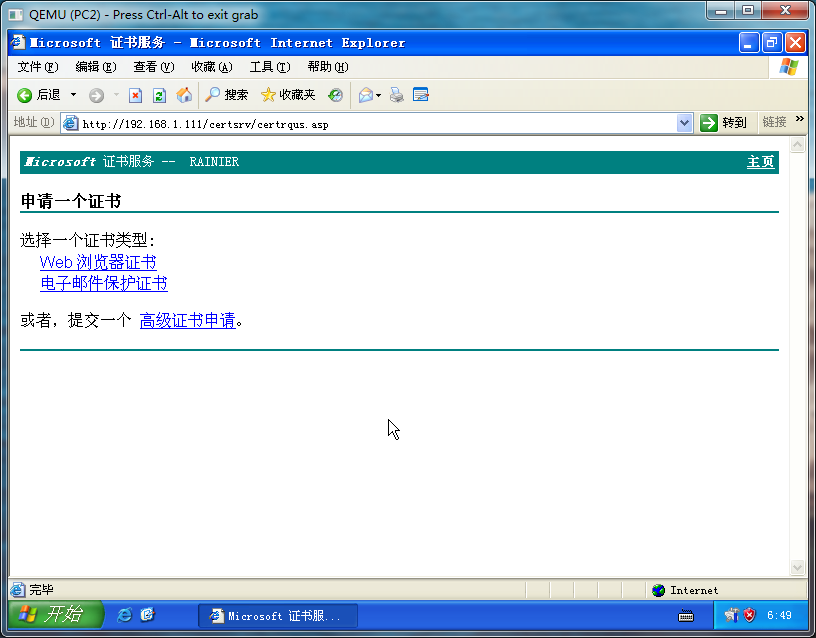


图12-15 申请Web浏览器证书

  申请‘Web浏览器证书’，‘姓名’是必填项，其他项目可不填，但由于CA服务器的管理员是根据申请人的详细信息决定是否颁发的，所以请尽量多填，并且填写真实信息，因为CA管理员会验证申请人的真实信息，然后进行颁发。需注意的一点是，‘国家（地区）’需用国际代码填写，CN代表中国。如果想查看更多选项，请点击‘更多选项’：



图12-16 Web浏览器证书标识信息

  默认情况下‘启用强私钥保护’并没有勾选上，建议将它勾选上，点击提交后就会让申请人设置证书的安全级别，如果不将安全级别设置为高级并用口令进行保护，则只要机器上装有该证书，任何人都可以用它作为认证，所以建议将证书设置为高级安全级别，用口令进行保护。以下将作相应操作，点击‘提交’：

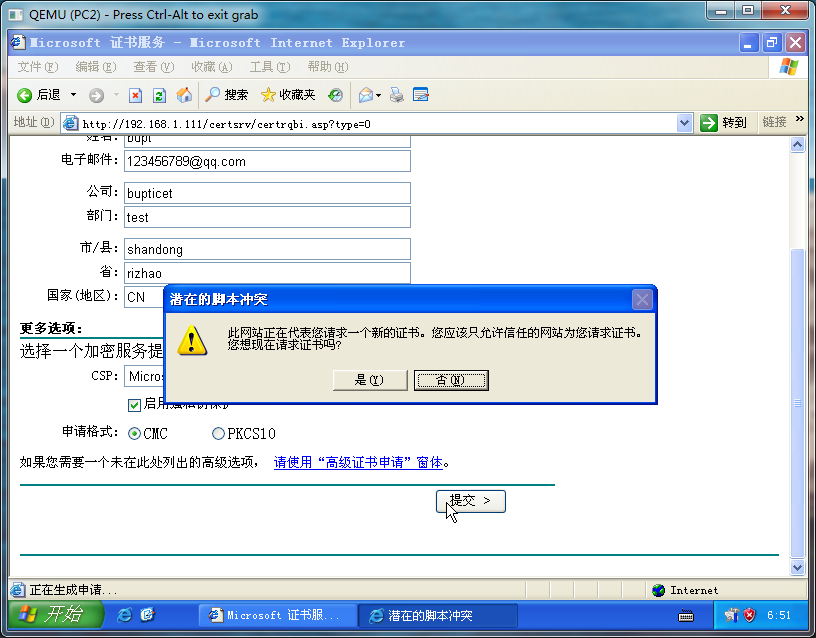


图12-18

单击‘是’后，单击‘设置安全级别’：



将安全级别设置为‘高’，单击‘下一步’后会弹出口令设置窗口：

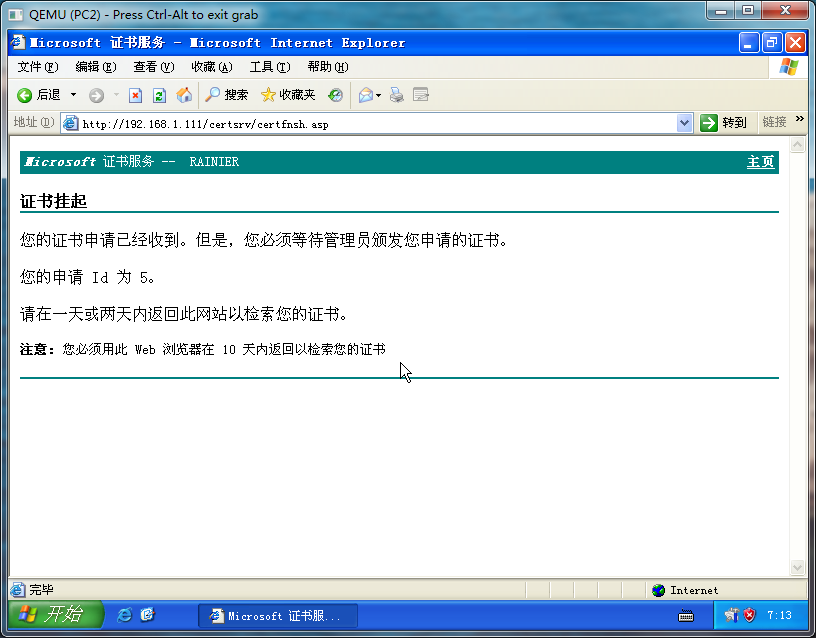


输入口令，对证书进行加密，并记住密码，因为在以后调用该证书的时候，浏览器会弹出输入密码的窗口。点击“完成”，如下图所示：



图12-19 证书申请成功示意图

单击‘确定’，浏览器页面跳向如下：



 4.2.3 Windows CA 证书服务器配置(三) —— CA 证书颁发

  在根CA所在的计算机上，单击“开始”按钮，选择“开始”→“管理工具”→“证书颁发机构”。在弹出的窗口左侧的菜单目录中选择“待定申请”，上一步申请的证书“bupt”出现在窗口右侧，如图12-20所示。

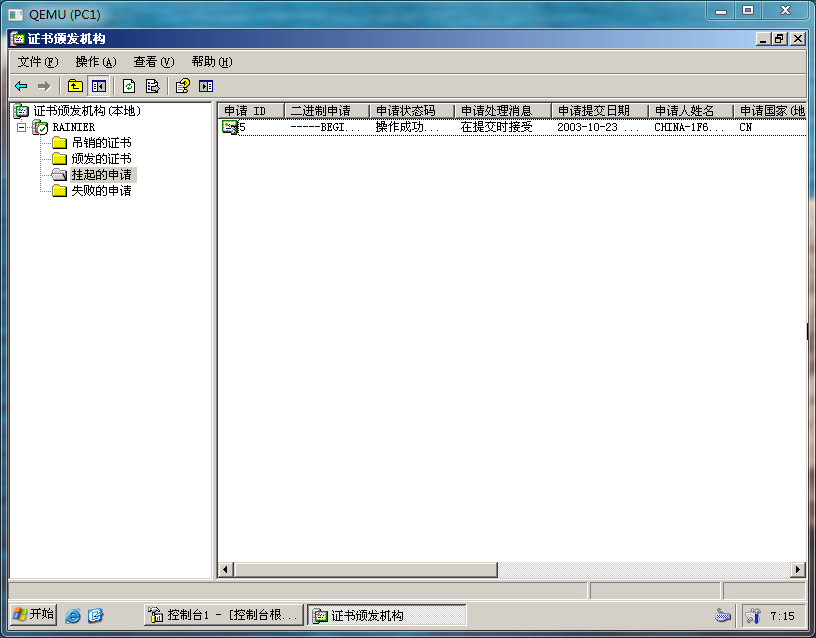


                   图12-20 待定申请的证书

选中证书鼠标右键，选择“所有任务”→“颁发”，进行证书颁发，如图12-21所示。

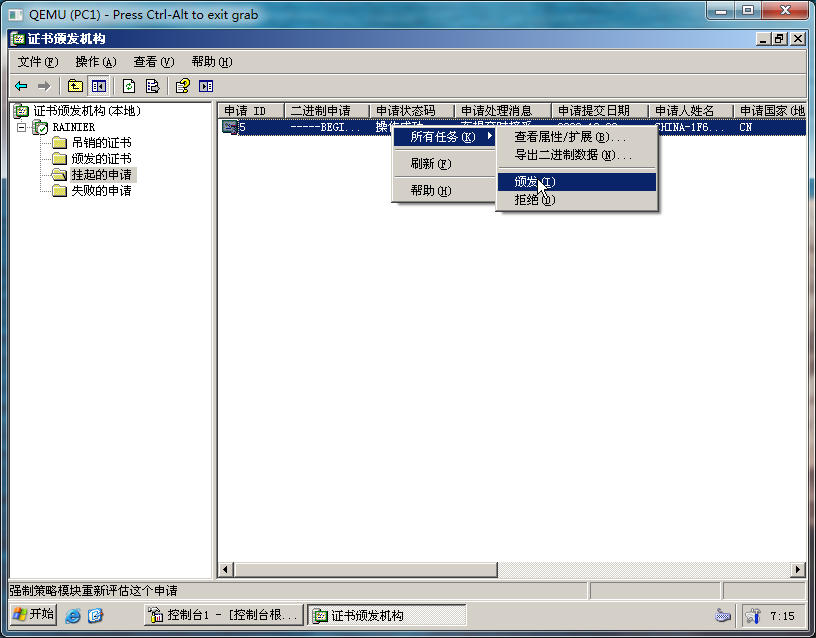


                     图12-21 颁发证书

 证书颁发后将从“待定申请”文件夹转入到“颁发的证书”文件夹中，标识证书颁发完成，如图12-22所示。

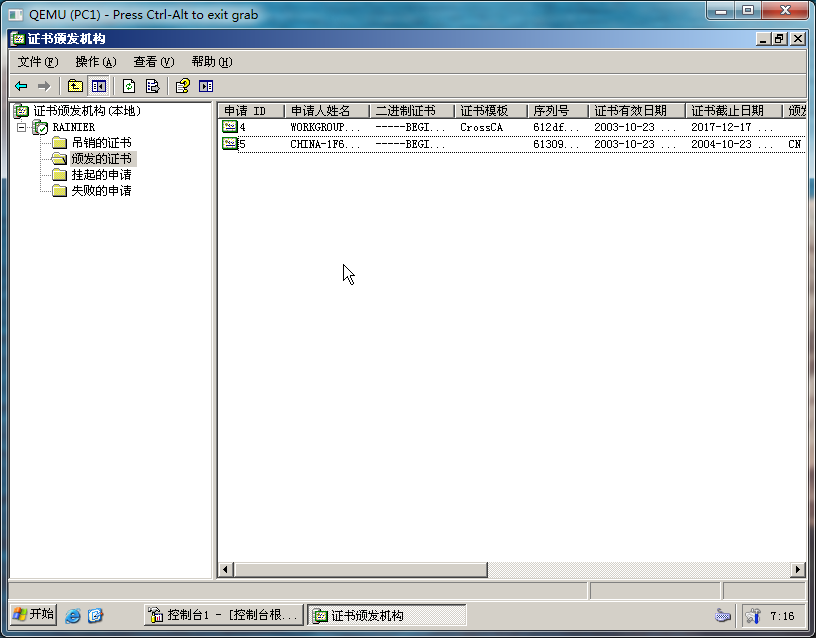


                     图12-22 已颁发证书

4.2.4证书的下载安装

  在申请证书的计算机上打开浏览器，在地址栏输入[http://域名/certsrv](http://xn--eqrt2g/certsrv)，进入证书申请页面。刚才完成了“申请证书”，下面选择“检查挂起的证书”，看看CA是否颁发了证书，如图12-23所示，点击下一步；

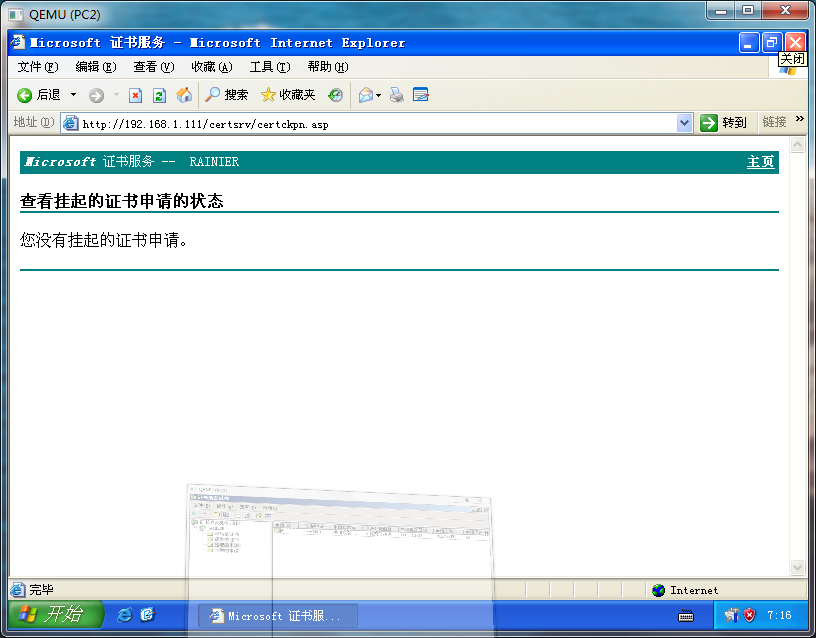


图12-23 检查挂起的证书

图12-26 安装证书

 在地址栏输入“域名/certsrv”，进入证书申请界面。选择“检索CA证书或证书吊销列表”，在弹出的窗口中单击“下载CA证书”超级链接，如图12-27所示：

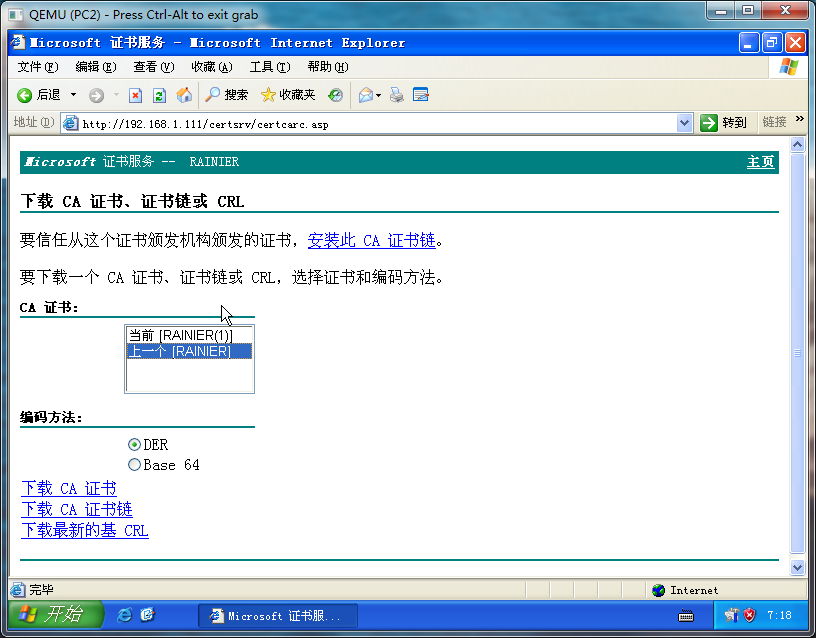


图12-27 下载证书示图

  在弹出的文件下载对话框中选择恰当的保存路径，将证书保存在本地。

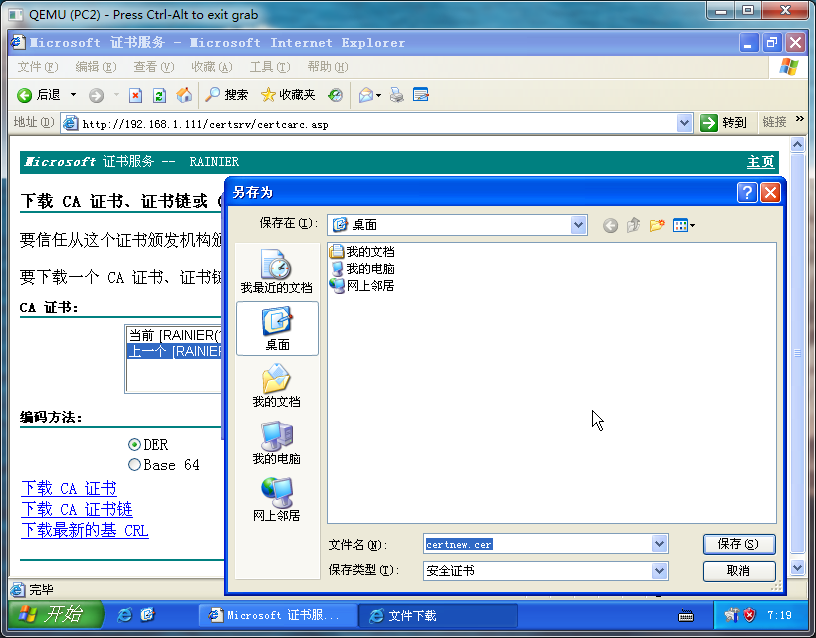


                图12-28 保存路径示图

 下载完毕后，在证书保存目录中双击此证书可查看证书信息，如图12-29所示。单击“安装证书”按钮，则进入证书导入向导，采用默认设置完成证书的导入，导入成功后， 单击“确定”按钮即可。

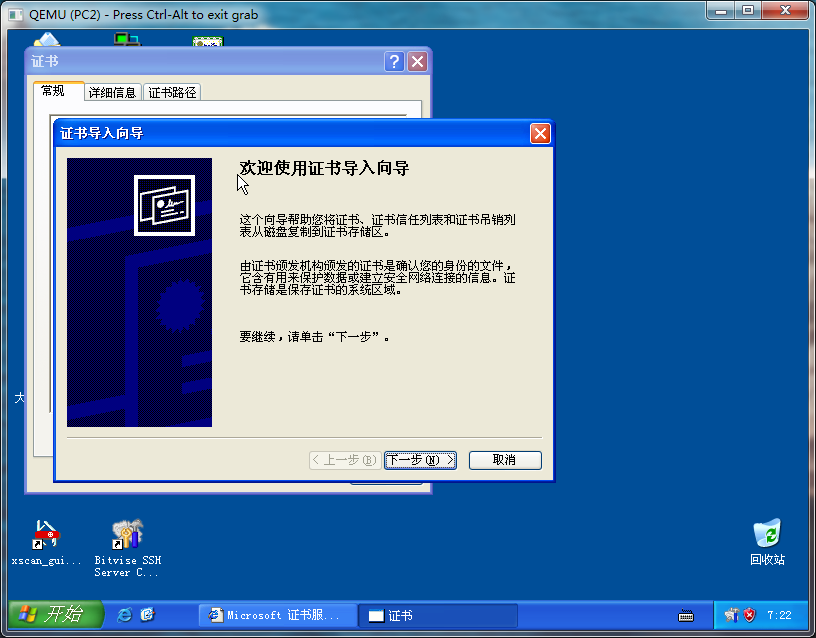


图12-29 证书信息

**4.3 实验步骤三：证书服务管理**

 在上面的证书发布机构菜单中，还有多项证书服务管理功能，下面通过操作，了解CA的管理功能。

 （1）停止/启动证书服务

进入“证书颁发机构”菜单，右击刚建立的CA节点，在“所有任务”中选择“停止服务”，即可停止服务，CA节点图标此时变成红叉；同样，单击“启动服务”，则可启动证书，如图12-30所示。

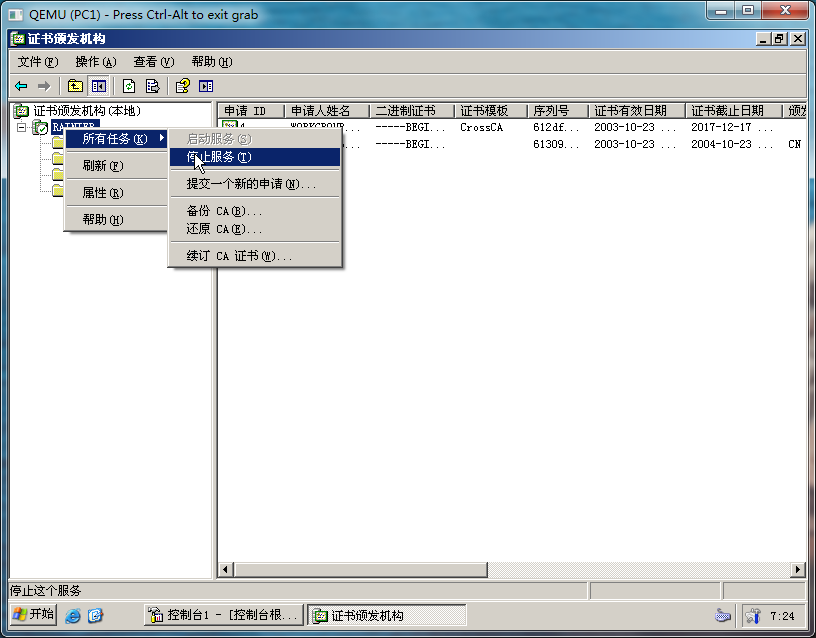
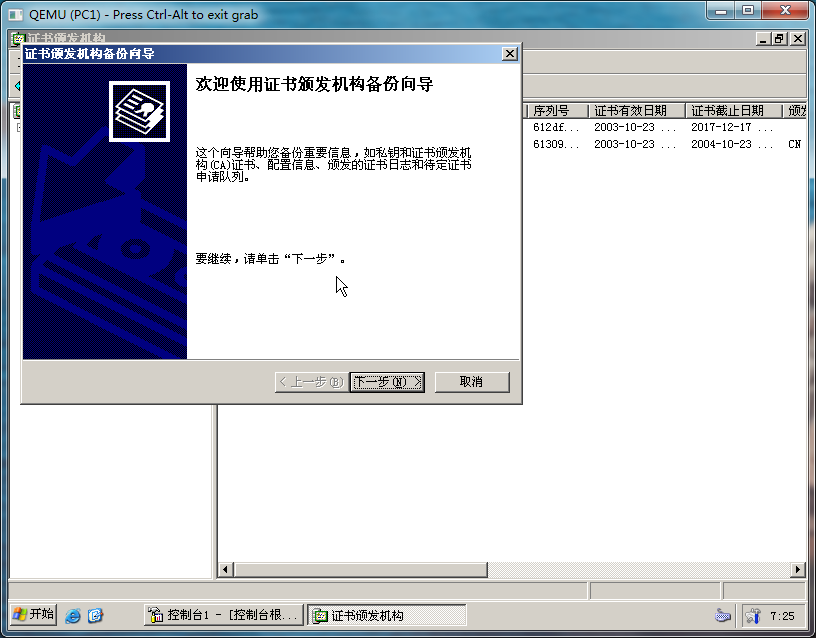


图12-30 停止证书服务

（2）CA备份/还原

 右击CA节点，在“所有任务”中选择“备份CA”，即进入“证书颁发机构备份向导”，如下图所示：



 单击“下一步”按钮，选择要备份的项目和要备份的文件夹，单击“下一步”按钮。如图12-31所示。

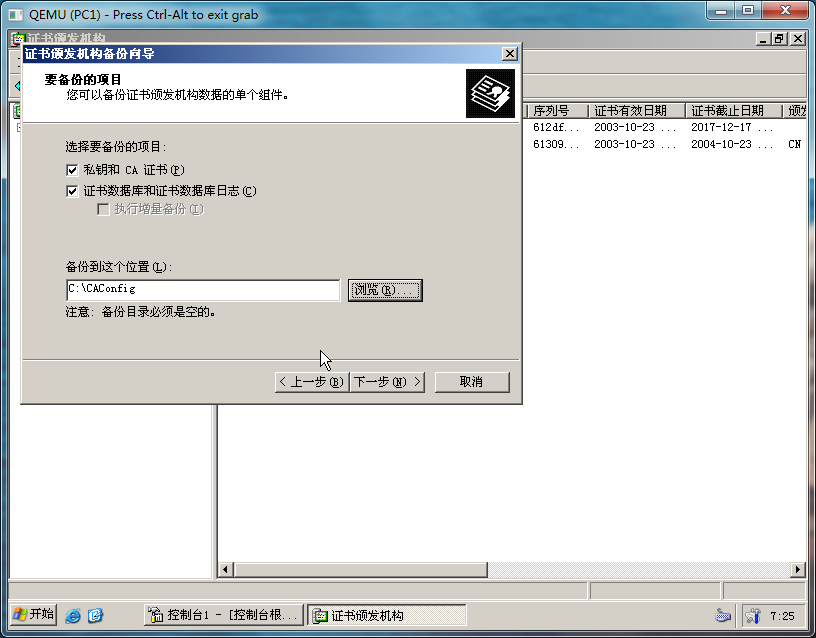


图12-31 证书备份

 为了保护私钥的安全性，接着要输入保护私钥和证书文件的秘密，如图12-32所示。然后点击下一步，即可选择完成操作。

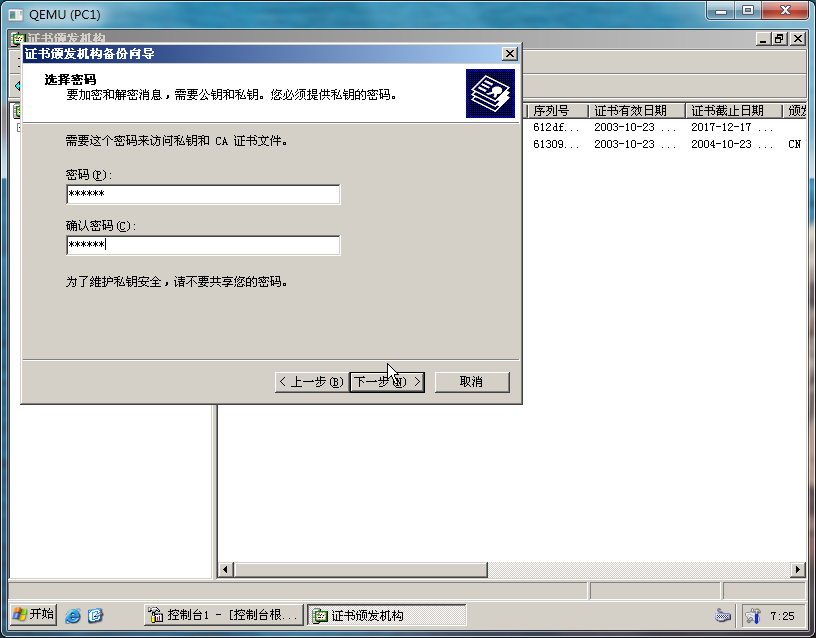


                 图12-32 为私钥提供密码

  CA的还原操作需要先停止CA服务，然后右击“CA公共名称节点”，在“所有服务”中选择“还原CA”，即进入“证书颁发机构还原向导”，单击“下一步”按钮，弹出如图所示的对话框，选择要还原的项目和证书文件所在的文件夹，单击“下一步”按钮。在出现的对话框中输入保护私钥和证书文件的密码，单击“下一步”按钮，单击“完成”，即完成CA的还原，如图12-33所示。

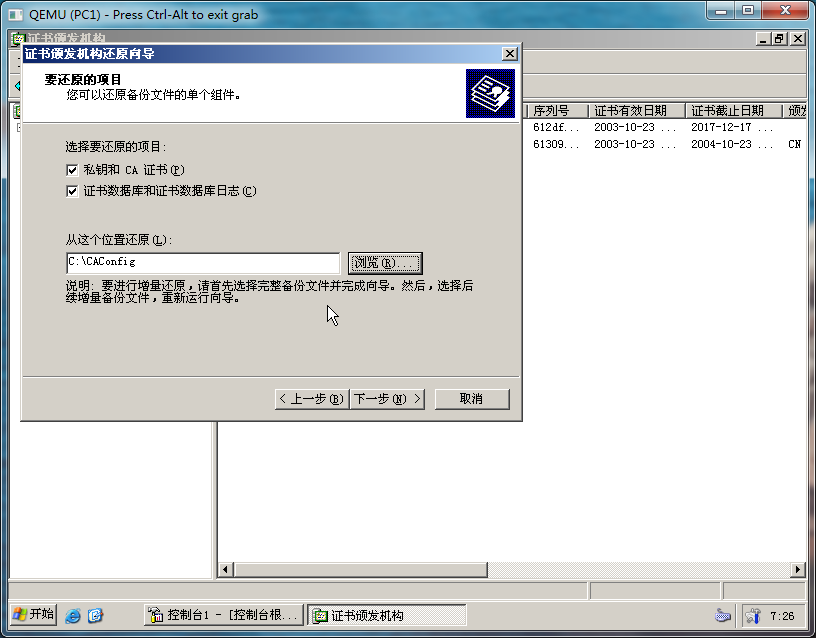


图12-33 CA的还原

（3）证书废除

右击“颁发的证书”中需要废除的证书，在弹出的菜单中选择“所有任务”中的“吊销证书”菜单项，如图12-34所示。在弹出的“证书吊销”对话框中选择吊销的理由，单击“是”按钮，这个被废除的证书就转移到了“吊销的证书”文件夹。

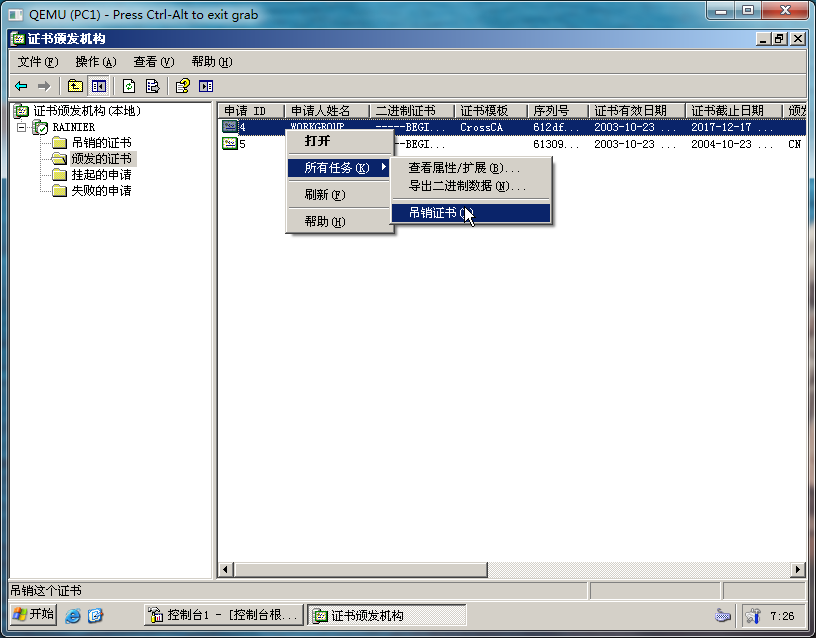


图12-34 吊销证书

 为了把吊销的证书对外发布，下面创建一个证书吊销列表，以供客户端下载查询。右击“吊销的证书”文件夹，在“所有任务”中单击“发行”，单击“是”，即可完成证书的吊销列表的创建和发布，如图12-35，图12-36所示。

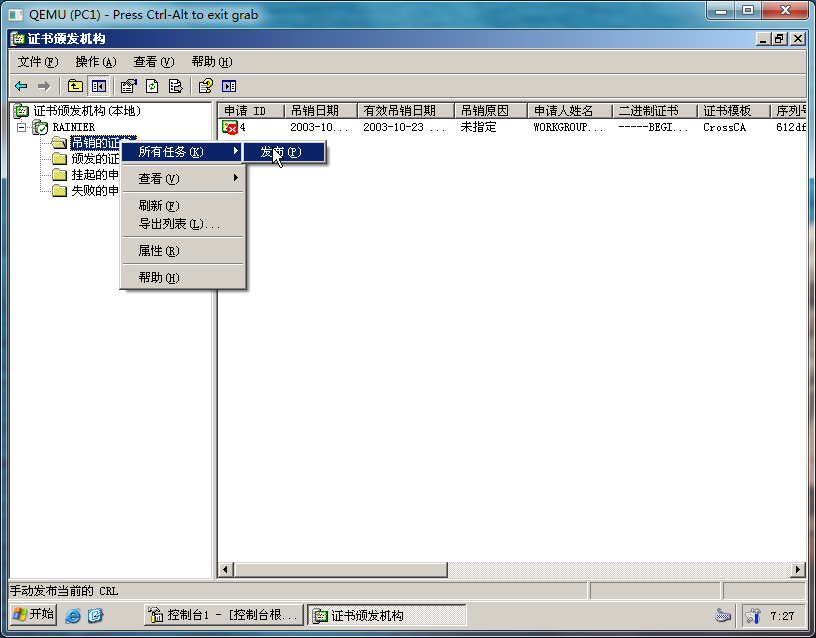


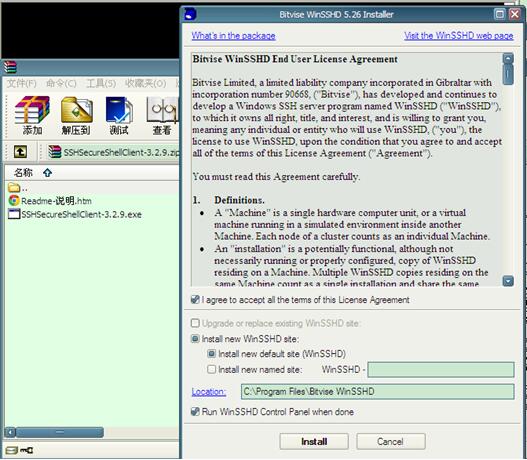
图12-35 创建证书吊销列表（1）

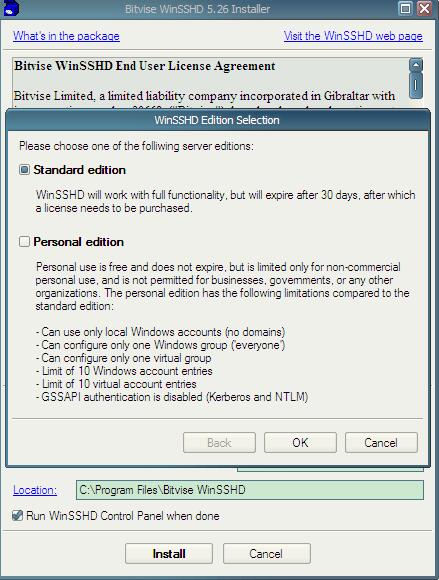
 如果要查看创建的证书吊销列表，右击“吊销的证书”文件夹，单击弹出菜单中的“属性”，弹出“吊销的证书属性”窗口，单击“查看当前CRL”按钮，则弹出“证书吊销列表”，如图12-31所示。在“常规”菜单中显示了证书吊销列表颁发者的信息，在“吊销列表”中显示了吊销的证书信息。

**4.4 SSH加密实验**

1. 配置SSH服务器

 选择一台计算机作为服务器，安装c软件，在安装时，它将自动产生用于加密信息的公钥和私钥对，并在安装信息中显示其公钥的MD5和BubbleBabble摘要值。





 安装完成后，在桌面上选择“开始”→“所有程序”→“Bitvise WinSSHD”→“WinSSHD Control Panel”命令，打开服务器端控制台。如图12-38所示。

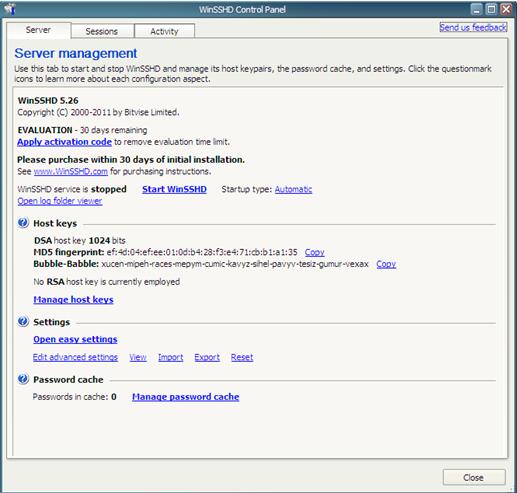
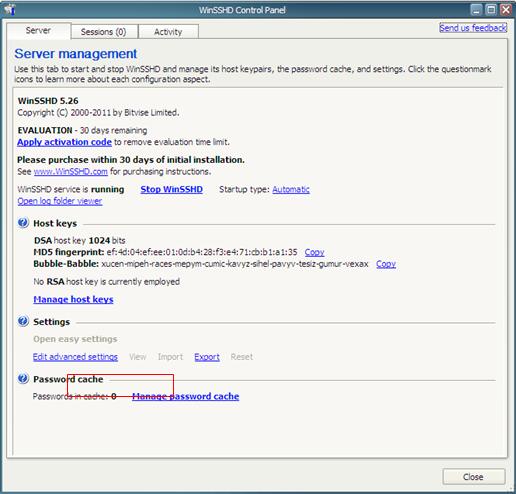


              图12-38 WinSSHD服务控制台

 在窗口中选择“Start WinSSHD”，开启服务。



 单击“Edit advanced settings”按钮，可查看并设置SSH服务端的参数。设置界面中包含了SSH服务监听的端口、日志、密钥交换算法、加密算法、完整性检验算法、压缩算法、实现对客户端访问控制的Windows组和用户信息、虚拟组合用户等。图12-34显示了可选的SSH支持的加密算法。

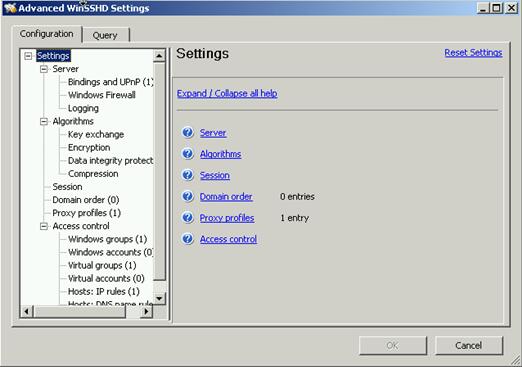


                图12-39 SSH支持的加密算法

 WinSSHD在安装时自动生成了公私钥对，选择控制台的“Manage Host Keys”可进入如图12-35所示界面，选择“Generate New Keypair”可生成新的密钥对。

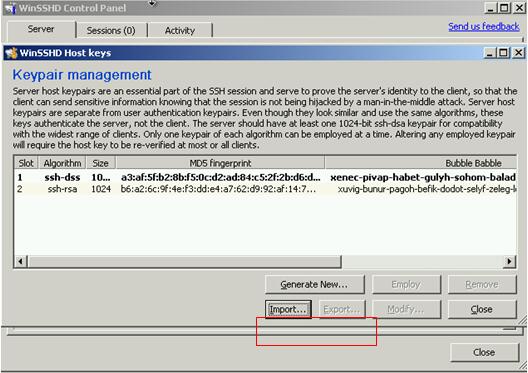


                 图12-40 产生新的密钥对

 4.4.2 配置SSH客户端

 选择一台计算机作为客户机，安装SSH Secure Shell客户端软件，安装完成后选择“开始”→“所有程序”→“SSH Secure Shell”→“Secure Shell Client”命令，打开SSH的客户端控制台，出现如图12-41所示界面。

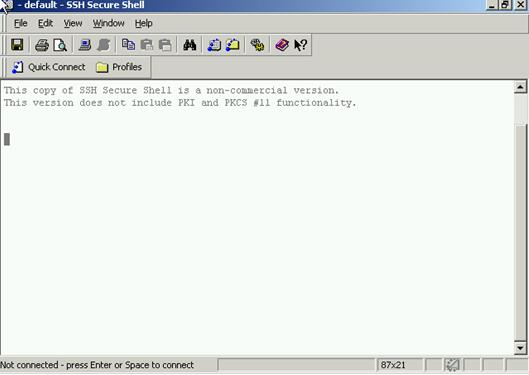


                图12-41 SSH客户端控制台

 单击SSH客户端界面“Profiles中的“Edit Profiles”选项，可以对客户端的参数进行设置。如图12-42所示。

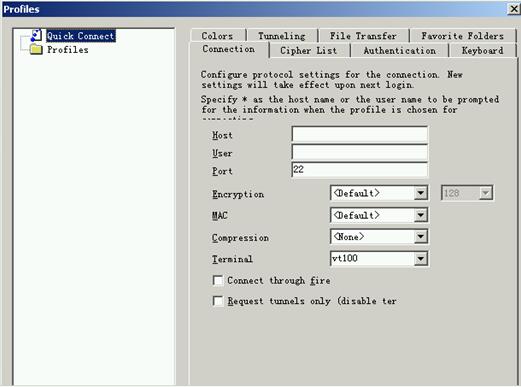


               图12-42 SSH客户端参数设定

 配置好参数后，单击“Quick Connect”选项，进行客户端与服务器的连接，如图12-38所示。在“Host Name”处填入SSH服务器的IP地址，在“User Name”处填入SSH服务器所在Windows操作系统的用户名，“Port”处填入SSH服务器的监听端口，“Authentication”选择默认选项，单击“Connect”，进行连接。在后面出现的Enter Password窗口中输入与User Name对应的登录密码。

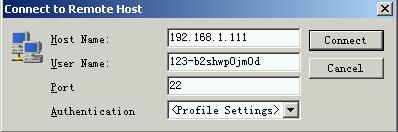
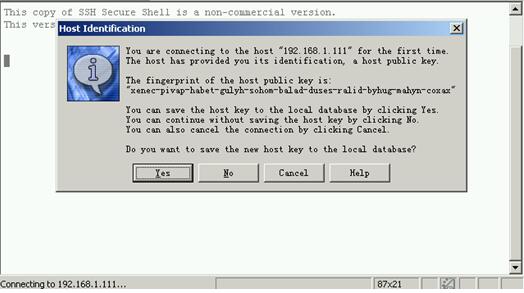


      图12-43 SSH客户端和服务器的连接出现提示框



SSH客户端将出现要求输入用户口令的窗口，输入用户口令后此口令将会以加密形式传给SSH服务器，如图12-44所示。



        图12-44 SSH客户端输入口令窗口

  单击“OK”后，SSH客户端将打开一个和SSH服务器连接的界面，可通过这个客户端界面对服务端的操作系统进行远程管理，例如输入dir命令，显示了服务器端的目录文件信息，

如图12-45所示。

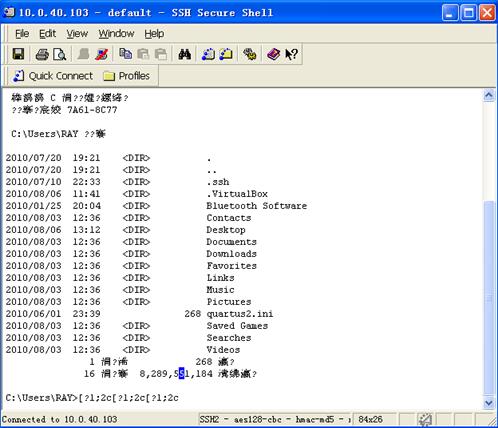


             图12-45 服务器端的目录文件信息

**4.5 配置基于Web的SSL连接**

1. Web服务器配置

单击“开始”按钮，选择“管理工具”→“Internet信息服务（IIS）管理器”。右击“网站”-à “默认网站”，选择“属性”，如图12-46所示。

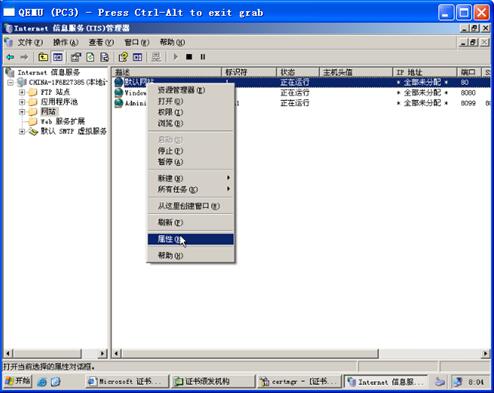


               图12-46 Web服务器证书申请

  在如下的窗口中选择“目录安全性”菜单，单击“安全通信”中的“服务器证书”。，如图12-47所示。



          图12-47 目录安全性

  在出现的欢迎使用Web服务器证书向导中，单击“下一步”按钮，如图，选中“创建一个新证书”，单击“下一步”。如图12-48所示。

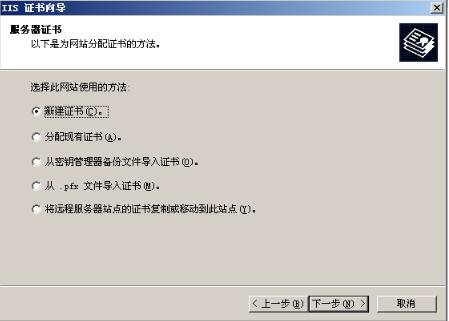


               图12-48 创建新证书

弹出提示对话框，单击“下一步”，如下图所示：



  在弹出的窗口中输入证书的名称，单击“下一步”按钮，如图12-49所示。



              图12-49 IIS证书向导

  根据窗口提示输入组织名和组织部门名，如下图所示：



单击“下一步”，输入站点的公用名称，单击“下一步”按钮，如图12-50所示。



           图12-50 选择站点的公用名称

  接着输入站点的地理信息，单击“下一步”按钮，如图12-51所示。



               图12-51 证书的地理信息

  接着输入证书请求文件的文件名和存放路径，单击“下一步”按钮。在这个证书请求文件中存放着刚才的用户信息和系统生成的公钥，如图12-52所示。



              图12-52 输入证书文件名

  出现确认窗口，单击“下一步”，接着单击“完成”按钮，完成服务器证书的申请，如图12-53所示。



               图12-53 完成申请

 接下来就是到CA的证书申请系统申请服务器验证证书。

 4.5.2 申请服务器证书

（1）在Web服务器的计算机上打开浏览器，在地址栏输入“http://根CA的IP/certsrv”，在出现的页面中选中“申请证书”，并单击“下一步”按钮。

（2）在弹出的页面中选中“高级申请”，单击“下一步”，高级申请可以由用户导入请求证书文件，将上面的证书请求文件通过这个界面提交，如图12-54所示。

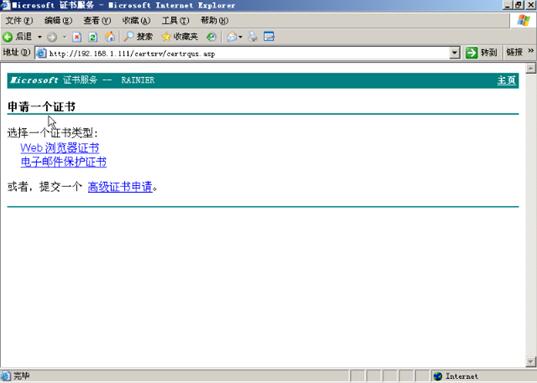


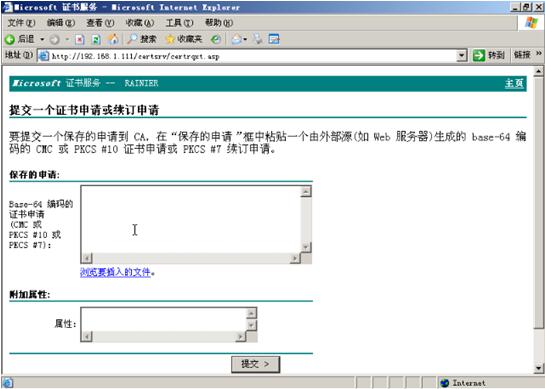
                      图12-54 选择“高级申请”

 （3）在弹出的页面中选中“Base64编码方式”，并单击下一步，如图12-55所示。



图12-55 选择“Base64编码方式”

（4）我们的用于申请的base64编码保存在一个名为certreq.txt的请求文件中。将其打开， 全选编码，并将其复制，粘贴到下图对应框中：



点击‘提交’：

（5）弹出如图12-56所示的页面，表示提交成功。我们已经向CA服务器发送证书请求信息，等待CA管理员对信息进行审核并颁发证书。

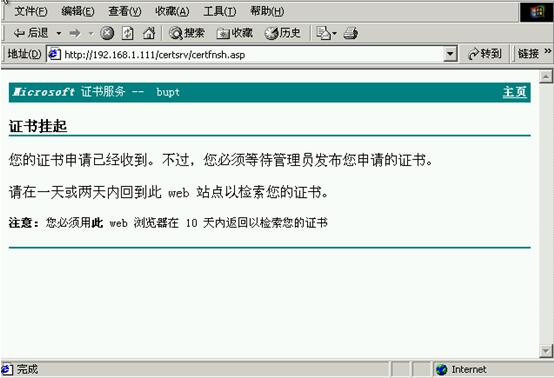


                   图12-56 申请提交成功

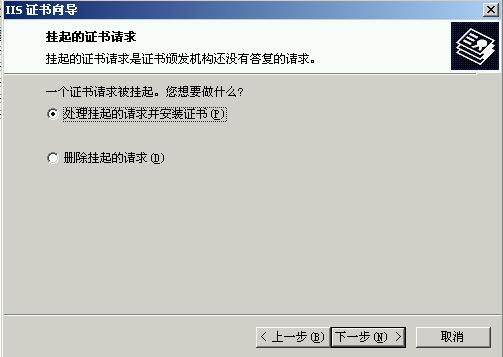
 （5）之后CA管理员审核证书信息后执行颁发，步骤和独立根CA实验的步骤一致；我们再次打开CA的证书申请系统，对证书进行下载和安装，步骤也同CA的，我们等一下要用到的就是该保存到本地的.cer文件。（如果有需要也可以将‘证书链’也下载，证书链里包含CA服务器的数字证书）

 （6）服务器以及客户机上申请、安装过程同CA的。

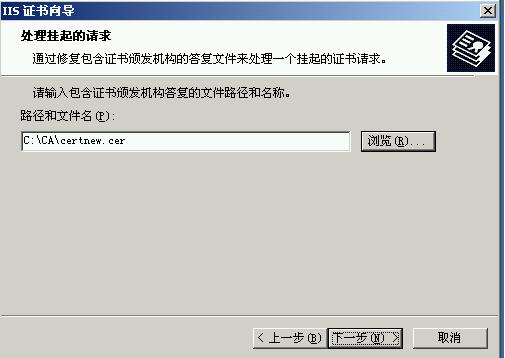
 1. 在服务器上配置SSL

（1）单击“开始”按钮，选中“管理工具”→“Internet服务管理器”。再打开的窗口里右击左侧菜单中的“默认Web站点”，选择“属性”。

（2）在弹出的窗口中选择“目录安全性”菜单项，单击“安全通信”中的“服务器证书”。进入“Web服务器证书向导”界面，单击“下一步”，处理挂起的证书：



（3）在挂起的证书请求页面中，选中“处理挂起的请求并安装证书”选项，单击“下一步”，在处理挂起的请求页面中，选择刚下载的证书文件目录及其文件名，



单击“下一步”，会显示证书目录，如下图所示：





然后单击“完成”。

通过此步，可将刚申请的Web服务器端的证书导入到IIS中，用于支持SSL协议。

 （4）选择面板上“安全通信”中“查看证书”项，如图12-57所示。



              图12-57 证书详细信息

 （5）单击“确定”按钮后返回到“目录安全性”面板，选择“安全通信”中“编辑”项，如下图所示：



 （6）选中“申请安全通道（SSL）”，这将在此Web服务器中启用SSL协议进行加密。在“客户证书”栏中选择“接受客户证书”，单击“确定”，如下图所示：



                 图12-58 选择“申请SSL”

（7）返回“目录安全性”面板，单击“确定”，完成配置。

4.5.4 客户端通过SSL与服务器建立链接

在客户端计算机上打开浏览器，输入“http://根CA的IP/certsrv”,提示“该网页必须通过安全频道查看”，要求采用HTTPS协议连接服务器。再次输入“https://根CA的IP/certsrv”，单击“确定”，完成了基于SSL的连接。