Windows安全原理与技术

— 第十三章：公钥基础结构

王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

PKI的由来

"On the Internet, nobody knows you're a dog."

在数字化的社会中，实体间建立信任关系的关键是能彼此确定对方的身份。

1 从网上获得 Bob 公钥

3 Alice向Bob发送密文

2 Alice 使用Bob的公钥加密

4 Bob 使用自己的私钥解密

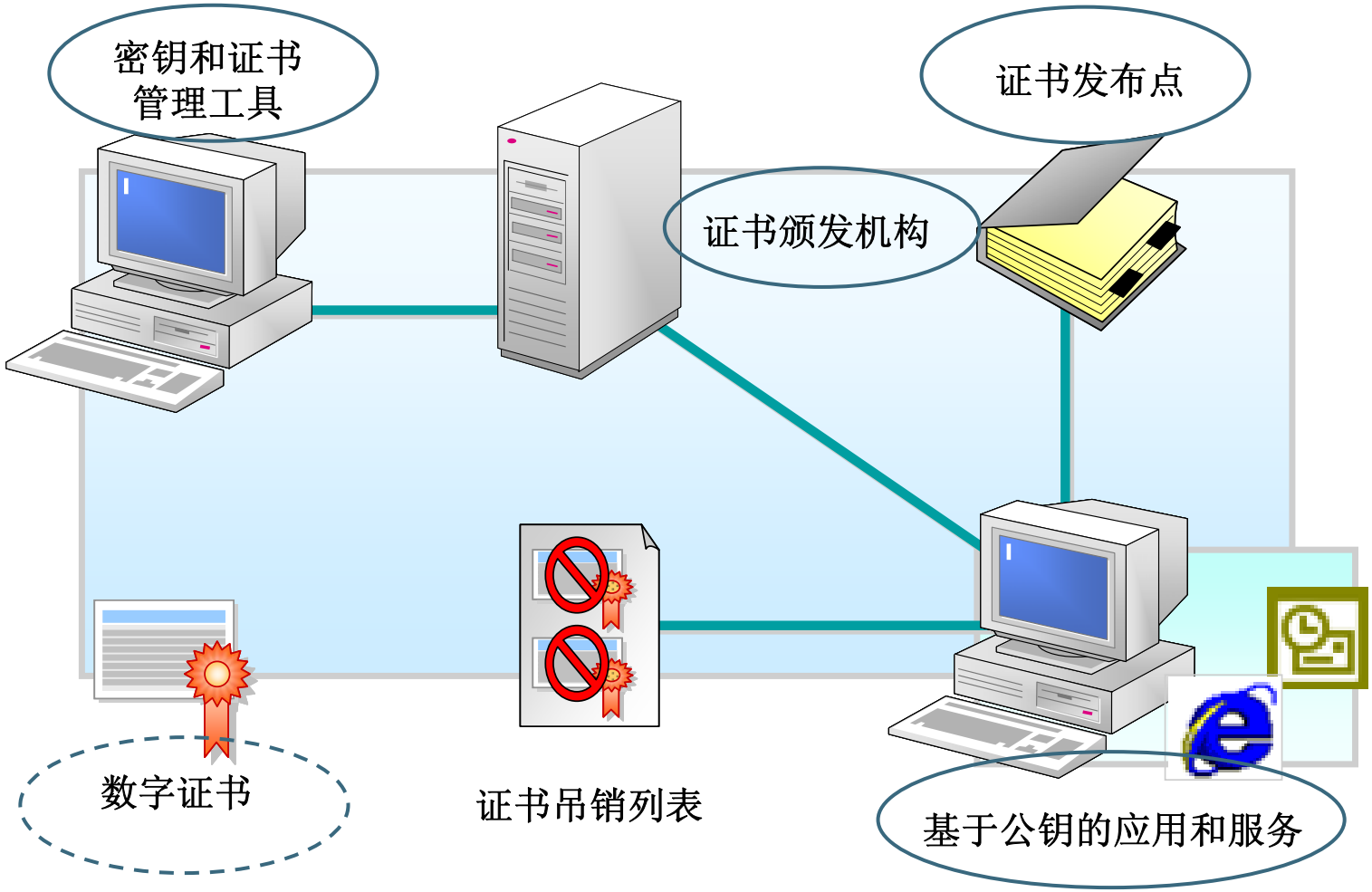
[存在的问题]

Alice如何能够确认从网上获取的Bob的公钥为真？

PKI（公钥基础结构）的功能

- 管理密钥
  - PKI方便了颁发新密钥、检查或吊销现有密钥、以及管理不同颁发者发行的密钥的信任程度。
- 发行密钥
  - PKI为客户端明确定义了定位和获得公钥，以及查看某公钥是否有效的途径。如果不能获得公钥和知道它的有效性，用户就不能利用公钥服务。
- 使用密钥
  - PKI为用户提供了便于使用密钥的途径。它不仅将密钥置于用户需要的地方，而且还提供了执行公钥加密的便于使用的应用程序，使之能保障电子邮件、电子商务和网络的安全。

PKI的组件



数字证书

- 数字证书是证明证书持有人的身份颁发机构所颁发的数字声明。
  - 证书提供了一种机制，用于确立对公钥和拥有相应私钥的实体之间关系的信任。
  - 由各种公钥安全服务和提供身份验证的应用程序、数据完整性和通过网络的安全通讯所使用。

Windows的标准证书格式是X.509 v3

证书颁发机构（CA）

- 功能
  - 向用户颁发证书，建立和确定证件持有者的身份。
  - 颁布“证书吊销列表”（CRL）。
- CA的层次结构
  - 根CA是一个机构的PKI中最可信任的CA类型。通常，只将根CA用于向下级CA发放证书。
  - 下级CA是已经被另一个CA鉴定过的CA。通常，下级CA针对特定的应用发放证书。下级CA也可以向其它的，更下级的CA发放证书。

Windows 2000支持PKI的特性

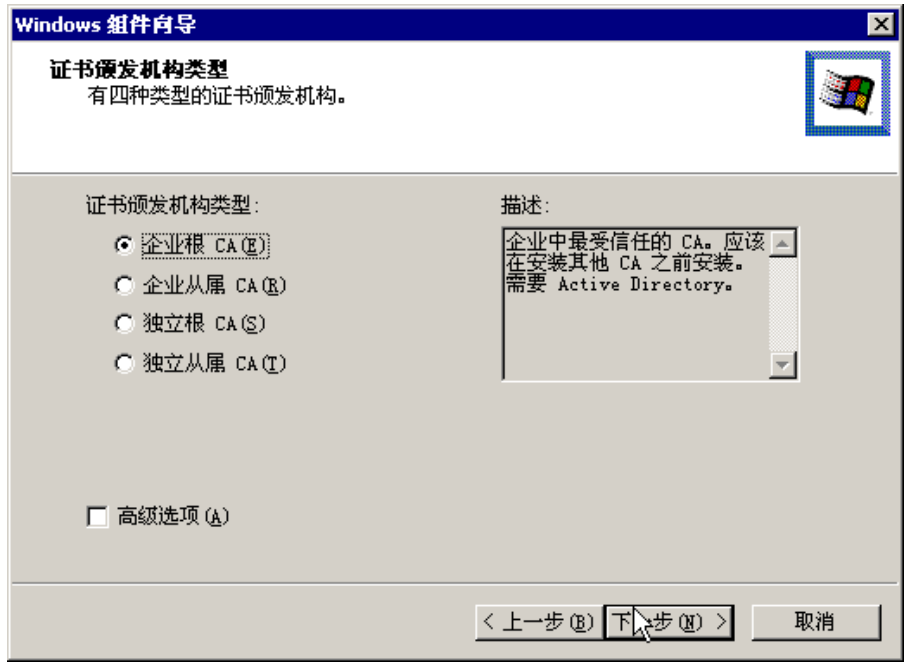
- 数字证书
- 证书服务（安装在Windows 2000 Server上）
  - 创建和管理证书颁发机构的组件。
  - 个别组件是CA Web登记页面。
- 智能卡支持
- 公钥策略
  - 可以使用组策略自动给计算机指派证书、建立证书信任列表和公用的信任证书颁发机构。

使用Windows 2000中的PKI

- 创建证书颁发机构（安装证书服务）
- 为用户颁发证书
- 证书的导出和导入
- 证书的更新
- 证书的撤销
- 证书服务的备份和还原

安装证书服务

“控制面板”→“添加/删除程序”→
“添加/删除Windows 组件”



- 选择证书颁发机构类型

- 证书颁发机构的类型
  - 企业根CA
  - 企业下级CA
  - 独立根CA
  - 独立下级CA
- 企业CA和独立CA的区别
  - 企业根CA和企业下级CA需要Active Diretory
  - 独立根CA和独立下级CA不需要Active Diretory

安装证书服务（续）

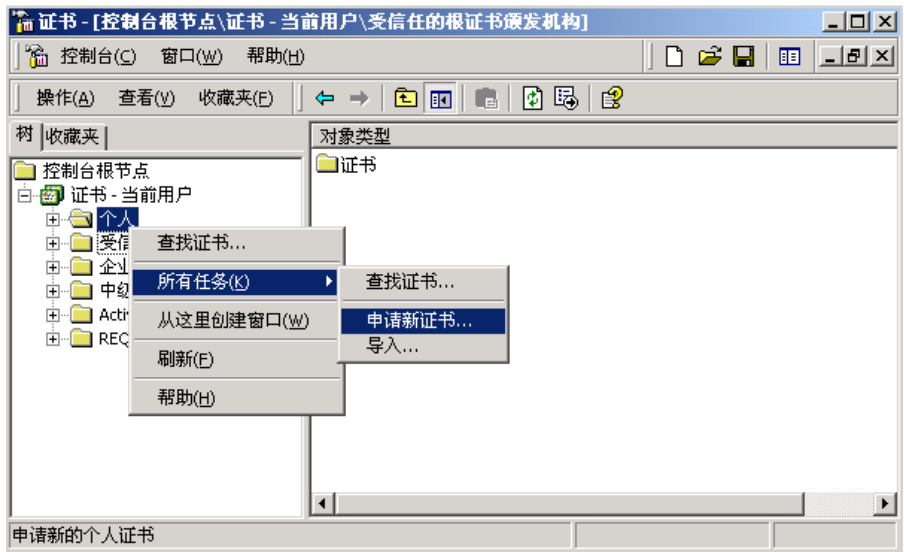
- 选择高级选项
  - 加密服务提供程序
  - 密钥长度
  - 散列算法
- 输入证书颁发机构标识信息
- 指定数据库和配置存储位置
  - 只有在安装了独立的CA但没有Active Directory时，该选项才有效。
  - 默认为%SYSTEMROOT%\system32\certlog

如果证书服务的主机是域的成员，那么有关CA的信息会自动发布到Active Directory

为用户颁发证书 — 申请证书（1）

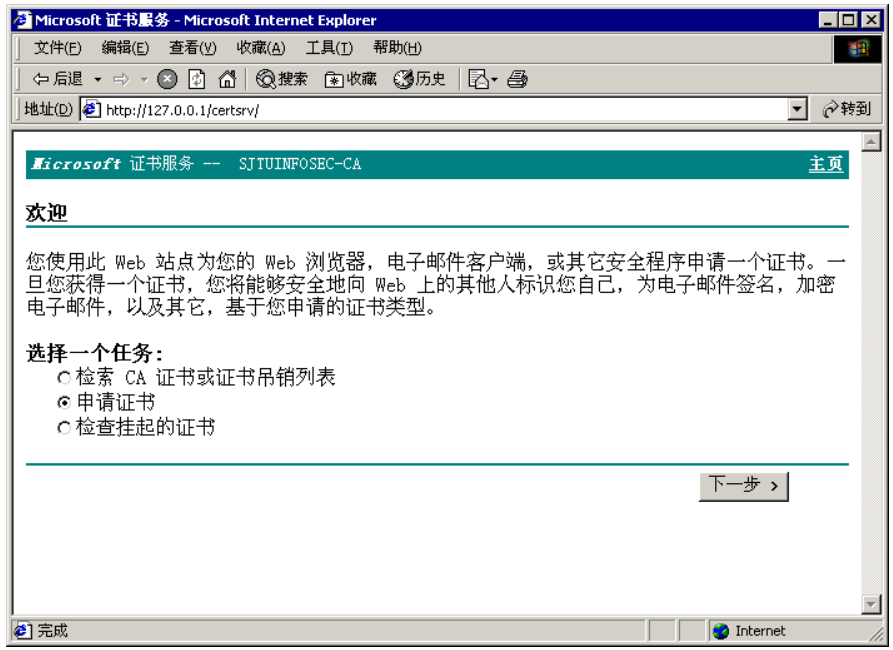
- 使用证书申请向导
  - 只有在Windows域中可用的企业证书颁发机构才可以使用。
  - 只提供“加密服务提供程序”等可选的申请功能。

打开“证书”管理单元→选择证书存储区→“所有任务”→“申请新证书”



为用户颁发证书 — 申请证书（2）

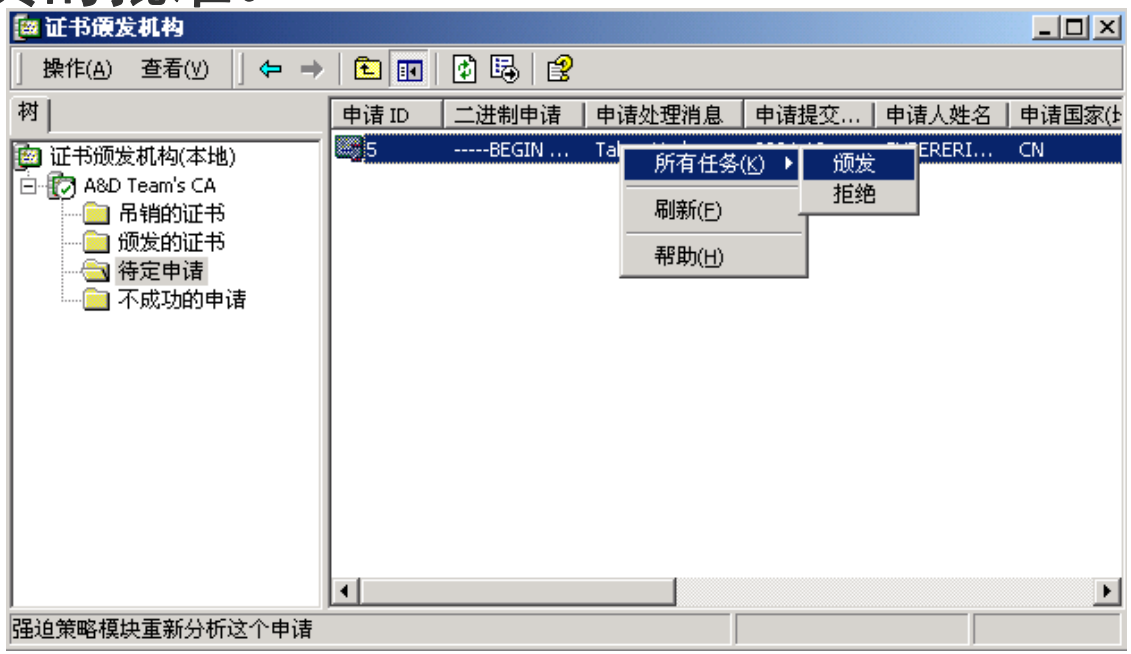
- 使用Windows 2000证书服务Web页
  - 既可用于企业证书颁发机构，也可用于独立颁发机构（不依赖于域）。
  - 提供了更多可选的申请功能。
    - 将密钥标记为可导出、设置密钥长度、选择散列算法以及将申请保存到PKCS #10文件等。

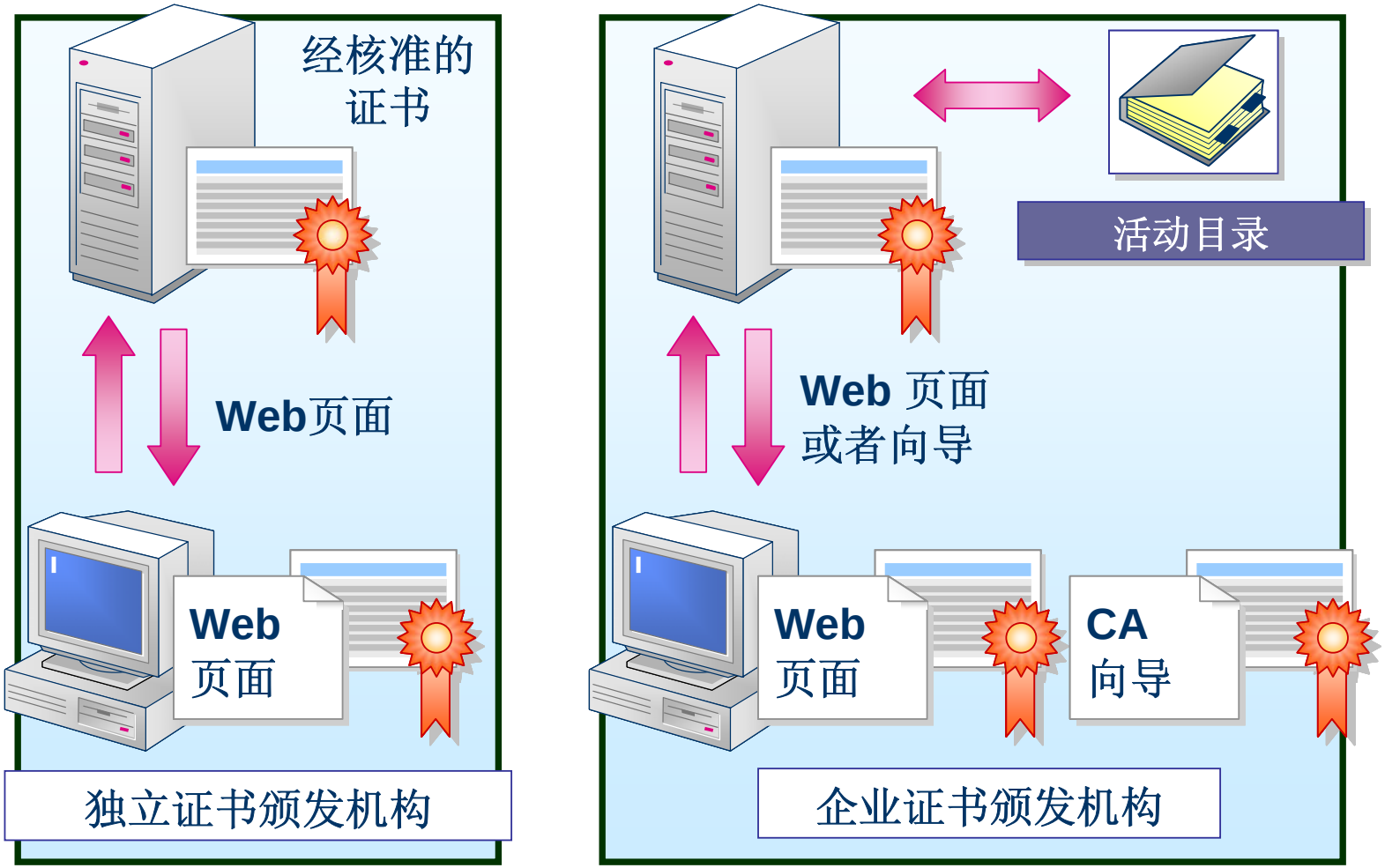


使用Web浏览器访问
http://servername/certsrv/

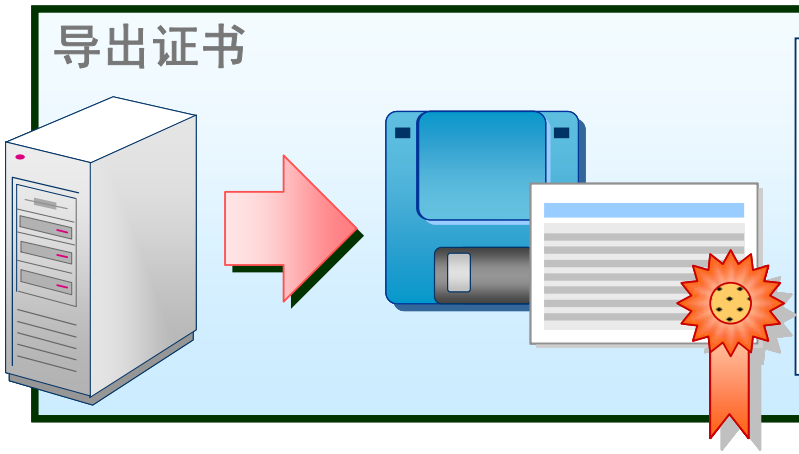
为用户颁发证书 — 处理证书申请

- 处理证书申请
  - 当证书请求提交到企业证书颁发机构时，它将被立即处理。
  - 当证书请求提交到独立证书颁发机构时，该申请被挂起，等待管理员的批准。

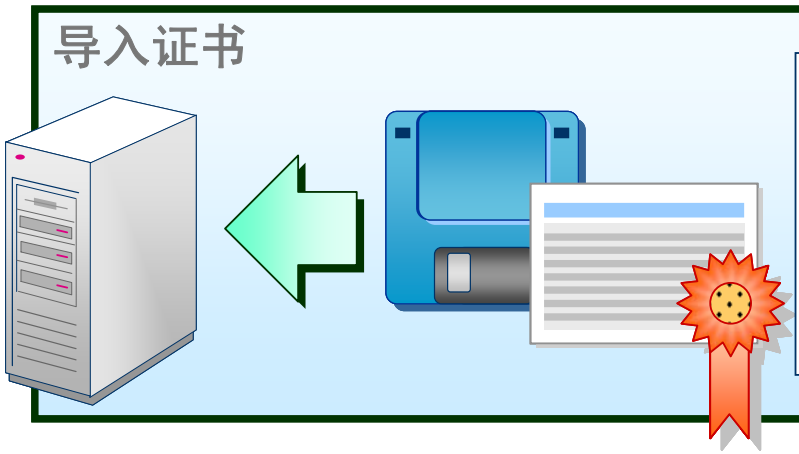



经核准的
证书
Web页面
Web
页面
独立证书颁发机构
活动目录
Web 页面
或者向导
Web
页面
CA
向导
企业证书颁发机构

证书和密钥的导出和导入



- 备份证书和密钥
- 计算机之间的证书拷贝
- 卸载原来的证书

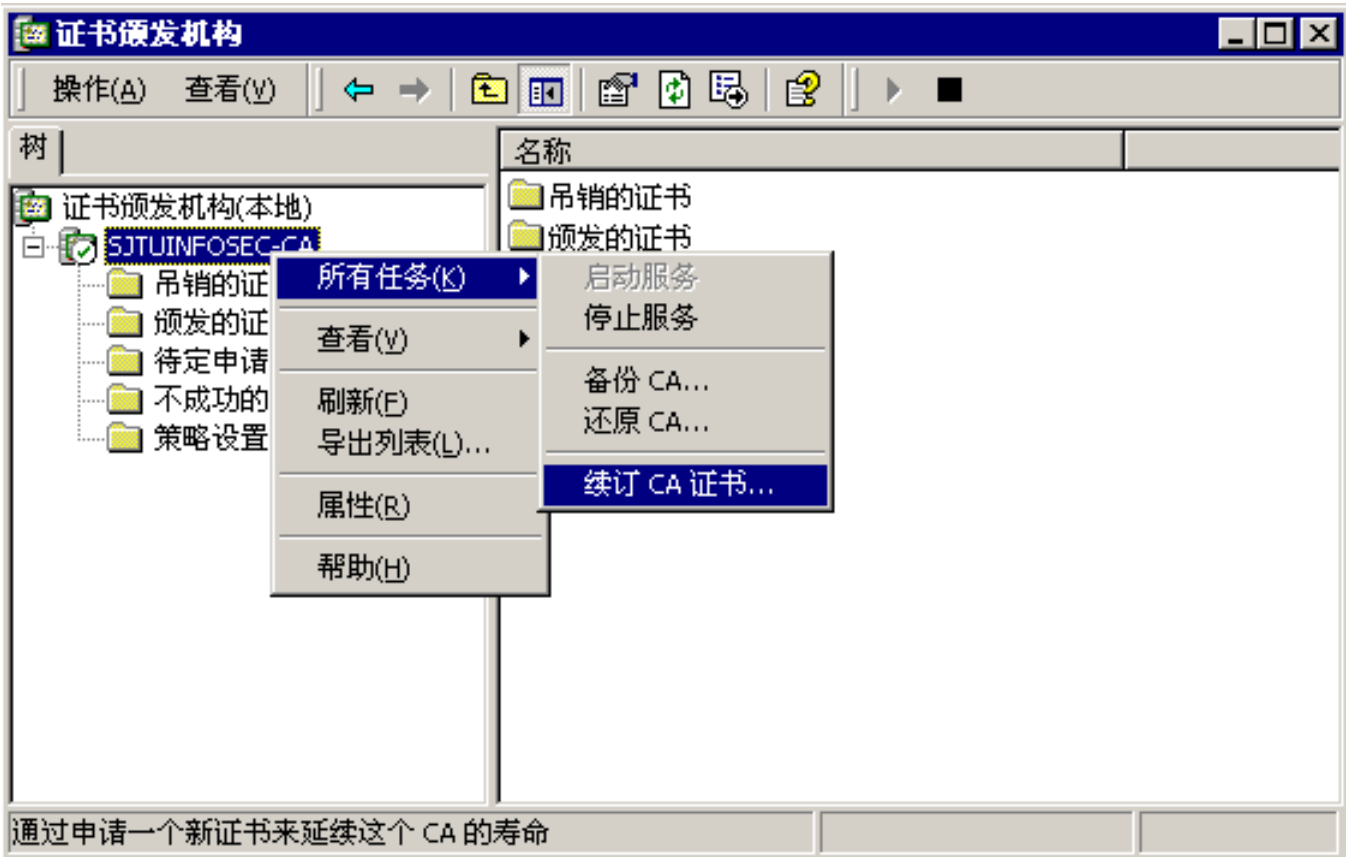


- 灾难恢复
- 从用户原来的计算机转移到新的计算机中
- 安装原来的证书

导出和导入格式

- 个人信息交换 (PKCS #12)
  - 业界格式，是 Windows 2000 中支持的导出证书及相关私钥的唯一格式。
  - 证书用于 EFS（加密文件系统）或 EFS 故障恢复才可导出私钥。
- 加密消息语法标准 (PKCS #7)
  - 允许将证书及证书路径中的所有证书从一台计算机传输到另一台计算机或可移动媒体。
  - 扩展名为.p7b。
- DER 编码的二进制 X.509
  - 可由不在 Windows 2000 服务器上的证书颁发机构使用，因此它支持互操作性。
  - 扩展名为.cer。
- Base64 编码的 X.509
  - 同上。

证书的更新


证书颁发机构
操作(A)
查看(V)
树
名称
证书颁发机构(本地)
SJTUINFOSEC-CA
吊销的证书
颁发的证书
吊销的证
颁发的证
待定申请
不成功的
策略设置
所有任务(K)
查看(V)
刷新(F)
导出列表(L)...
属性(R)
帮助(H)
启动服务
停止服务
备份 CA...
还原 CA...
续订 CA 证书...
通过申请一个新证书来延续这个 CA 的寿命

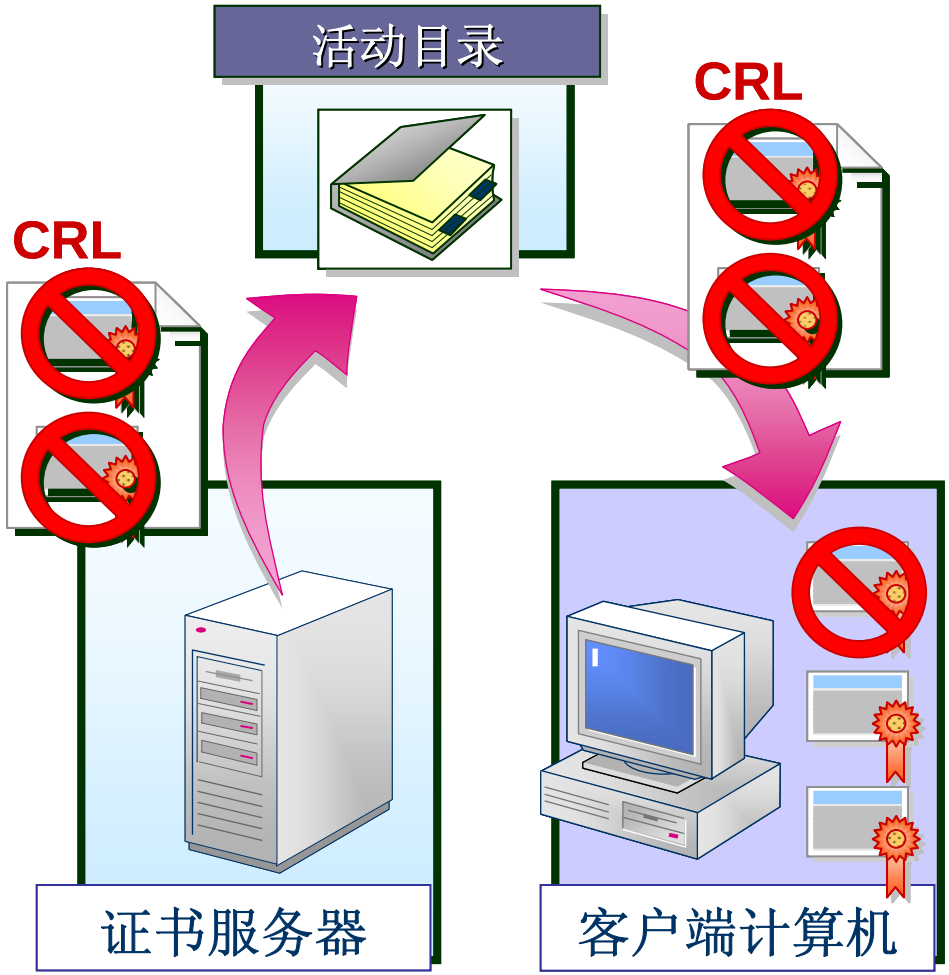
证书的吊销

- 证书为什么需要吊销？
  - 证书受领人已离开单位
  - 证书受领人的私钥已泄露
  - 其他一些与安全相关的事件规定它不再需要将证书视为“有效”。
- 证书吊销列表（CRL）
  - 当证书被CA吊销时，它将被添加到该CA的证书吊销列表中。

证书的吊销 —— 安排CRL的发布

- **CRL的发布期**
  - 发布期是CA自动发布更新的CRL的时间间隔。
- **CRL的有效期**
  - 有效期是证书验证者将CRL视为权威的时间段。
  - 只要证书验证者在其本地缓存中具有有效的CRL，它就不会尝试从发布它的CA检索另一个CRL。
  - 默认情况下，证书服务将发布期延长10%（最多可加上12个小时）来建立有效期。

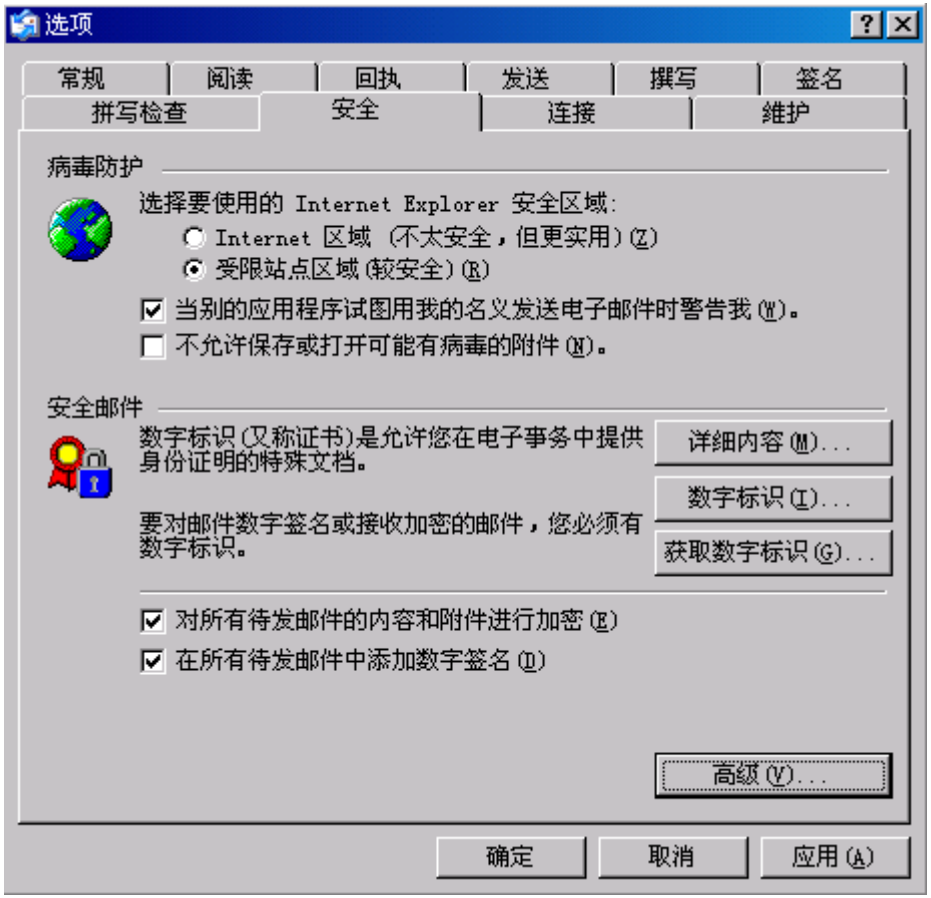
CRL的发布和客户端的缓存



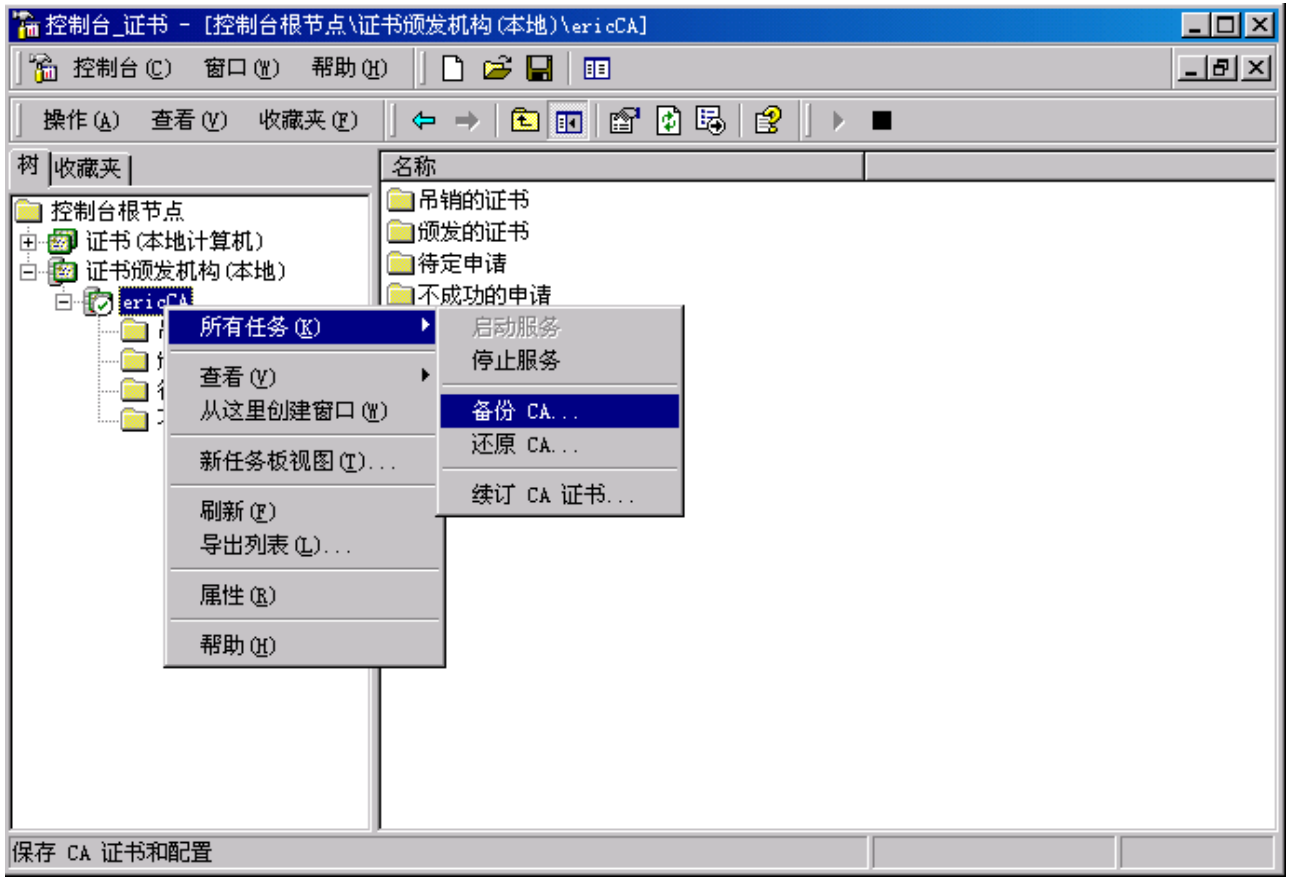
证书使用方法

- WEB服务的安全
  - 用SSL加密IIS的传输
- E-mail的安全
- 加密文件系统（EFS）
- IPSec证书
- 智能卡登录
- 数字签名

安全 E-mail


选项
常规
阅读
回执
发送
撰写
签名
拼写检查
安全
连接
维护
病毒防护
选择要使用的 Internet Explorer 安全区域:
Internet 区域 (不太安全，但更实用)(Z)
受限站点区域(较安全)(R)
当别的应用程序试图用我的名义发送电子邮件时警告我(W)。
不允许保存或打开可能有病毒的附件(N)。
安全邮件
数字标识(又称证书)是允许您在电子事务中提供身份证明的特殊文档。
详细内容(M)...
数字标识(I)...
获取数字标识(G)...
要对邮件数字签名或接收加密的邮件，您必须有数字标识。
对所有待发邮件的内容和附件进行加密(E)
在所有待发邮件中添加数字签名(D)
高级(V)...
确定
取消
应用(A)

证书服务的备份和还原


控制台_证书 - [控制台根节点\证书颁发机构(本地)\ericCA]
控制台(C)
窗口(W)
帮助(H)
操作(A)
查看(V)
收藏夹(F)
树
收藏夹
控制台根节点
证书(本地计算机)
证书颁发机构(本地)
ericCA
名称
吊销的证书
颁发的证书
待定申请
不成功的申请
所有任务(K)
查看(V)
从这里创建窗口(W)
新任务板视图(T)...
刷新(F)
导出列表(L)...
属性(R)
帮助(H)
启动服务
停止服务
备份 CA...
还原 CA...
续订 CA 证书...
保存 CA 证书和配置

SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消