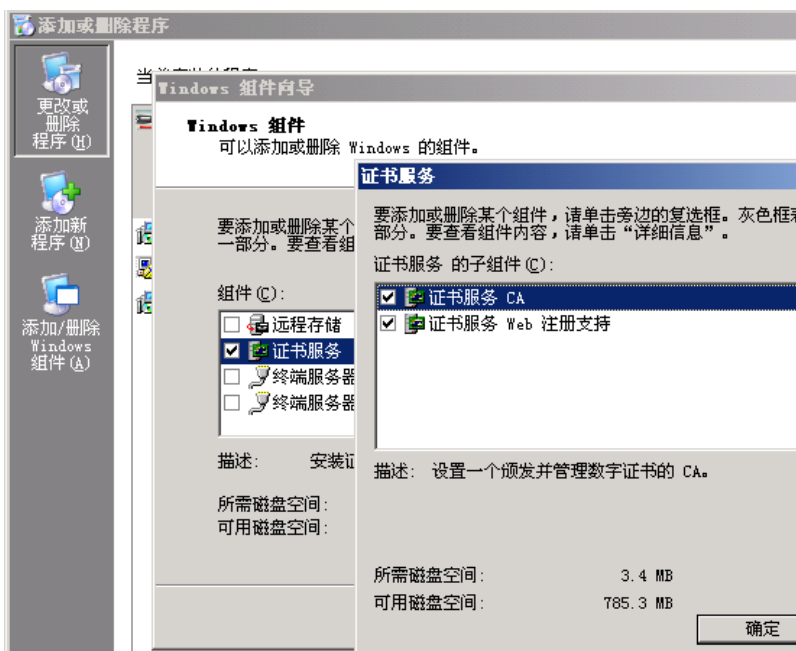
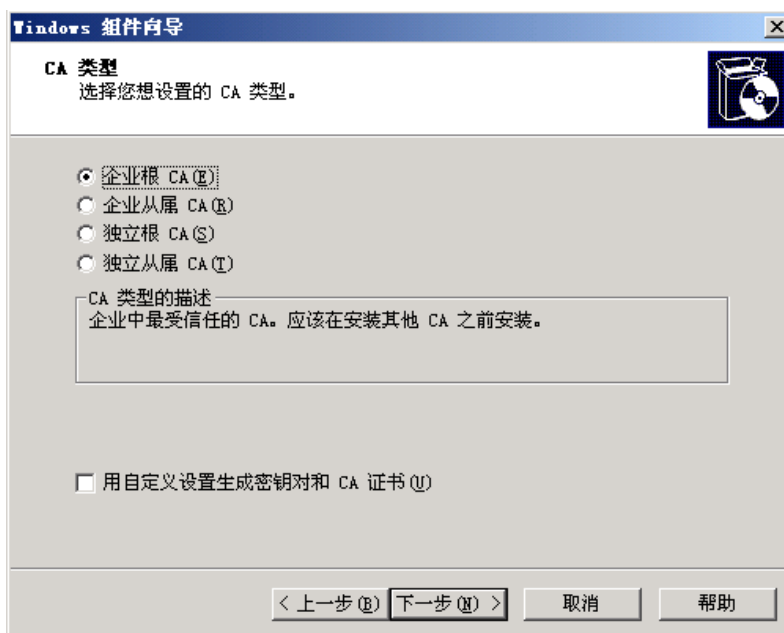


使用 USB Key 登录 Windows 域的配置方法

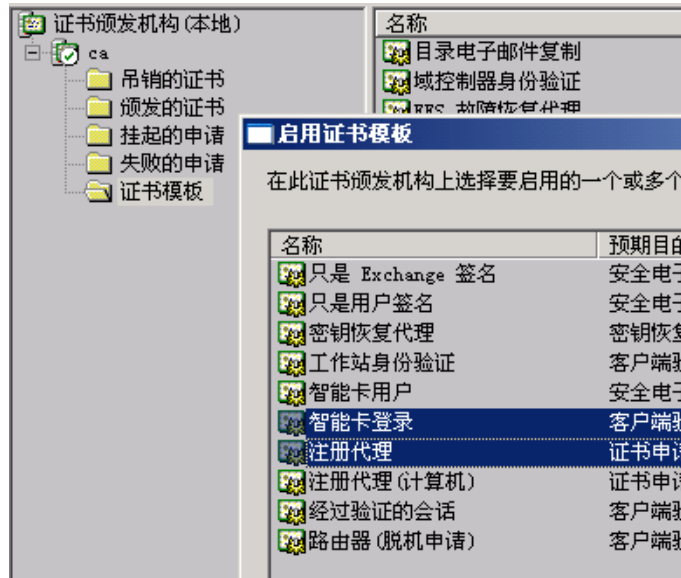
1. 在 AD 域控制器(或加入域的“成员服务器”，使用域管理员登录)上安装 Microsoft CA。
在“添加删除软件→添加删除 Windows 组件”中，添加 IIS 服务和证书服务。



在安装过程中，将 CA 的类型选为“企业根 CA”，随后按照安装过程的要求启动 IIS 的 ASP 功能。

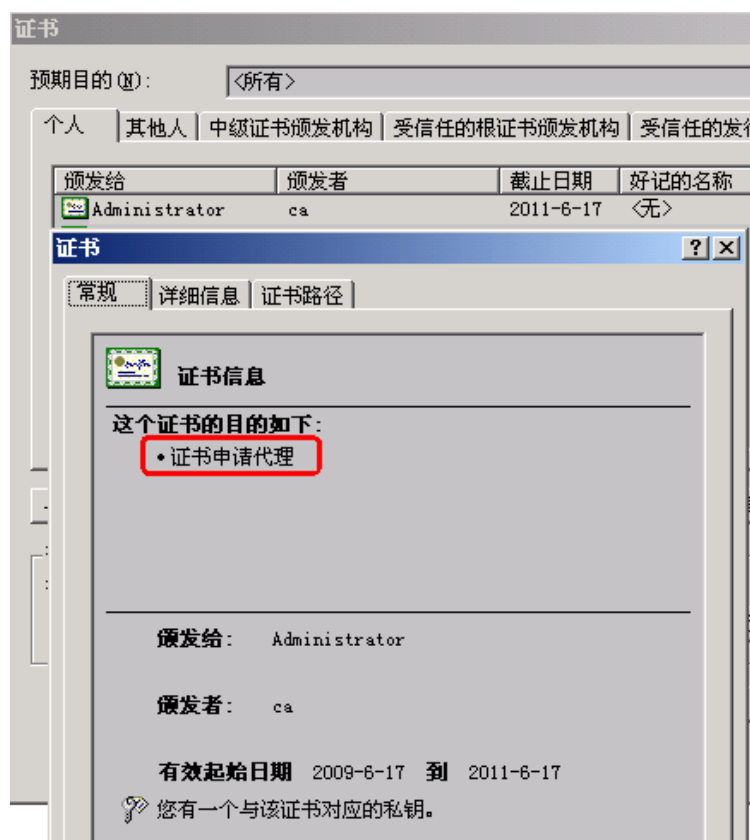


2. 在“管理工具”中打开“证书颁发机构”，在其中的“证书模板”中，新建“注册代理”模板，新建“智能卡用户”或“智能卡登录”模板。

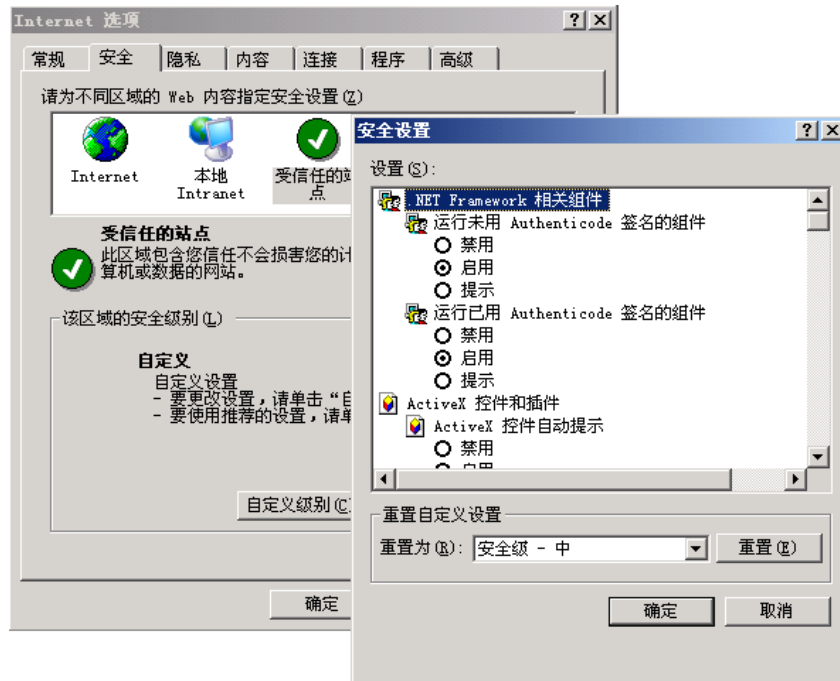


3. 在 MS CA 的发布界面 <http://localhost/certsrv>，进入“申请一个证书”-->“高级证书申请”-->“创建并向此 CA 提交一个申请”，在申请页面中的“证书模板”中，选择“注册代理”，提交后，如果 CA 配置成“自动颁发证书”，则证书申请成功，安装此证书。





4. 在安装 MS CA 的域控制器或成员服务器上安装 USB Key 设备驱动（含 CSP）。
5. 在 MS CA 的发布界面的主页，进入“申请一个证书”--> “高级证书申请”-->“通过使用智能卡证书注册站来为另一用户申请一个智能卡证书”【注意此处可能会因为浏览器安全限制使 ActiveX 无法正常工作，可以将 localhost 加入信任站点列表，或修改解决】。



Microsoft 证书服务

智能卡证书注册站

注册选项:

证书模板: **智能卡登录** **证书模板**

证书颁发机构: **ca**

加密
服务提供程序: **eToken Base Cryptographic Provider** **USB Key的CSP**

管理员
签署证书: **Administrator** **选择证书...**

为注册代理颁发的证书

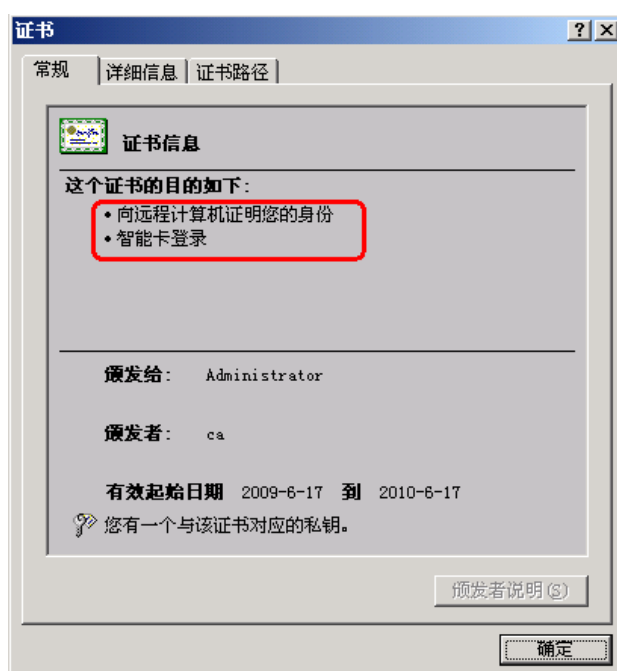
要注册的用户:

VMDMAdministrator **选择用户...**

状态:

请将用户智能卡插入到阅读器中，然后按“注册”。

在最后一个页面中选择“智能卡登录”、选择与 USB Key 对应的“CSP”、选择域中要颁发证书的“用户”，随后将要发放给此最终用户的 USB Key 插入 USB 口，然后按“注册”。注册成功后，USB Key 中将产生私钥和证书，同时证书也会保存在浏览器中。



如果在注册过程中选择“智能卡用户”，则证书信息中会多一项“保护电子邮件信息”目的。

6. 在 USB Key 自带的用户管理工具和管理员管理工具中，也可以查看，编辑一些证书的属性，或修改多个证书的先后顺序、删除证书等。
7. 在所有需要使用 USB Key 登录的 Windows 上安装 USB Key 设备驱动（含 CSP），安装好后，登录界面会自动增加智能卡(USB Key)登录提示。



此时,就可以在 Windows 登录界面中使用 USB Key 登录了。【注意:如果 USB Key 中存有多个证书,会以默认证书的身份登录】

8. AD 域中的用户属性中, 和智能卡 (USB Key) 有关的选项如下图所示。勾选后, 用户将必须使用智能卡 (USB Key) 登录, 而不能使用账号密码方式登录。

