一、安全现状

允许外界远程访问 WEB 应用越来越普遍，拥有网络信息资产的公司越来越容易受到黑客或恶意入侵者的攻击。企业内部员工账号口令没有得到重视，混乱使用，导致企业内部信息泄露，责任无法确定。

二、解决方案

使用现有 Microsoft® Windows 2003 Server、Windows Server 2008 或 Windows Server 2012 的基础结构，企业可以利用智能卡极大地增强其网络安全强度.特别是登录 WEB 网页的认证可以使用数字证书方式强认证。

三、优点

安全性得到增强：智能卡双因素身份验证不仅要求拥有智能卡还必需知道智能卡 PIN 码。

灵活：智能卡内存包含安全证书，可用于内部开发项目。

简单：智能卡简单易用。不附带麻烦的密码生成器。不需要控制庞大的设备。

利用现有的基础结构：使用 Windows 2003 Server、Windows Server2008 或 Windows Server 2012 的 PKI 可以创建自己的安全证书，并无需依靠外部合作伙伴即可在内部管理此进程。

四.产品和技术

Windows2003Server、Windows Server 2008 以及 Windows Server 2012

Active Directory®

基于 Windows 的公钥基础结构(PKI) 和证书颁发机构(CA)

可使用智能卡的 Windows

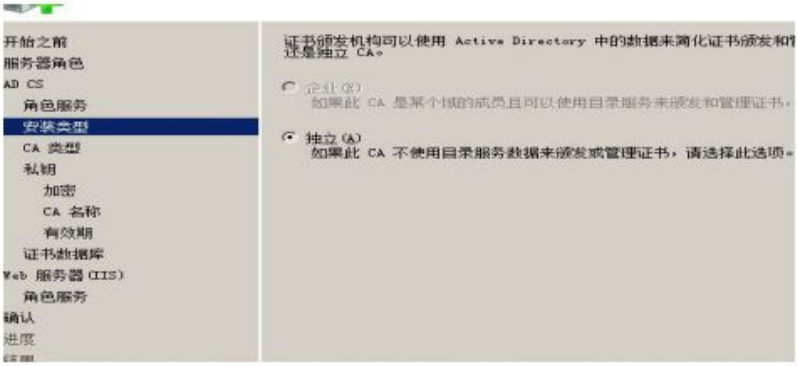
智能卡（USB 设备，免读卡器的智能卡）

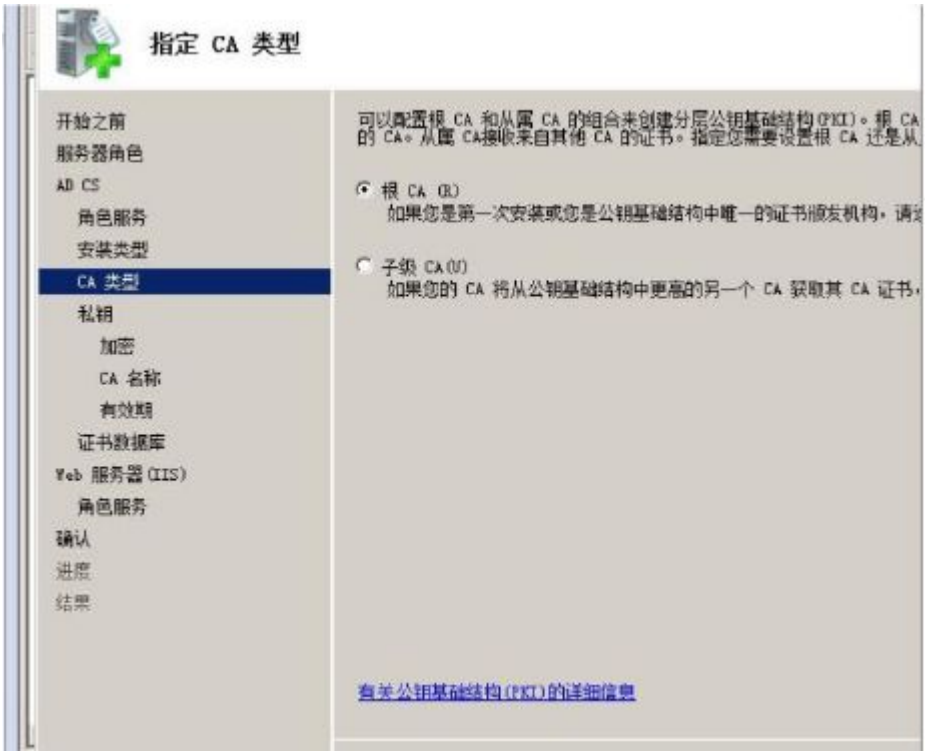
五、在 windows server2008 R2 部署

打开服务器管理-角色一添加角色一下一步一选中ActiveDirectory证书服务和WEB服务（IIS）

下一步---下一步—选中证书颁发机构、证书颁发机构 WEB 注册

再下一步


开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
证书颁发机构可以使用 Active Directory 中的数据来简化证书颁发和管
还是独立 CA。
企业(E)
如果此 CA 是某个域的成员且可以使用目录服务来颁发和管理证书，
独立(A)
如果此 CA 不使用目录服务数据来颁发或管理证书，请选择此选项。


指定 CA 类型
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
可以配置根 CA 和从属 CA 的组合来创建分层公钥基础结构(PKI)。根 CA
的 CA。从属 CA接收来自其他 CA 的证书。指定您需要设置根 CA 还是从
根 CA(R)
如果您是第一次安装或您是公钥基础结构中唯一的证书颁发机构，请
子级 CA(U)
如果您的 CA 将从公钥基础结构中更高的另一个 CA 获取其 CA 证书，
有关公钥基础结构(PKI)的详细信息


若要生成证书并颁发给客户端，CA 必须有一个私钥。指定您要新建私钥还是使
新建私钥(R)
如果您没有私钥或者要新建一个私钥以增强安全性，请使用此选项。系统将
供程序并指定私钥的密钥长度。若要颁发新证书，还必须选择一个哈希算法
使用现有私钥(U)
使用此选项可确保重新安装 CA 时与先前颁发的证书的连续性。
选择一个证书并使用其关联私钥(C)
如果您在此计算机上有一个现有证书，或者如果您希望导入一个证书并使
择此选项。
选择此计算机上的现有私钥(E)
如果您已保留来自以前安装的私钥或需要使用其他来源的私钥，请选择此
前
角色
服务
类型
类型
密
A 名称
有效期
数据库
务器(IIS)
服务


添加角色向导
设置私钥
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
选择加密服务提供程序(CSP)(C):
RSA#Microsoft Software Key Storage Provider
密钥字符长度(K):
2048
选择此 CA 颁发的签名证书的哈希算法(H):
sha1
md2
md4
md5
使用由 CSP 提供的强私钥保护功能(每次 CA 访问该私钥时，可能需要和
有关 CA 的加密选项的详细信息

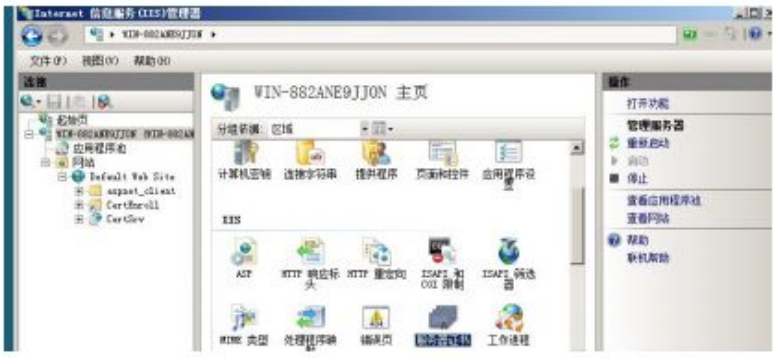

添加角色向导
配置 CA 名称
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
键入公用名称以识别此 CA。此名称会被添加到由该 CA 颁发的所有证书中动生成的，但可以修改。
此 CA 的公用名称(C):
wenlogin-CA
可分辨名称后缀(D):
可分辨名称的预览(P):
CN=wenlogin-CA
有关配置 CA 名称的详细信息


添加角色向导
设置有效期
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
会将一个证书颁发给此 CA 以保护与其他 CA 和请求证书的客户端
基于许多因素，包括 CA 的预期目的以及为保护 CA 您已采取的安
选择为此 CA 生成的证书的有效期(V):
20
年
CA 过期日期: 2035/4/22 16:02
请注意，CA 仅在其过期日期之前才能颁发有效的证书。
有关设置证书有效期的详细信息

选择 ASP.NET、基本身份登录、windows 身份登录、客户端证书映射身份验证

下一步默认安装完成

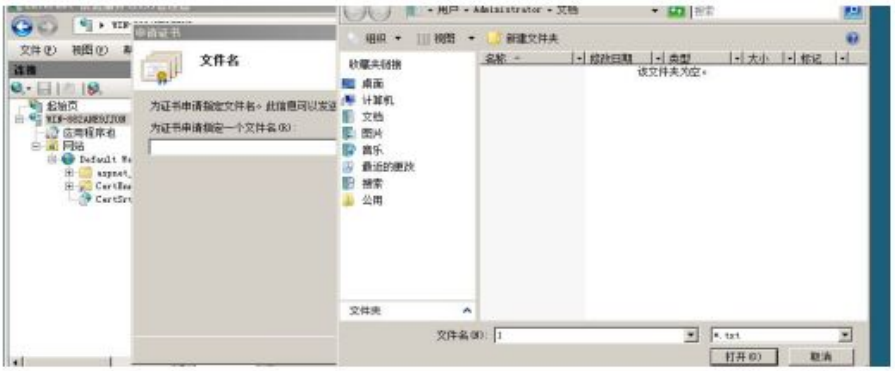
2,服务器端证书申请



打开服务器证书

创建证书申请，注：通用名称最好是与网站 IP 地址一致。

下一步---下一步



保存 1.TXT 文件

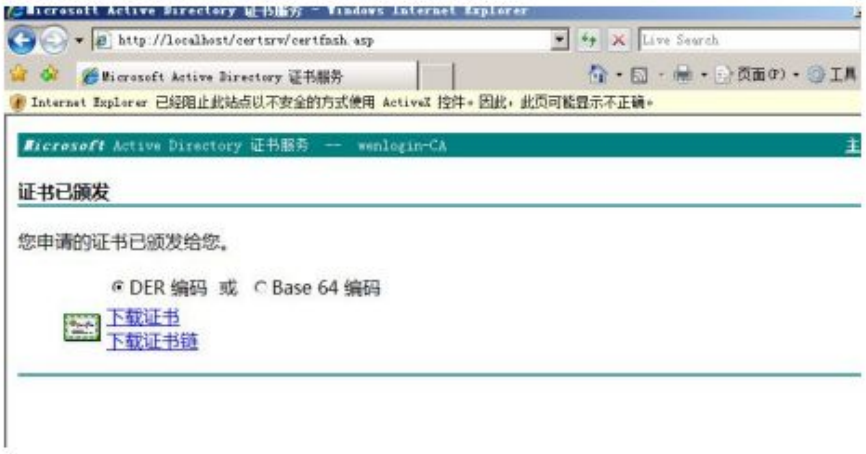
打开 http://localhost/certsrv

申请证书---高级证书申请

选下面那个 BASE64----把上面保存的 1.TXT 中的全部 copy

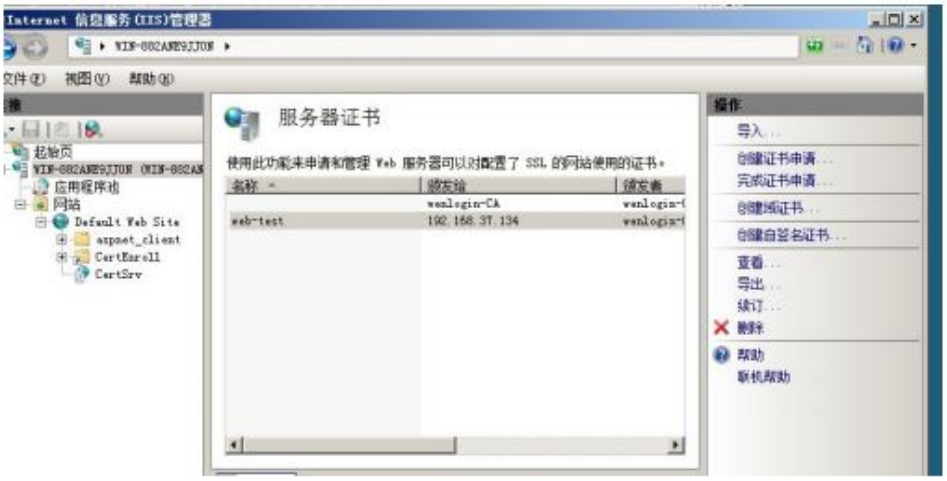

Microsoft Active Directory 证书服务 - Windows Internet Explorer
http://localhost/certsrv/certrqxt.asp
Live Search
Microsoft Active Directory 证书服务
页面(P) 工具(O)
提交一个证书申请或续订申请
要提交一个保存的申请到 CA，在“保存的申请”框中粘贴一个由外部源(如 Web 服务器)生成的 base-64 编码的 CMC 或 PKCS #10 证书申请或 PKCS #7 续订申请。
保存的申请:
Base-64 编码的证书申请 (CMC 或 PKCS #10 或 PKCS #7):
BgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQU
LeIwDQYJKoZIhvcNAQEFBQADgYEAWRcVIOzT2HFq
X9Y+ULDNv6pJ/Qb2R8IlaK3Uyo5I7Bo6+19fb3BA
thx7bWsKJJj5xuIwBmxf7kLRnevRk8HYcDu7KrOq
IyGQT/A=
-----END NEW CERTIFICATE REQUEST-----
附加属性:
属性:
提交 >

提交


Microsoft Active Directory 证书服务 - Windows Internet Explorer
http://localhost/certsrv/certfnsh.asp
Live Search
Microsoft Active Directory 证书服务
页面(P) 工具
Internet Explorer 已经阻止此站点以不安全的方式使用 ActiveX 控件。因此，此页可能显示不正确。
Microsoft Active Directory 证书服务 -- wenlogin-CA
证书已颁发
您申请的证书已颁发给您。
DER 编码 或 Base 64 编码
下载证书
下载证书链

下载证书—保存

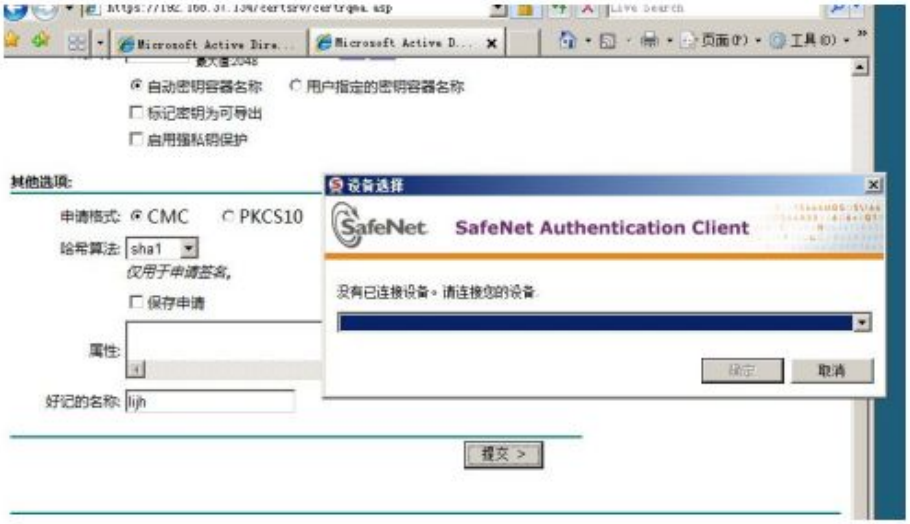
再次打开 IIS---服务器证书---完成证书创建



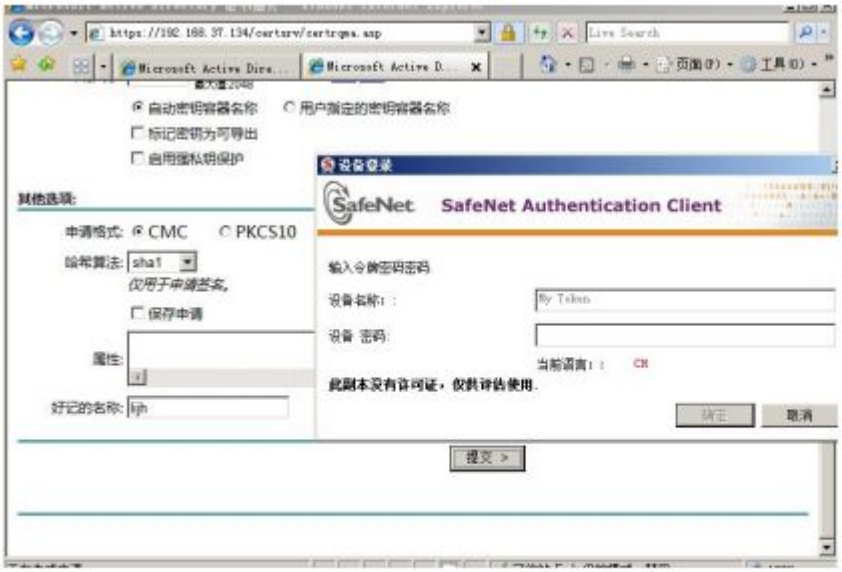
3、申请客户端证书---绑定 default web site,SSL 选择 WEB-TEST

打开浏览器输入 https://192.168.37.134/certsrv，申请证书---高级证书申请---创建并向此 CA 提交一个申请。另安装 SAC，配置如下图

提交



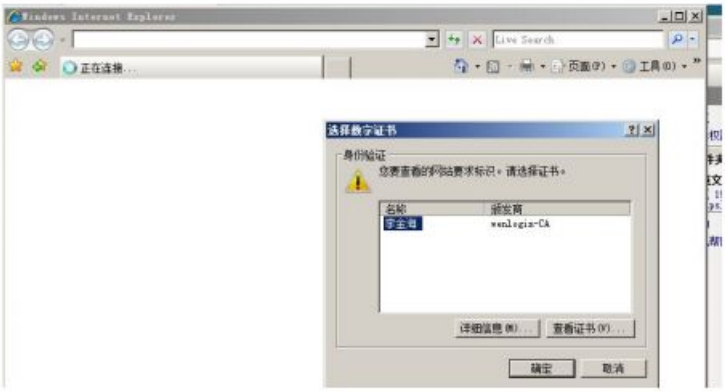
插入 etoken



输入密码，默认 1234567890，第一次登录需更改密码

申请证书成功。

4、绑定你们的 web 工程---选择 SSL 为 web-test.测试你的程序。在登陆电脑上必须安装 SAC




Windows Internet Explorer
正在连接...
Live Search
页面(P)
工具(O)
设备登录
SafeNet
SafeNet Authentication Client
输入令牌密码密码.
设备名称:
eToken PRO Java
设备 密码:
当前语言:
此副本没有许可证，仅供评估使用.
确定
取消


IIST - Windows Internet Explorer
https://192.168.37.134/
Live Search
IIST
页面(P)
工具(O)
Willkommen
Bienvenue
歡迎
Velkommen
Benvenuto
Welkom
Välkommen
Hoş Geldiniz
Microsoft 仿冒网站筛选
帮助使您的浏览器更安全：
设置仿冒网站筛选
打开自动仿冒网站筛选(推荐)(O)
关闭自动仿冒网站筛选(F)
网站地址不会发送给 Microsoft，除非您选择检查网站地址。
稍后询问(A)
确定