一、方案综述

Microsoft Windows 操作系统提供了整合的网络登录解决方案，登录 Windows 域计算机时的身份验证机制覆盖了从简单的用户名和密码到全面的 PKI 智能卡验证的范围。 eToken 使得网络管理员对基于密码的登录和智能卡登录，都可以执行强大的双因素用户身份验证机制。

在 Windows 网络登录(GINA)机制中，缺省提供了使用智能卡中的数字证书登录域环境的功能，所以配置和实施起来非常稳定和可靠。由于微软的域结构非常复杂，包含了许多通讯协议和组件，所以如果自己开发一套域登录解决方案的话，在兼容性上存在很多问题。而使用 Windows 自带的智能卡登录功能，不会有任何兼容性的问题，同时也不需要改变 Windows 的登录界面，给用户一个熟悉的操作环境。

二, 解决方案优点

- 针对智能卡登录方案，eToken 提供了安全的板载生成 PKI 密钥和数字证书的机制，由于私钥永远不会离开 eToken，同时用户资料安全地存储在 eToken 设备中，增强了安全性和可移植性。
- 通过双因素身份验证机制，要求用户必须提供 eToken 设备和 eToken 密码才能使用此设备。eToken 提供了强大的保护能力，以及紧凑的 USB 设备带来的便携性，保护您的企业网络，避免未经授权的访问。
- 支持两种模式：一个 eToken 既可以支持基于密码的身份验证，在 eToken 中保存 Windows 操作系统的登录帐号和密码；也可以支持基于 PKI 的网络身份验证，在 eToken 中安全地保存用户的网络访问数字证书，确保最大的灵活性和易用性。
- 支持在一个 eToken 上存储和管理多个用户资料和第三方应用登录凭证，可以配合 SafeNet eToken SSO 软件，无缝地升级到单点登录解决方案。

三, 系统安装和实施部署主要步骤

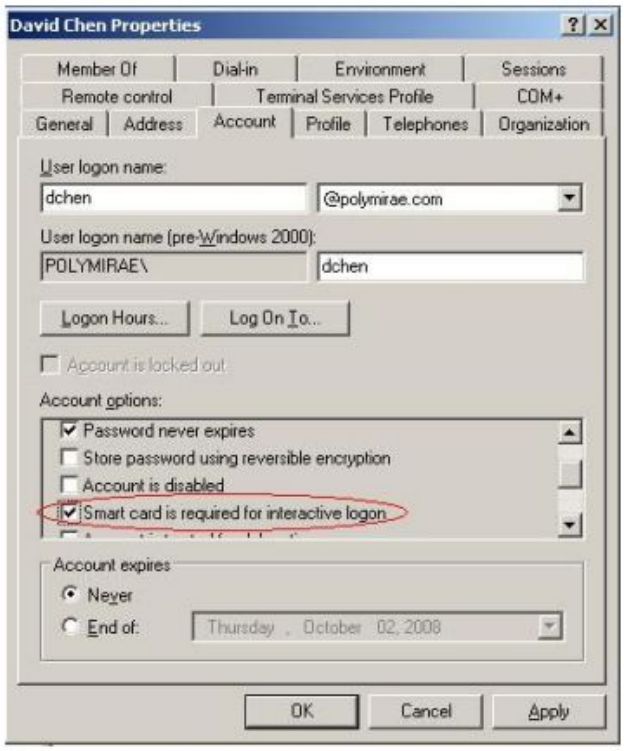
1. 在现有域成员服务器上或者新建的域服务器上安装 IIS 以及 SAM 认证管理系统。

2. 安装 Windows 操作系统中自带的 Microsoft Enterprise CA，配置证书模板，允许用户申请 Windows 智能卡登录证书。
3. 配置 SafeNet SafeNet 认证管理系统，允许管理员在分配令牌的同时，系统会自动到 MSCA 上申请证书并且自动写入到用户的 eToken 中。
4. 在 AD 中创建用户并且分配 eToken，用户的 Windows 登录证书自动写入到 eToken 中，将 eToken 发放给用户。
5. 在用户客户端电脑上需要安装 SAC 软件才能够正常读取 eToken 中证书。
6. 用户拿到令牌以后，启动计算机，如果安装了 SAC 以后，在启动界面上会显示下图所示的智能卡图标。

7. 在开机界面中插入 eToken，显示输入 PIN 码界面。

8. 输入正确的 eToken 密码以后，就可以安全地登录操作系统。

9. 管理员可以定义此用户必须使用智能卡才能够登录操作系统，即使知道了操作系统的用户名和密码也无法登录操作系统，增强了系统的安全性。



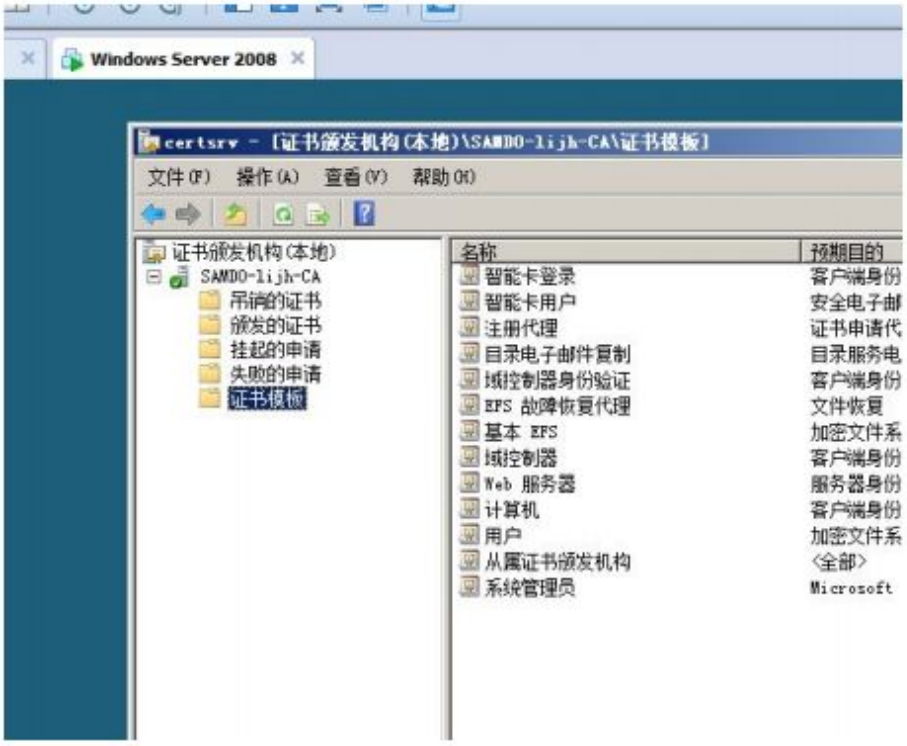
10. 当用户试图使用静态密码登录操作系统时，显示出错信息。

11. 管理员还可以根据用户组策略配置当用户拔出 eToken 时候计算机的响应，管理员可以有几个选项可以选择：没有操作；锁定计算机；强制退出和中断远程终端连接会话。

四、部署的详细步骤

1. 域控初始状态

2、打开证书颁发机构



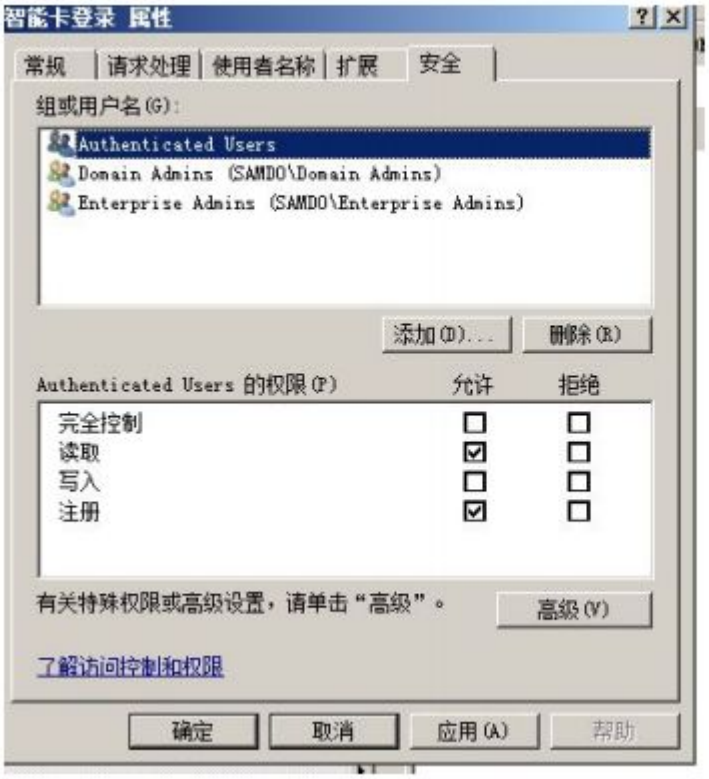
3、右键证书模版---新建---要颁发的证书模版

4、选择智能卡登录，智能卡用户，注册代理；点击确定

5、右键证书模版—管理

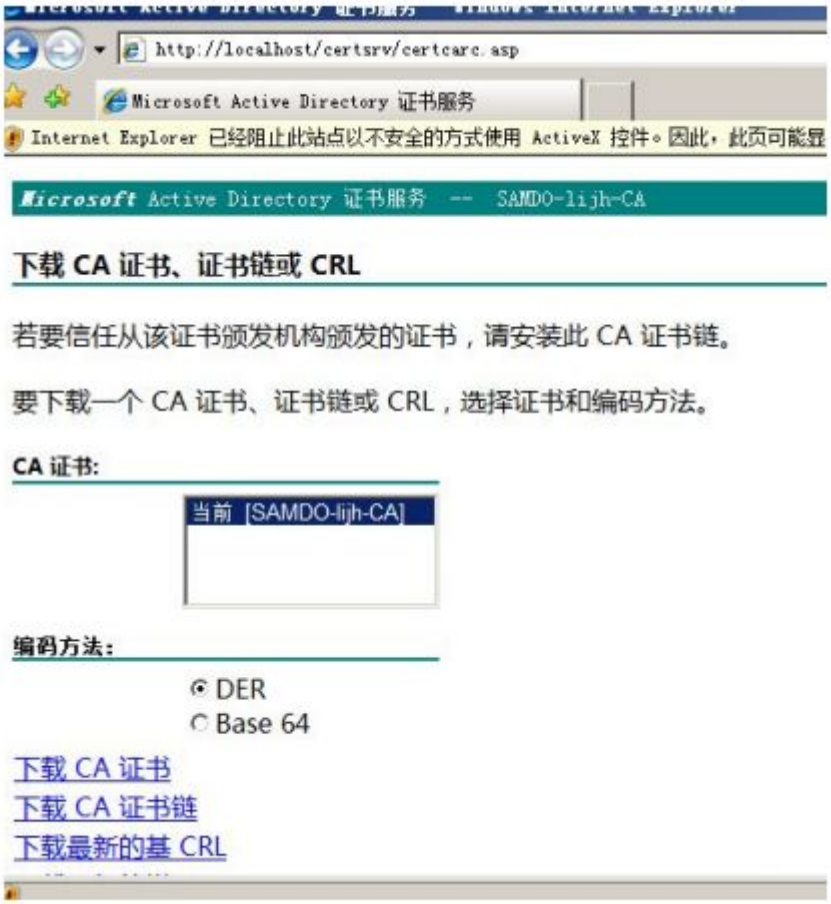
6、右键智能卡用户-属性设置如下图

7、右键智能卡登录-属性，设置如下图



8、打开 IE，输入 http://localhost/certsrv/

9、下载 CA 证书、证书链或 CRL

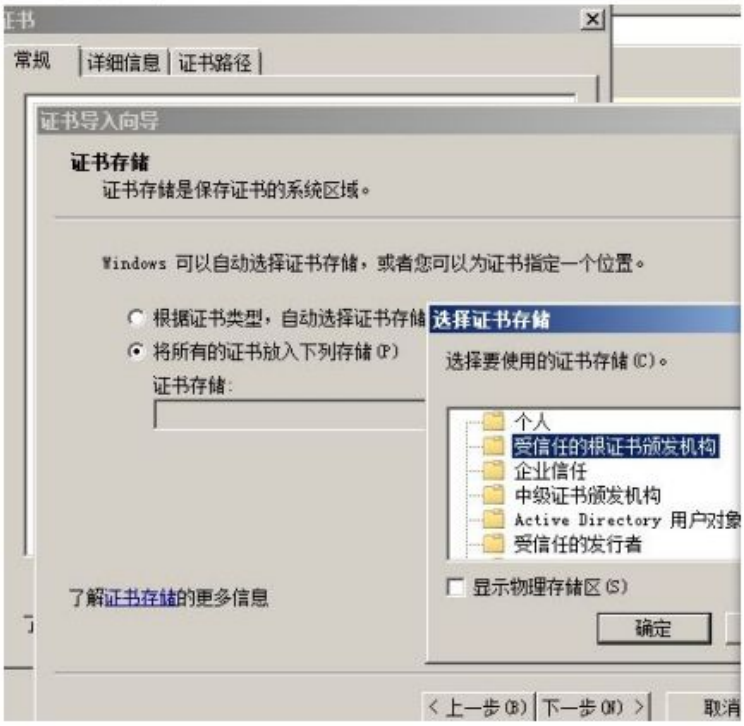


10、下载 CA 证书

DER
Base 64

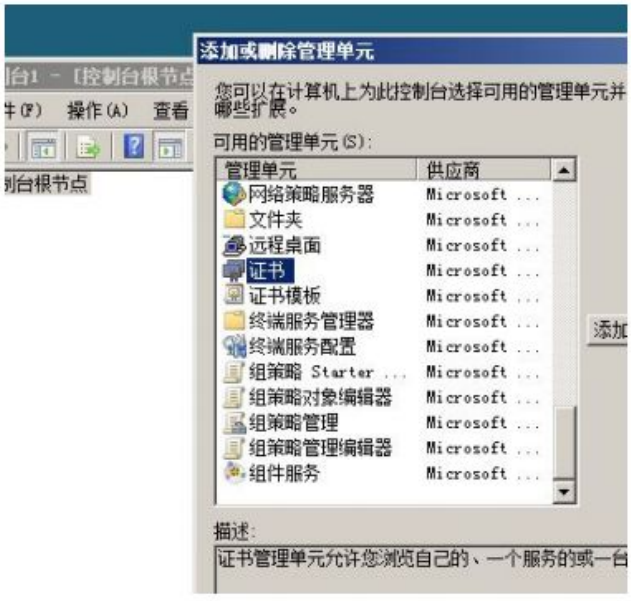
11、打开

12、安装证书

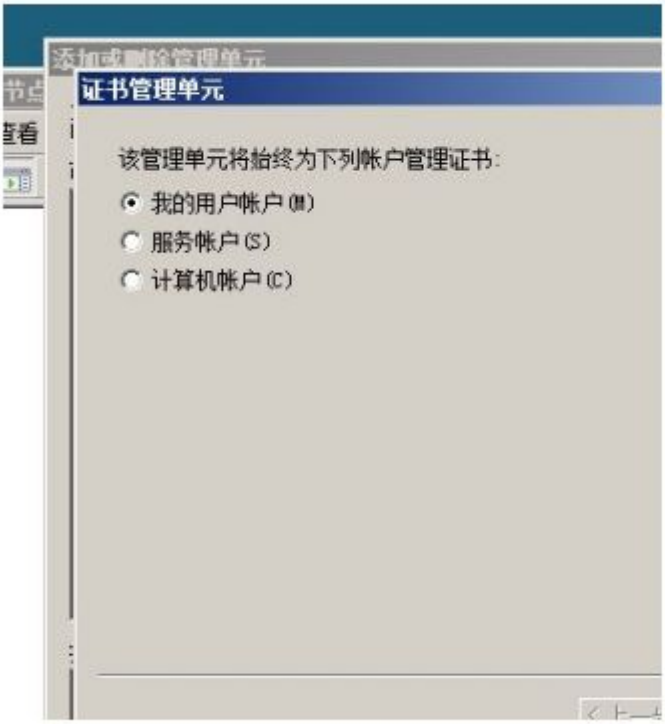


确定，下一步，完成，导入成功。

13、在运行--输入 MMC，打开控制中心，添加/删除管理单元



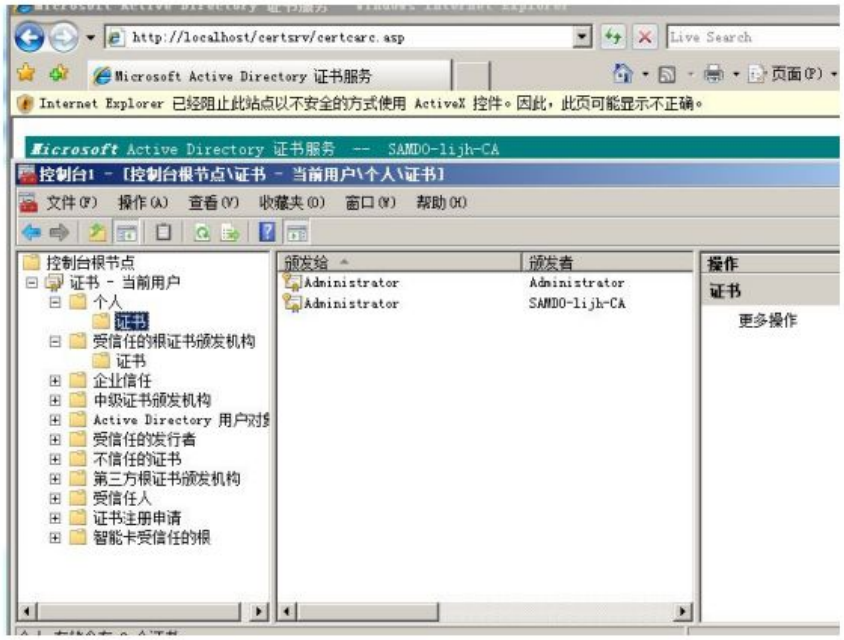
14、证书—添加



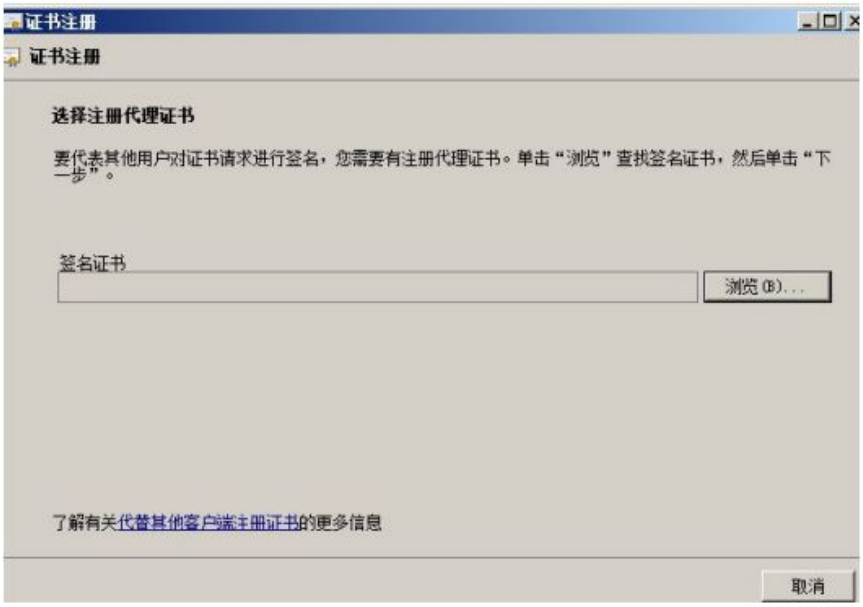
15、完成—确认

16、右键个人--所有任务--申请新证书--下一步

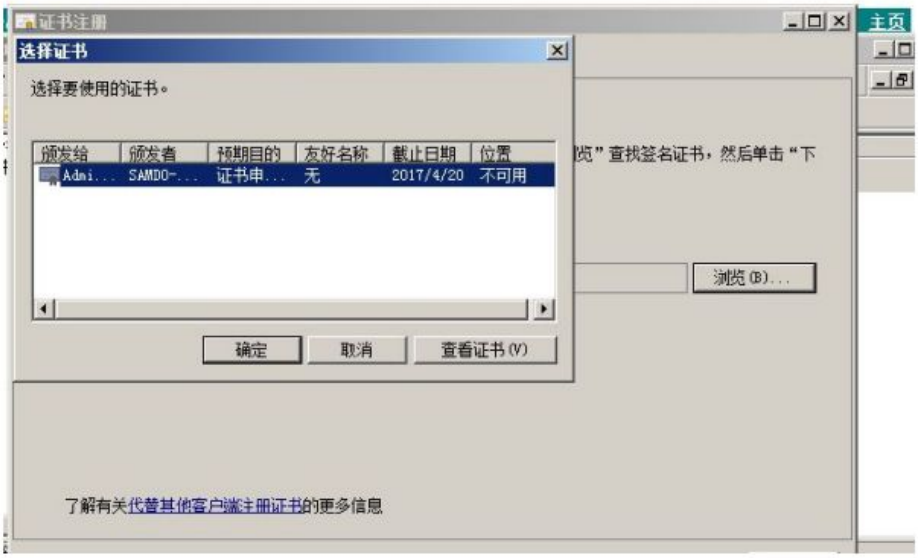
17、注册代理---注册-成功-完成—右键证书



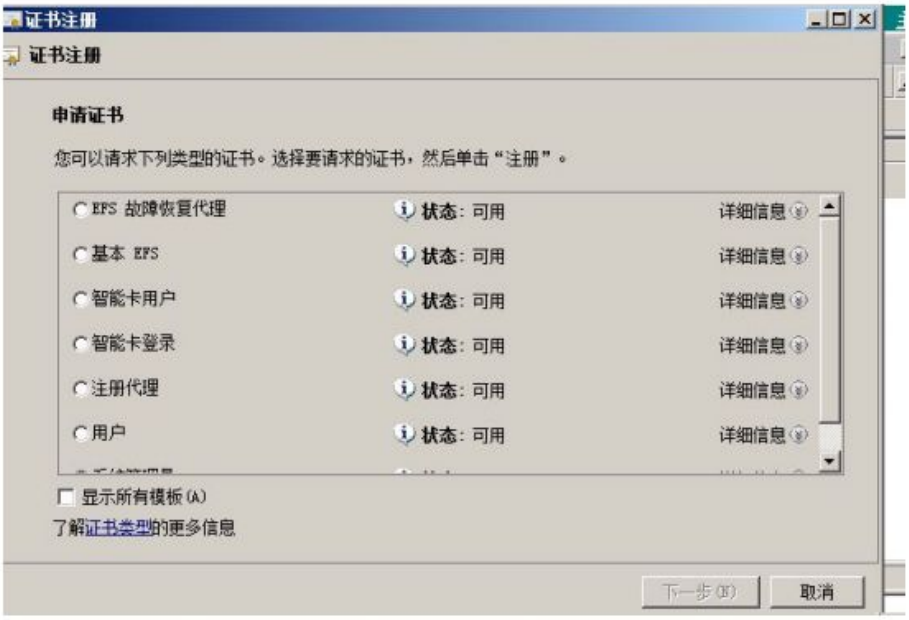
18、所有任务—高级操作---注册代表—下一步



19、浏览

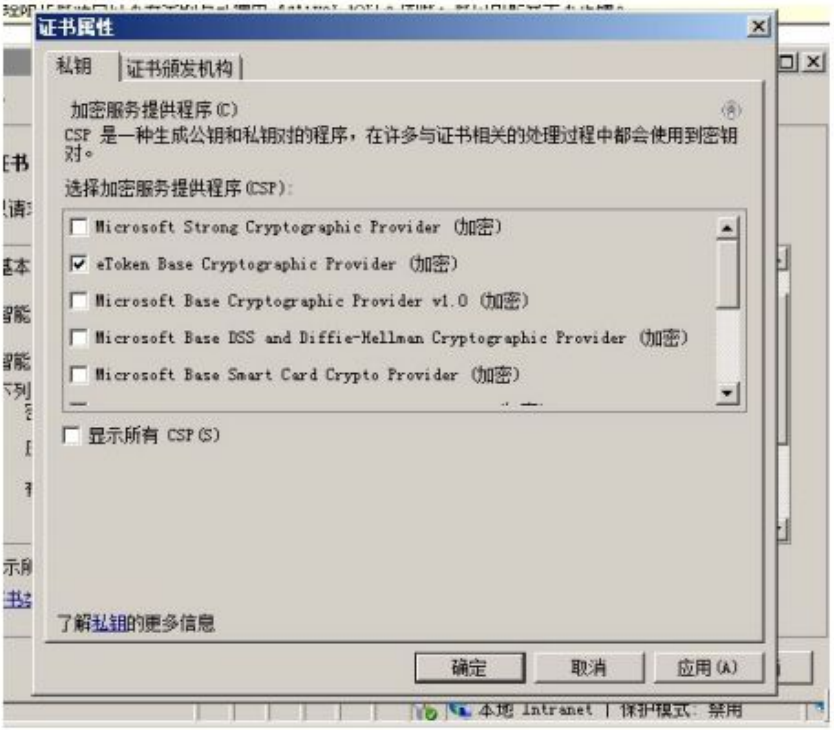


20、选择证书确定---下一步---智能卡登录



21、详细信息---属性

22、如下图，应用确定---下一步--浏览选择给域用户

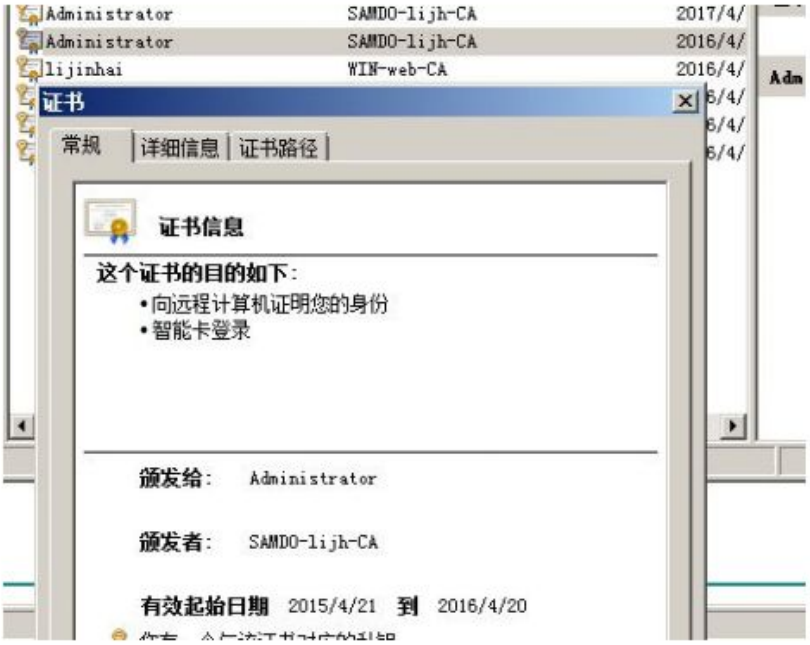


23、注册

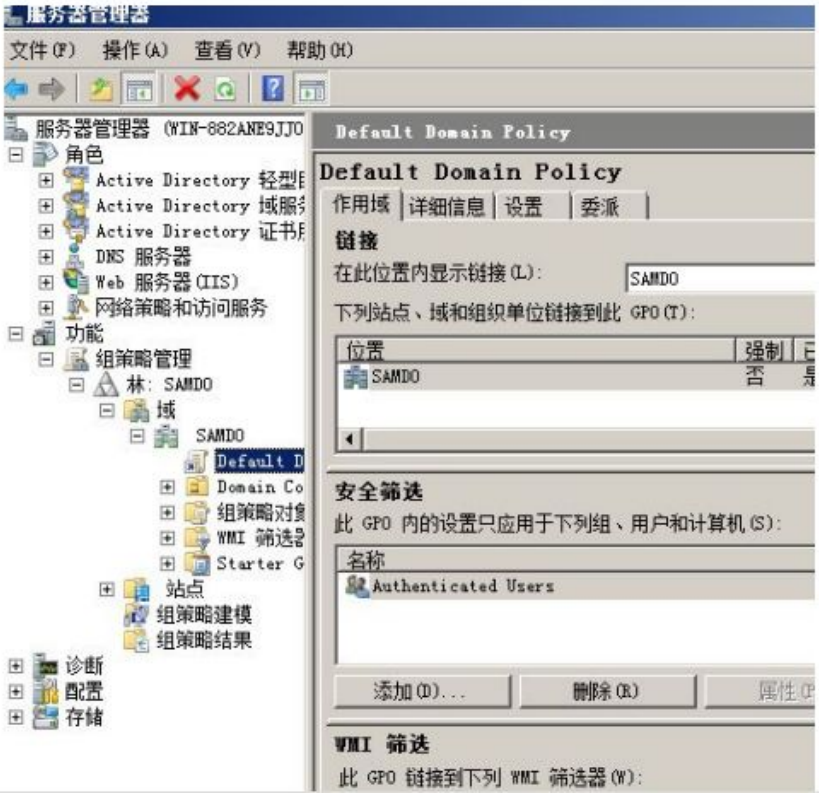
24、插入智能卡输入密码

25、注册成功

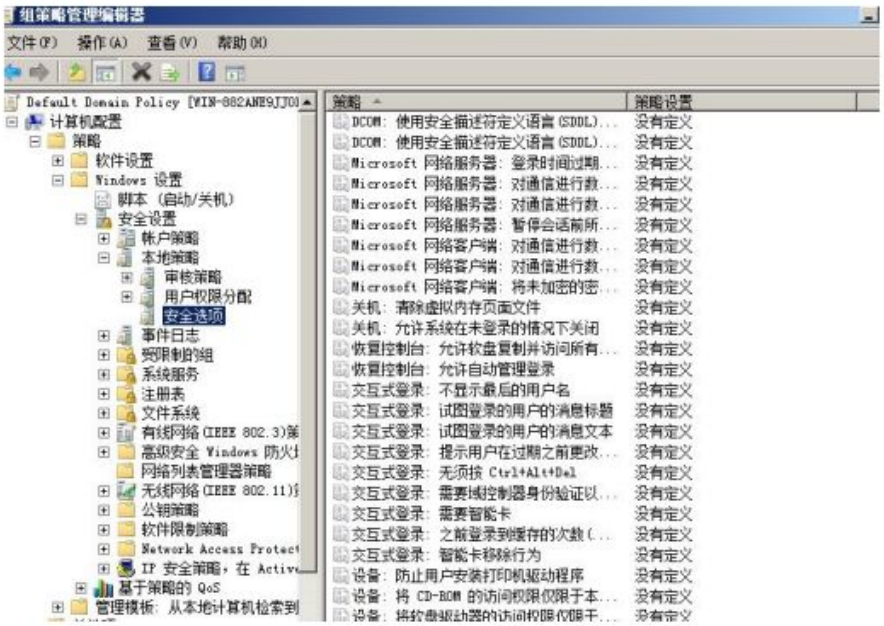
（可查看用户证书如下图）



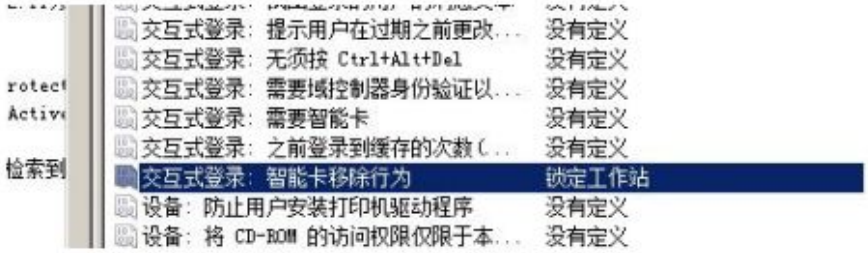
26、打开服务器管理-如下图



27、右键 default domain policy—编译



28、打开安全选项



29、回到服务器管理

30、点第二个 administrator 右键属性配置如下

31、确定---生效

实现必须使用 USB-eToken 才能登录域环境。