

第3章 PKI 技术

本章内容

- ❖ 3.1 PKI技术的引入
- ❖ 3.2 数字证书
- ❖ 3.3 PKI的组成
- ❖ 3.4 PKI应用与典型案例

3.1 PKI技术的引入



数字化社会，如何确定对方的身份

❖ Internet上没人知道你是一只狗



在网络虚拟世界里，我如何相信你？

网络中需要实现的安全功能

1.1你是谁?

1.1我是Bob.

1.2怎么确认你是Bob?

1.2 我有数字身份证.

• 认证

2.你能读取信息,
但不能修改

2. 我能干什么?

• 授权

3. 使用密钥加密消息。

• 保密性

• 完整性

• 防抵赖

3.如何让别人无法偷听?

4.别怕,你把
消息生成摘要
要发给我,
我来验证

4.如何保证信息
不能被篡改?

5.我有你的罪证, 你每次来访问系
统都留有你的指纹。

5.我偷了机密文件,我不承认。



Internet/Intranet



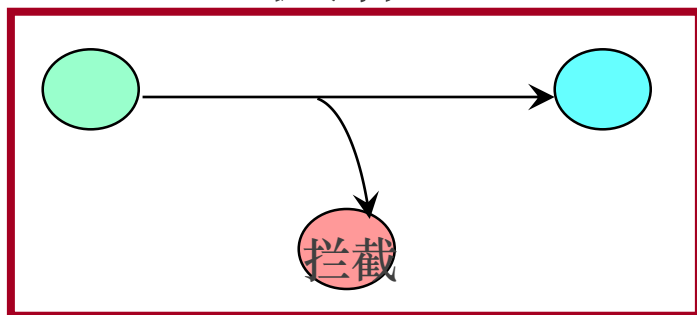
Bob



Alice

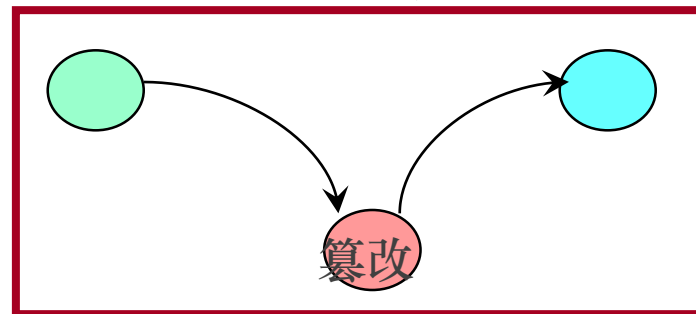
网络通讯的四个安全要素

机密性



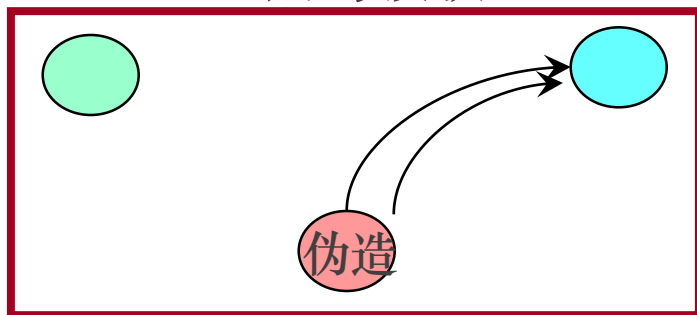
通讯是否安全?

完整性



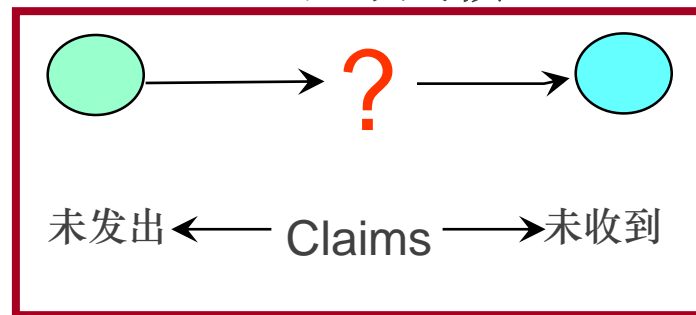
发出的信息被篡改过吗?

鉴别与授权



我在与谁通讯?/是否有权?

不可抵赖



是否发出/收到信息?

如何解决网络通讯中的安全要素

信任类型	现实世界	数字世界
身份认证	身份证、护照、信用卡、驾照	数字证书、数字签名
完整性	签名、支票、第三方证明	数字签名或MAC
保密性	保险箱、信封、警卫、密藏	对称加密或公钥加密
不可否认性	签名、挂号信、公证、邮戳	数字签名

太麻烦啦，有没有一个系统包括上面所有的技术

有效的解决方案 — PKI

❖ 公钥基础设施 (Public Key Infrastructure)

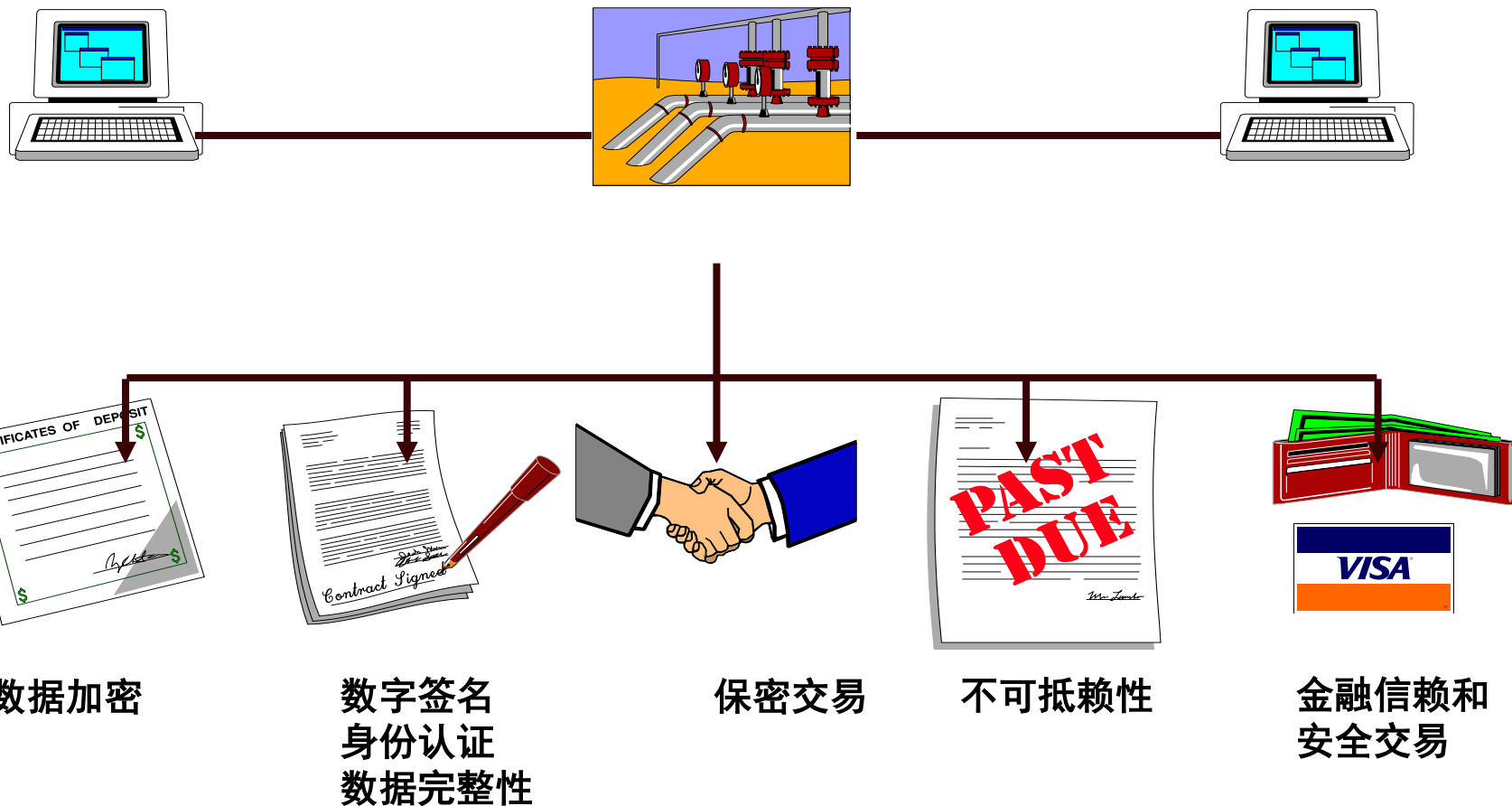


❖ 利用公开密钥理论和技术建立的提供安全服务的在线基础设施。它利用加密、数字签名、数字证书来保护应用、通信或事务处理的安全。

- 基于公钥理论
 - 相对于传统的秘密密钥（对称密钥）算法
- 基础设施
 - 如同电力基础设施为家用电器提供电力一样
 - PKI为各种互联网应用提供安全保障

PKI 可以提供的安全服务

以PKI为基础的安全网络

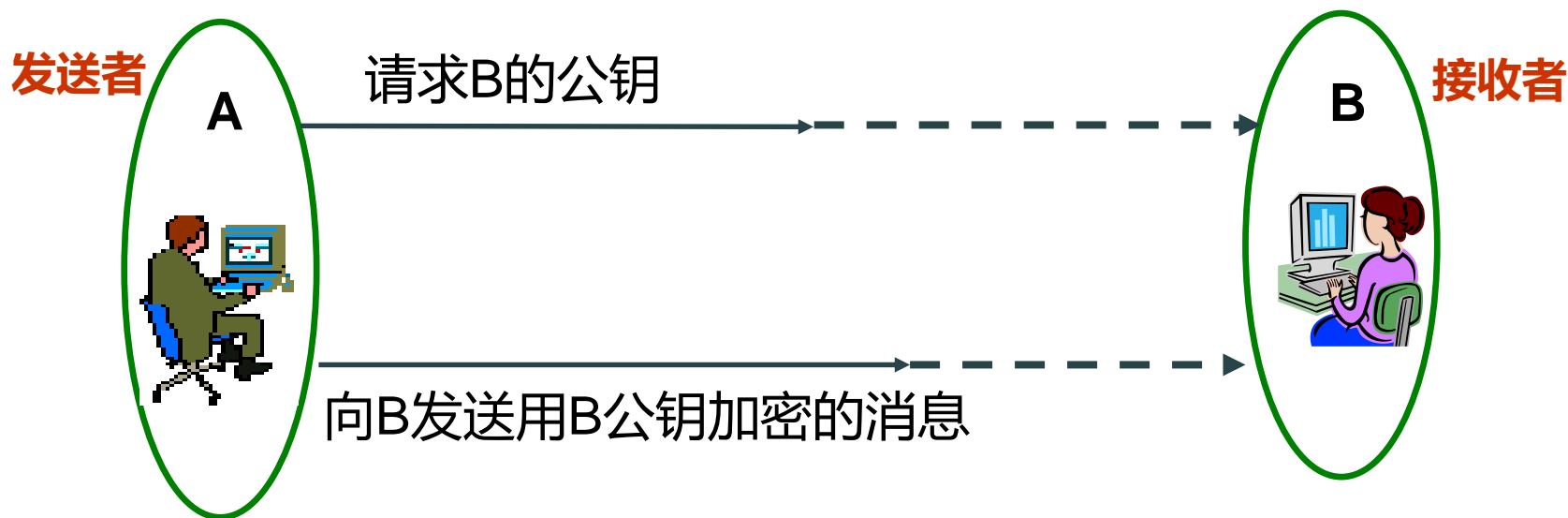


3.2 数字证书



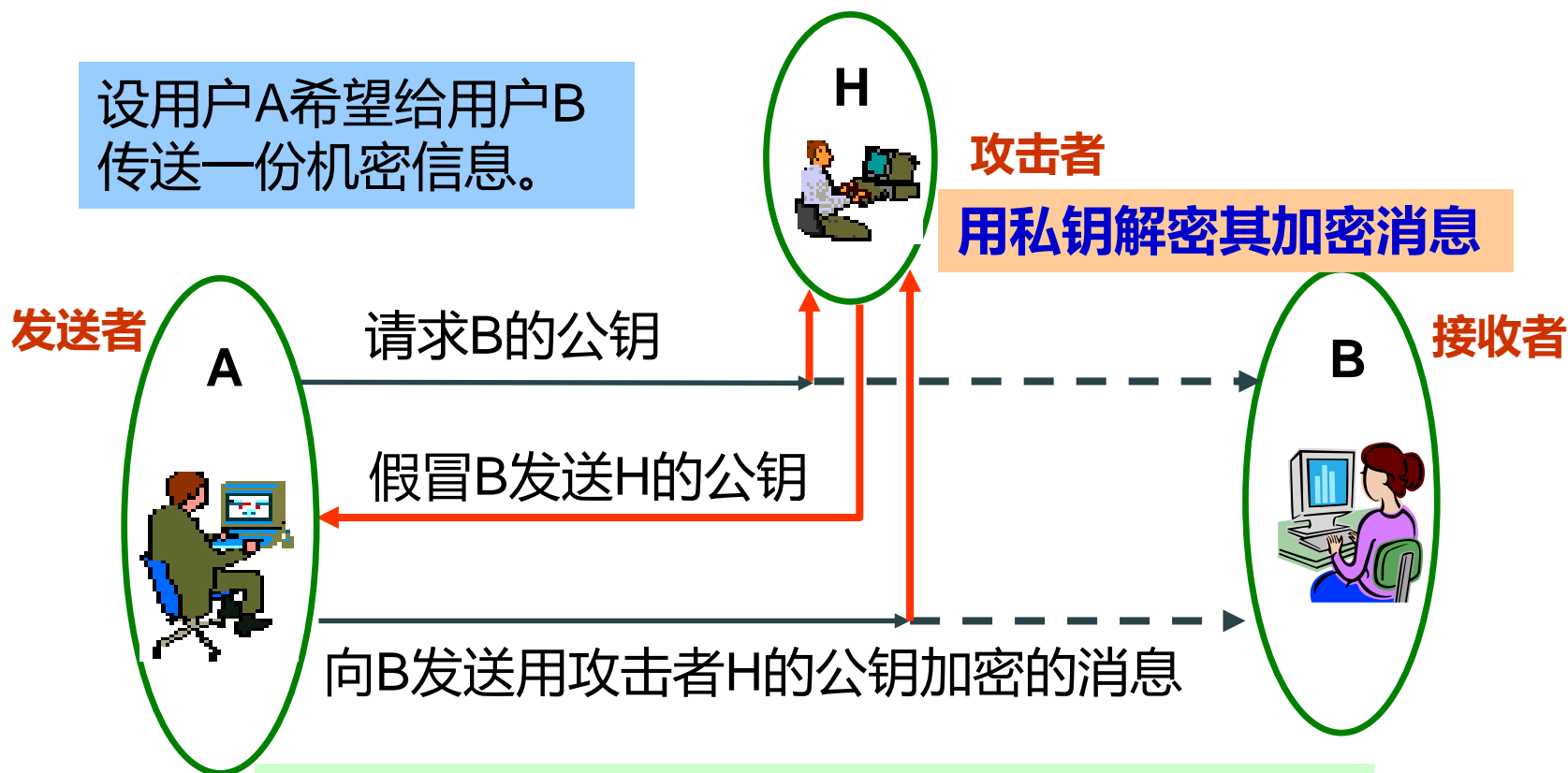
数字证书的提出

设用户A希望给用户B
传送一份机密信息。



数字证书的提出

- ❖ 怎样才能知道任意一个公开密钥是属于谁的？如果收到一个自称是某人的公开密钥，能相信它吗？



问题所在：对公钥缺乏鉴别机制！

什么是数字证书？



数字证书的概念： 一个用户的身份与其所持有的公钥的结合，由一个可信任的权威机构CA来证实用户的身份，然后由该机构对该用户身份及对应公钥相结合的证书进行数字签名，以证明其证书的有效性。

如果让你设计数字证书，
你怎么设计？

数字证书 VS 身份证

- ◆ 姓名：王明
- ◆ 序列号：
484865
- ◆ 签发者：XXXCA
- ◆ 发布时间：2002-01-01
- ◆ 有效时间：2002-12-31
- ◆ Email：wm@sina.com.cn
- ◆ 公钥：38ighwejb
- ◆

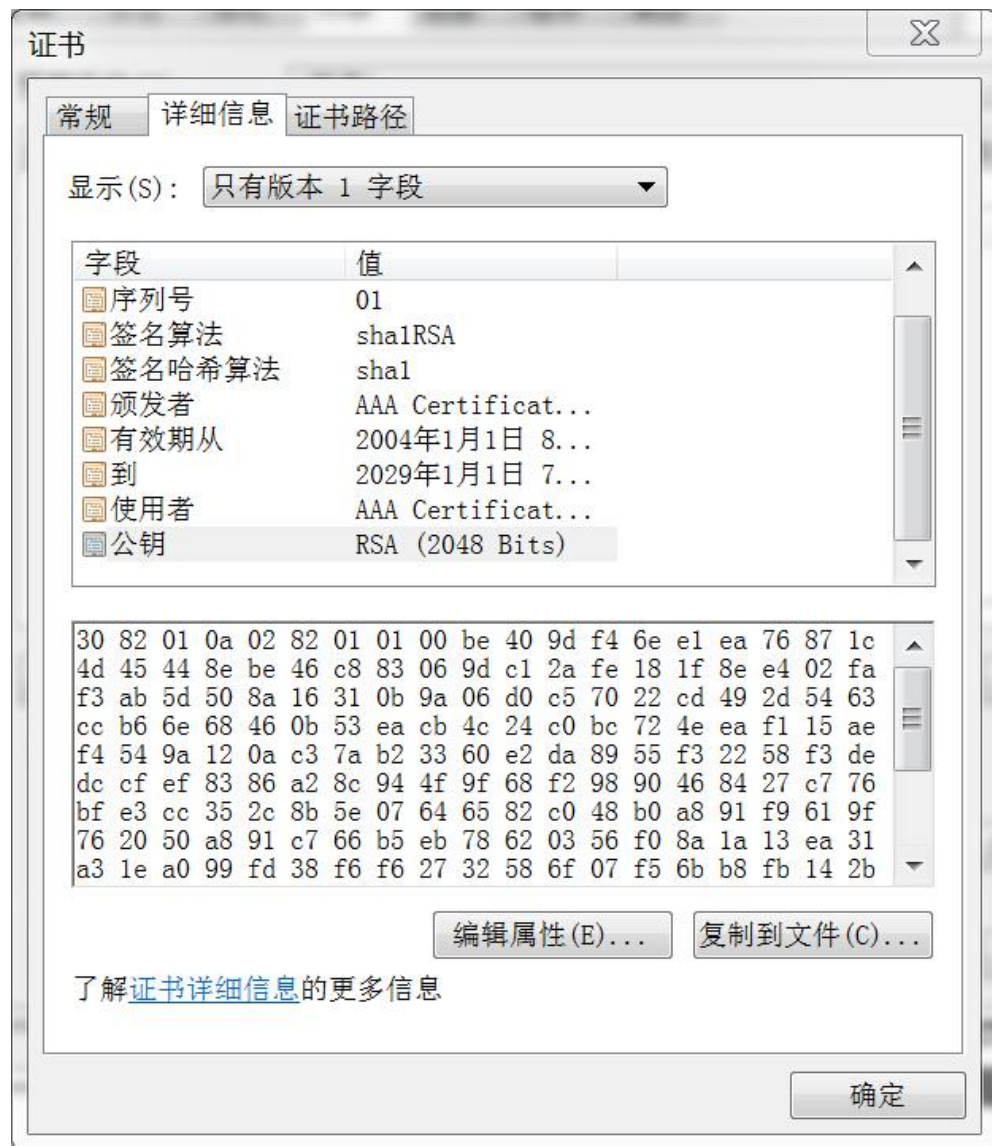
- ◆ 姓名：王明
- ◆ 编号：
110104197312061536
- ◆ 签发者：北京市公安局海淀分局
- ◆ 发布时间：2000-04-05
- ◆ 有效期：20年
- ◆ 住址：北京市海淀区中科院南路6号

数字证书格式——X. 509

基于PKI的数字证书将公钥与其用户的身份捆绑在一起，证书必须要有一定的标准格式。目前广泛采用的证书格式是国际电信联盟（ITU）提出的X.509v3格式。

内容	说明
版本V	X. 509版本号
证书序列号	用于标识证书
算法标识符	签名证书的算法标识符
参数	算法规定的参数
颁发者	证书颁发者的名称及标识符(X.500)
起始时间	证书的有效期
终止时间	证书的有效期
持证者	证书持有者的姓名及标识符
算法	证书的公钥算法
参数	证书的公钥参数
持证书人公钥	证书的公钥
扩展部分	CA对该证书的附加信息，如密钥的用途
数字签名	证书所有数据经H运行后CA用私钥签名

数字证书实例



3.3 PKI 的组成



PKI 系统的组成

一个PKI系统由以下几部分构成：

❖ 证书认证机构

Certification Authorities (CA)

❖ 证书注册机构

Registration Authorities (RA)

❖ 证书持有者

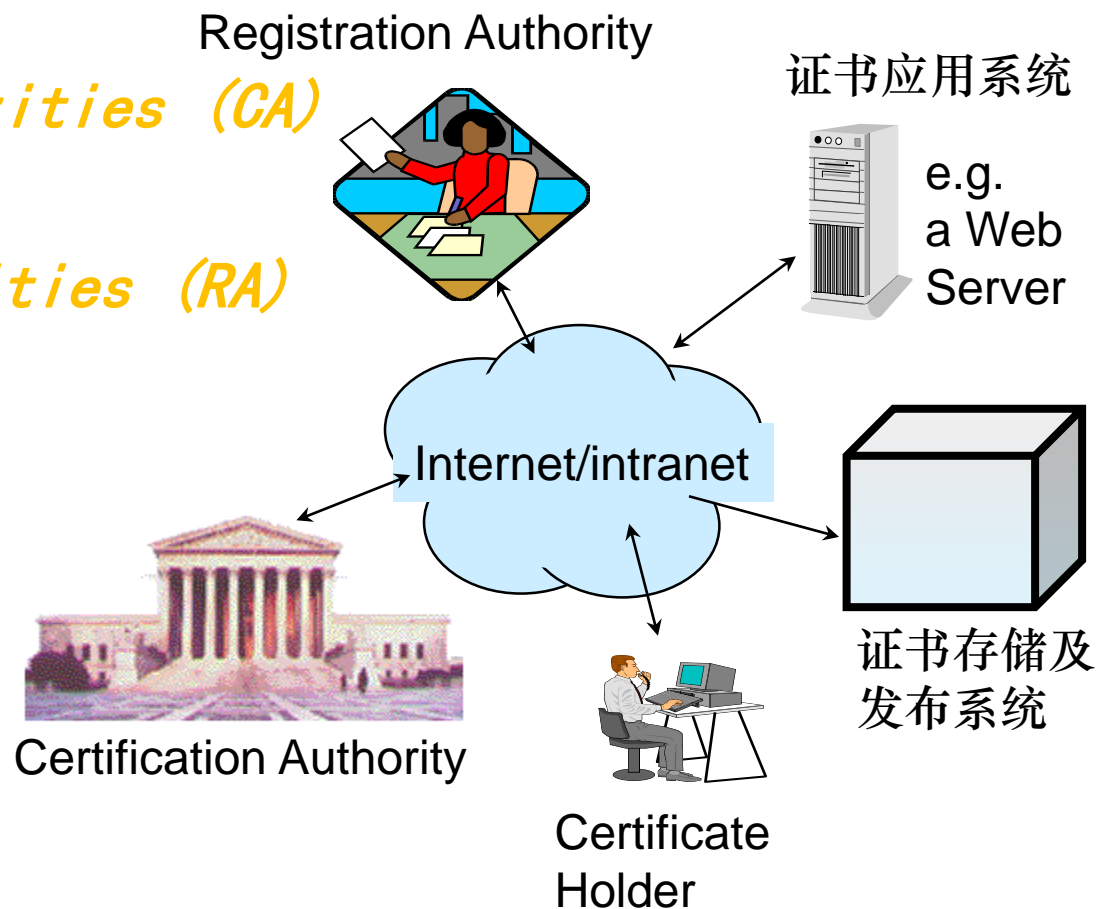
Certificate Holders

❖ 证书应用系统

Relying Parties

❖ 证书存储及发布系统

Repositories



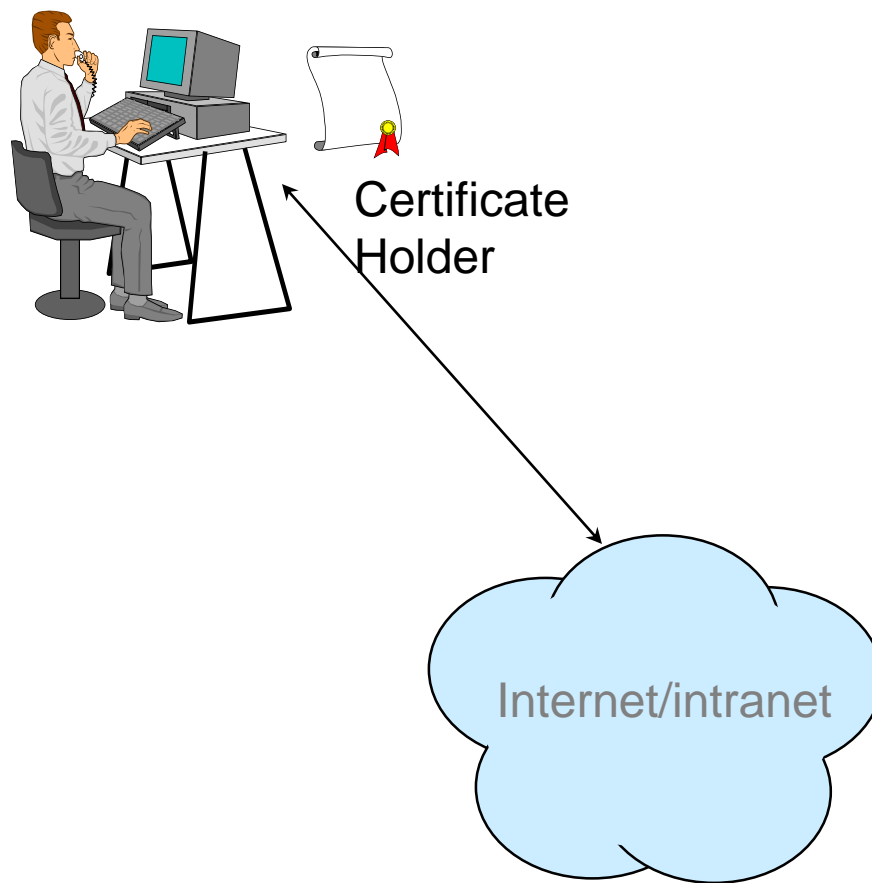
1. 证书持有者

❖ 机关

❖ 企业

❖ 个人

❖ 服务器



2. 证书认证机构（CA）

思考：为什么要设立一个证书认证机构CA？

必须有一个可信任的机构对任何一个主体公钥进行公证，证明主体的身份以及它与公钥的匹配关系。

CA的基本功能：

- ❖ 签发数字证书
- ❖ 证书管理：对证书进行管理，包括颁发、废除、更新、验证证书和管理密钥。
- ❖ CA密钥的管理
- ❖ 提供证书和证书状态查询



3. 证书注册机构 (RA)

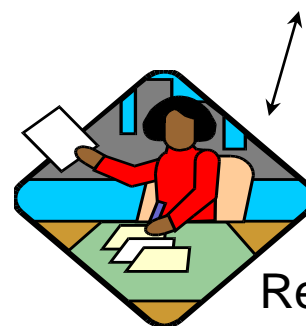
由于认证机构CA的任务很多，如签发新证书、维护旧证书、撤销因故无效的证书等，因此可以将手里证书申请的工作转交给第三方：注册机构RA。

RA的基本功能：

- ❖ 受理最终客户的证书申请和管理请求
- ❖ 对证书申请者身份进行审核并提交CA制证
- ❖ 提供证书生命期的维护工作



Certification Authority



Registration Authority



User

4. 证书存储和发布系统

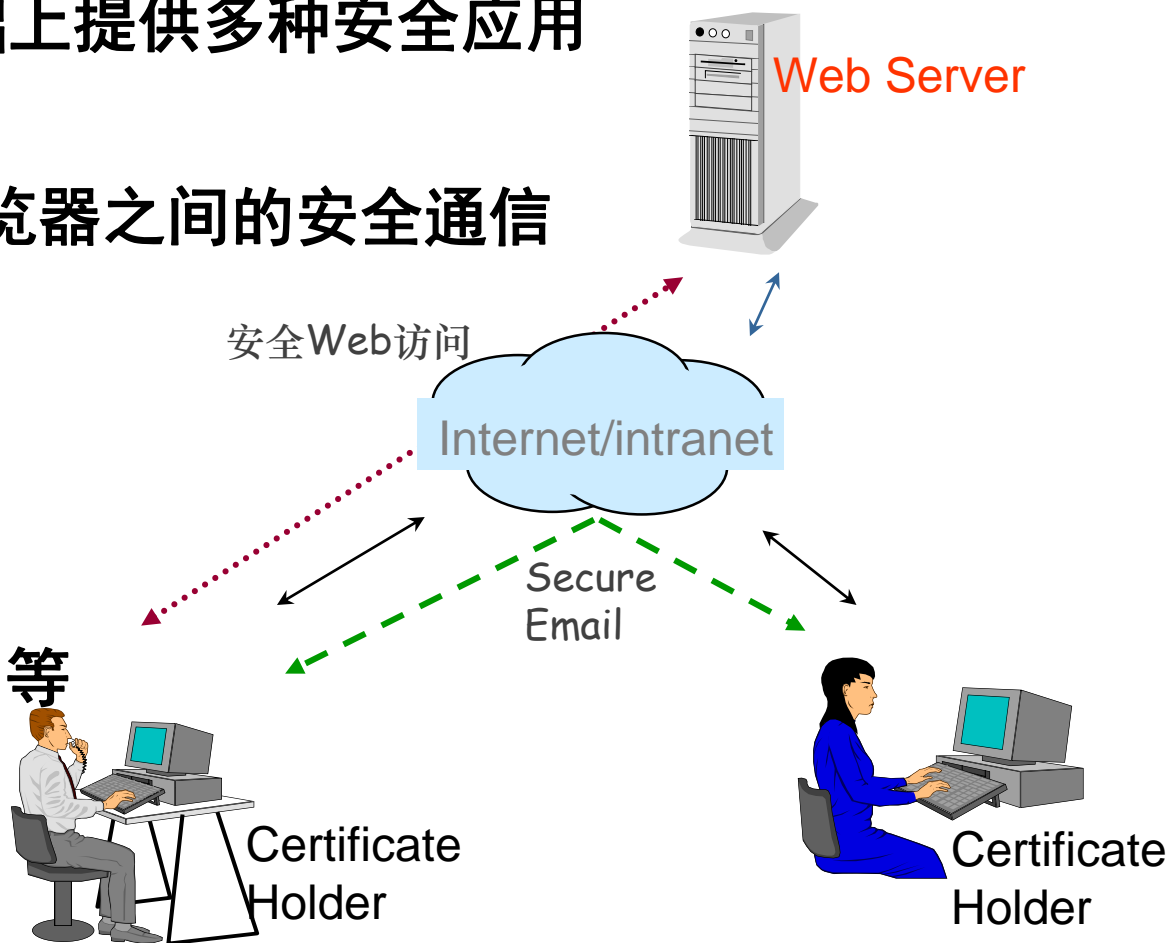
- ❖ 证书存储和发布系统负责证书的分发，用户可在此获取自己或其它用户的证书。
- ❖ 证书分发可有多种途径，如：用户自己发布，或通过目录服务器向外发布。
- ❖ **证书库**是一种网上公共信息库，用于证书的集中存放，用户可以从此处获得其他用户的证书和公钥。实现证书库的方式有多种，包括**X. 500**、**轻量级目录访问协议(LDAP)**、Web服务器、FTP服务器、域名解析服务器DNS、数据库服务器等。具体使用哪种根据实际需要而定，但真正大型的企业级PKI一般使用X. 500目录服务和轻量级目录访问协议LDAP。

5. 证书应用系统

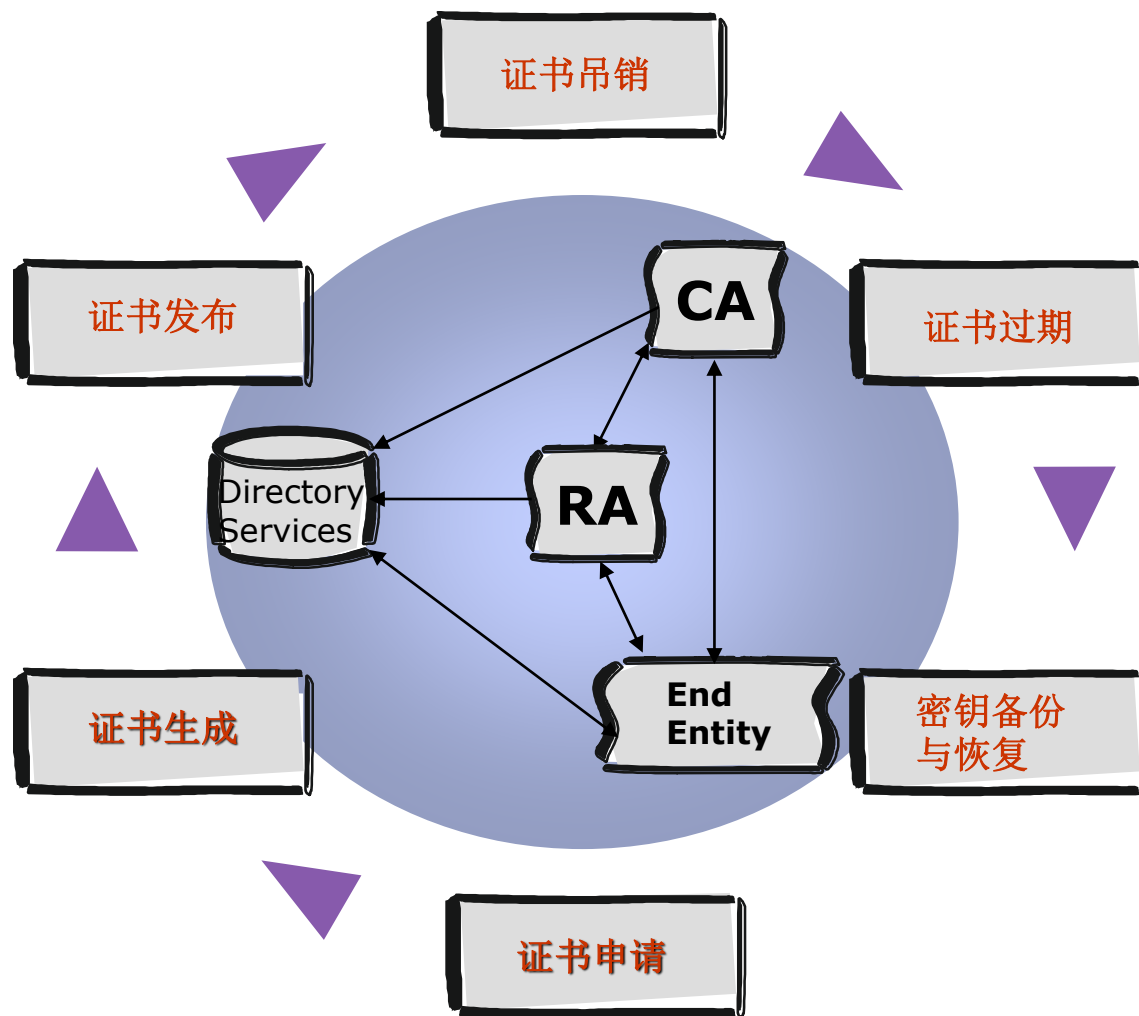
一个完整的PKI系统必须提供良好的应用接口，可以在此基础上提供多种安全应用服务。如

- ❖ 实现Web服务器和浏览器之间的安全通信
- ❖ 安全电子邮件
- ❖ 电子数据交换(EDI)
- ❖ 网上的信用卡交易
- ❖ 安全虚拟专网(SVPN)等

证书应用系统



数字证书的生命周期



证书撤销

❖ 证书在有效期之内由于某些原因可能需要废除

废除证书的原因

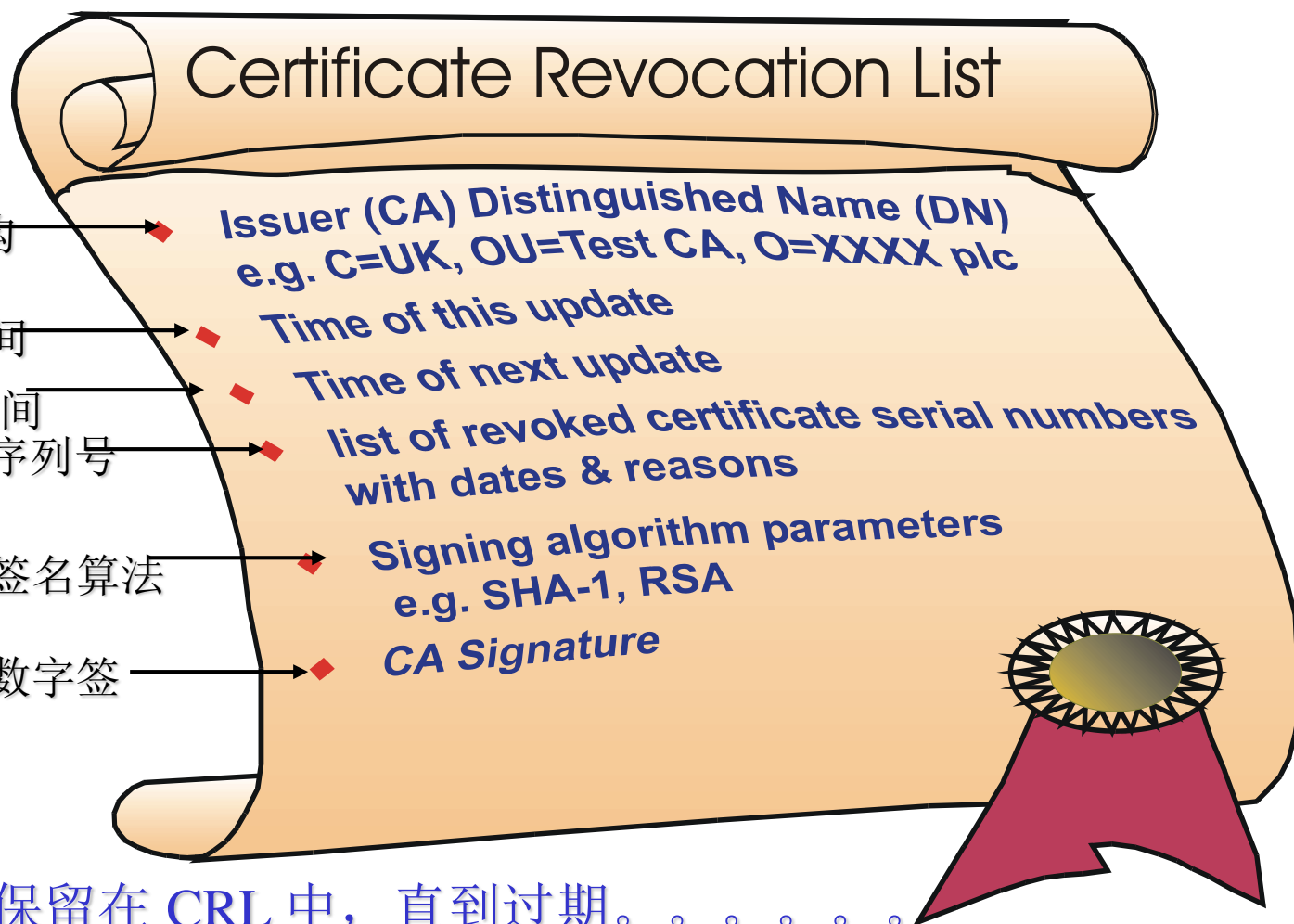
- ❑ 证书用户身份信息的变更
- ❑ CA签名私钥的泄漏
- ❑ 证书对应私钥的泄漏
- ❑ 证书本身遭到损坏
- ❑ 其他原因

❖ 废除证书一般是把证书列入证书撤销列表（CRL）中来实现

证书撤销列表

- ❖ 采用“坏”证书列表，由CA周期性发布，最终用户本地存储
- ❖ 优点：
 - 我们不需要直接接触CA也能验证证书
 - 降低 CA的通信需求
- ❖ 缺点：
 - 在我们得到最新列表之前，证书可能已经变坏
 - 列表可能巨大

证书撤销列表——黑名单



签发本黑名单的CA机构

本黑名单的签发时间

下次发布黑名单的时间

被列入黑名单的证书序列号

CA对黑名单签名的签名算法

CA机构对黑名单的数字签名

被撤销的证书一直保留在 CRL 中，直到过期。。。。。。

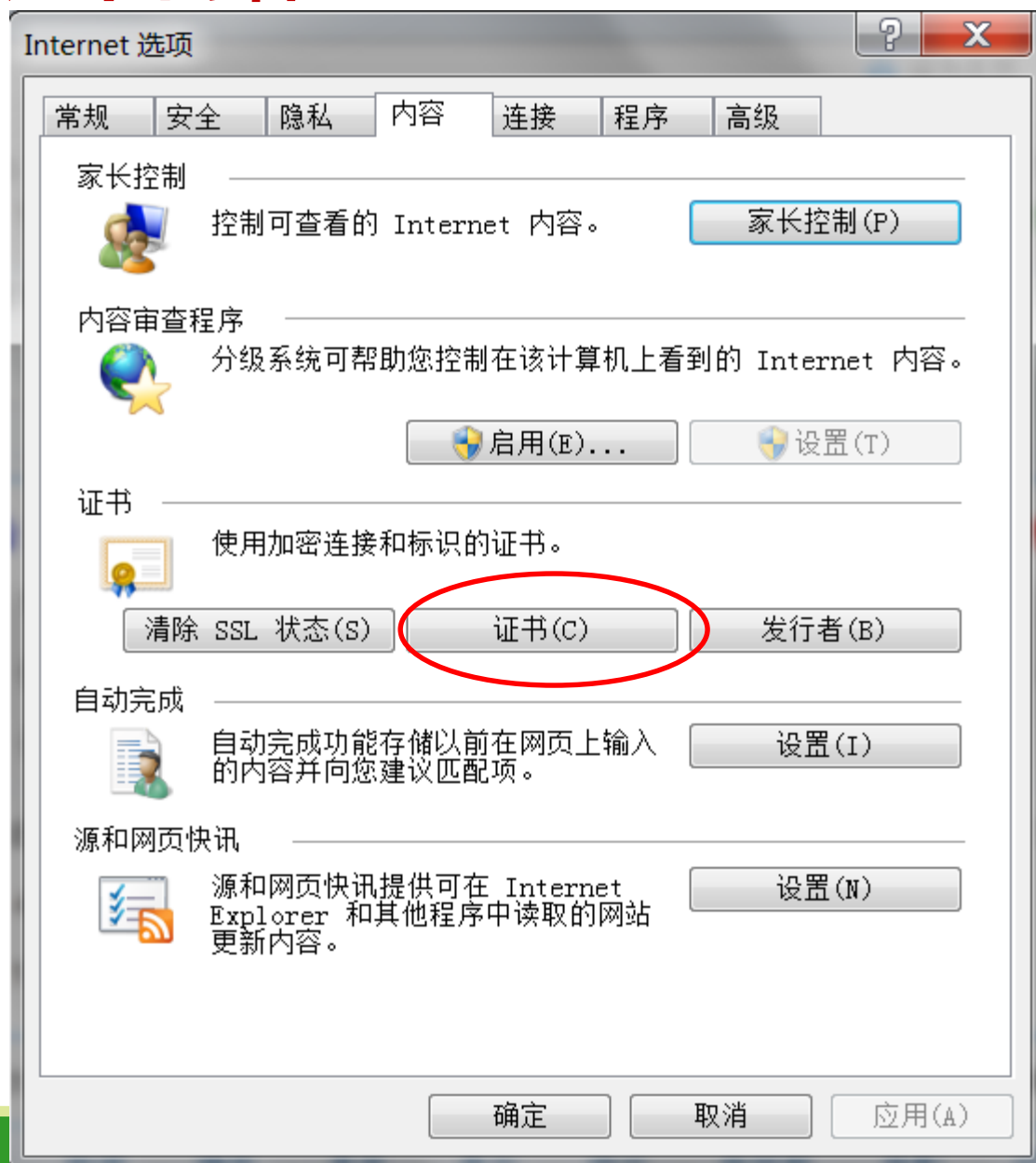
3.4 PKI 应用与典型案例



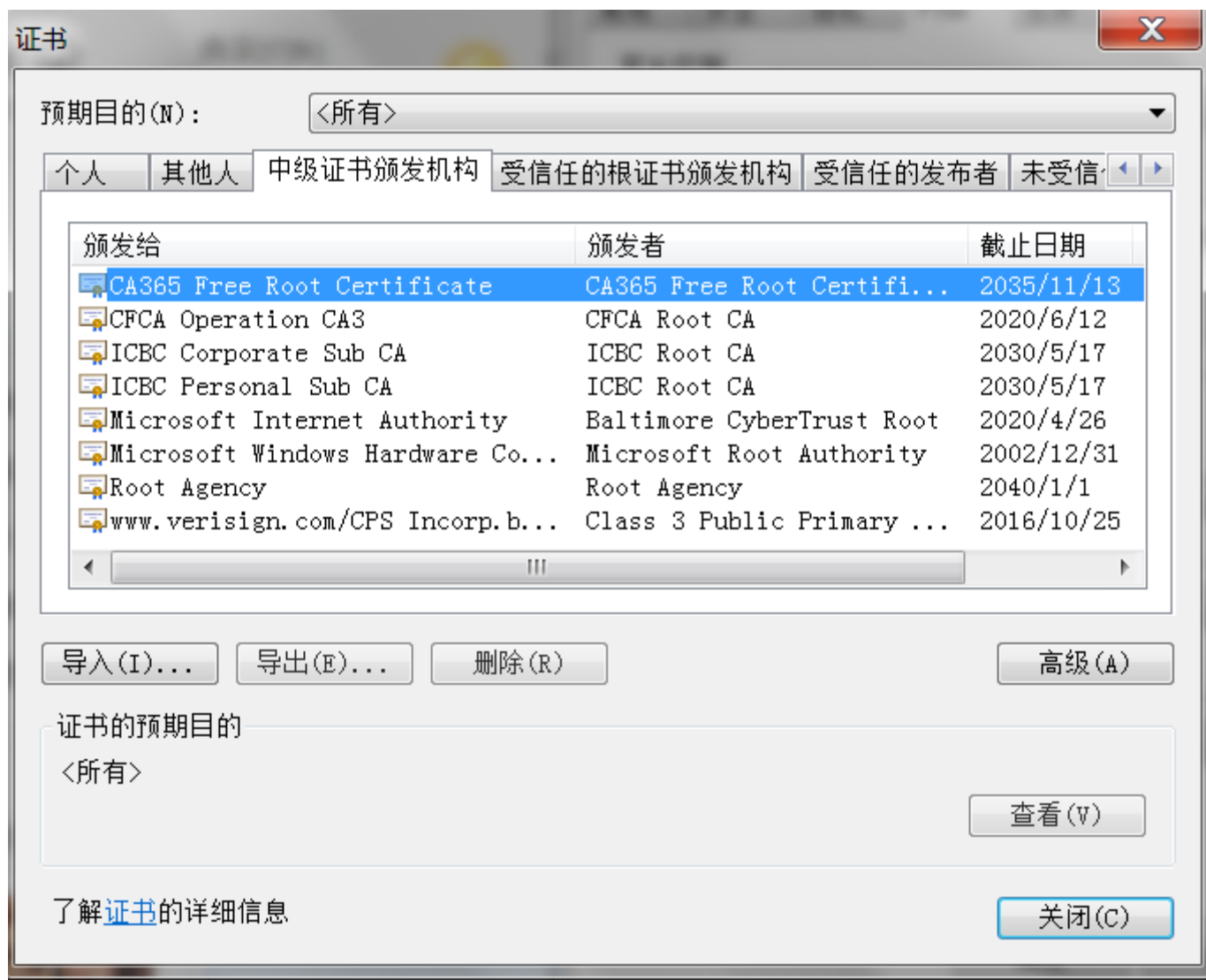
PKI 应用与典型案例

- (1) 查看数字证书内容
- (2) 国内外CA简介
- (3) 数字证书的申请及应用操作实例

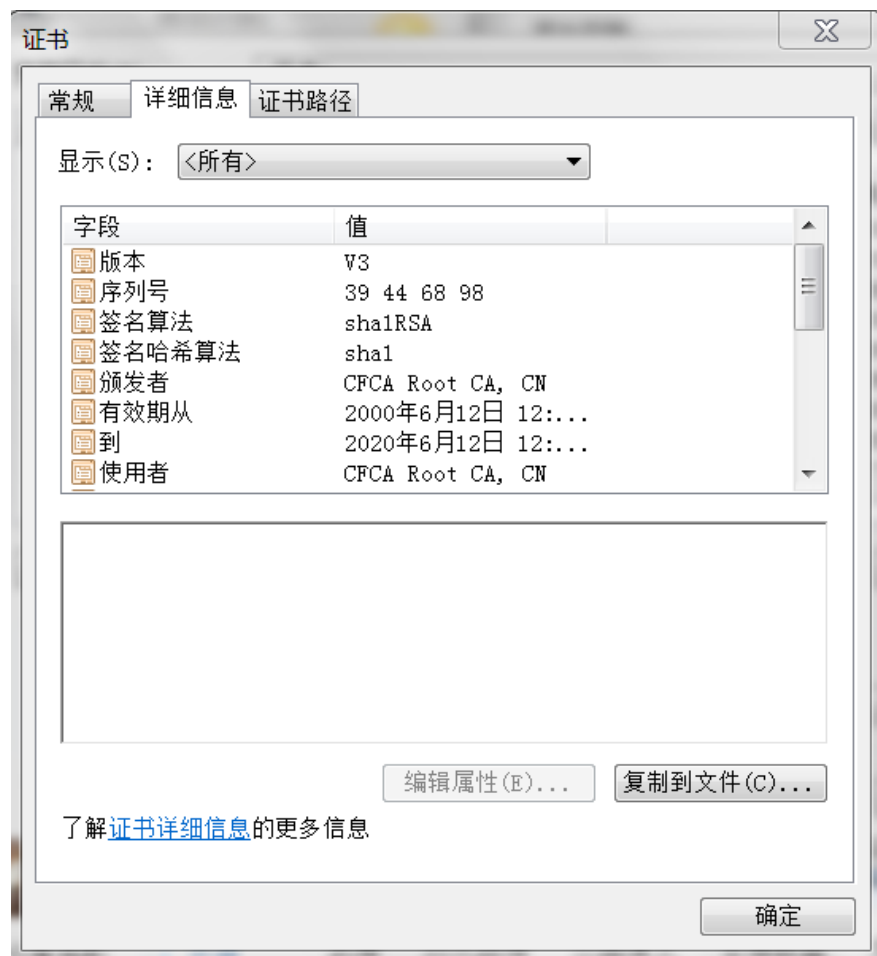
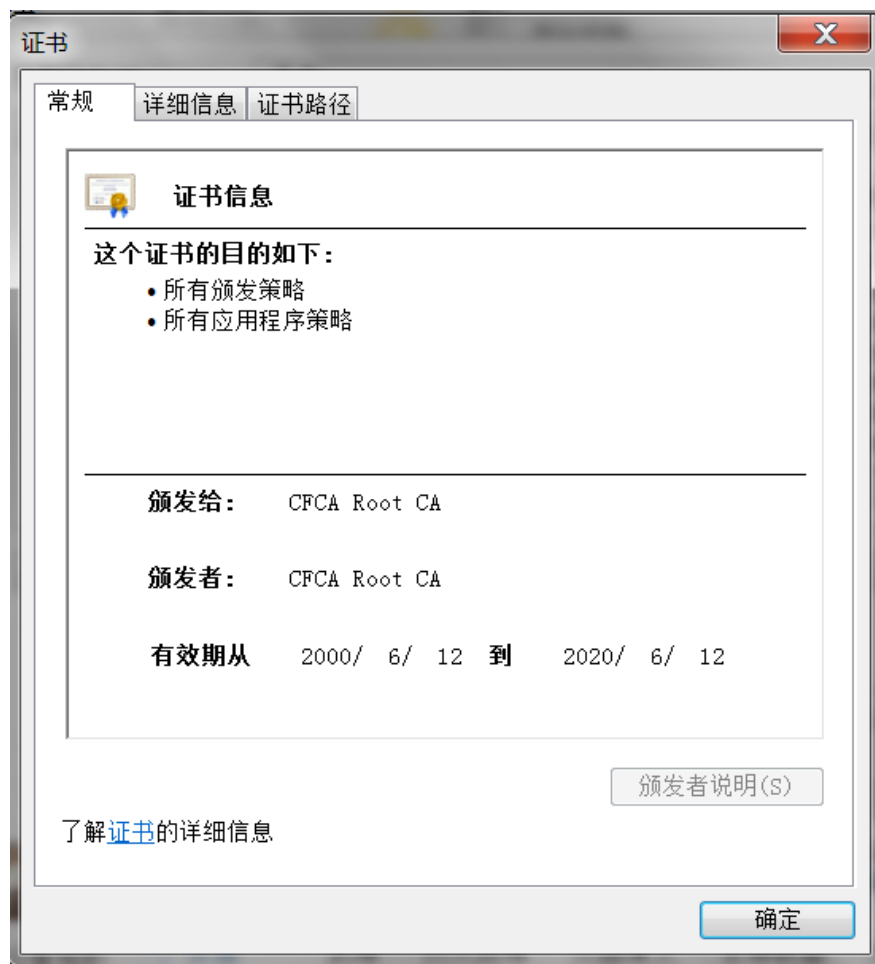
查看数字证书内容



查看数字证书内容



查看数字证书内容



国内外CA简介

❖ 国外常见的有：Verisign、Entrust，它们是目前世界最著名的两大CA

❖ 国内常见的CA有：

中国数字认证网

(<http://www.ca365.com>)

天威诚信安全身份认证服务中心

(<http://www.itrus.com.cn>)

中国金融认证中心

(<http://www.cfca.com.cn>)

数字证书的申请

1. 证书的获得和安装

(1) 登录中国数字认证网，安装根CA证书。只有安装了根证书(证书链)的计算机，才能完成后面的申请步骤和正常使用数字证书。在提示的界面中，单击“根CA证书”链接，下载并安装根证书

会员登录

用户名：

密 码：

登 录

[忘记密码](#)☐ 记住我的用户名还不是会员？[立即注册](#)，填写资料

重要：WIN7操作系统申请证书，请先下载[WIN7证书补丁](#)并安装。Vista操作系统申请证书，请先下载[Vista证书补丁](#)并安装。

企业证书

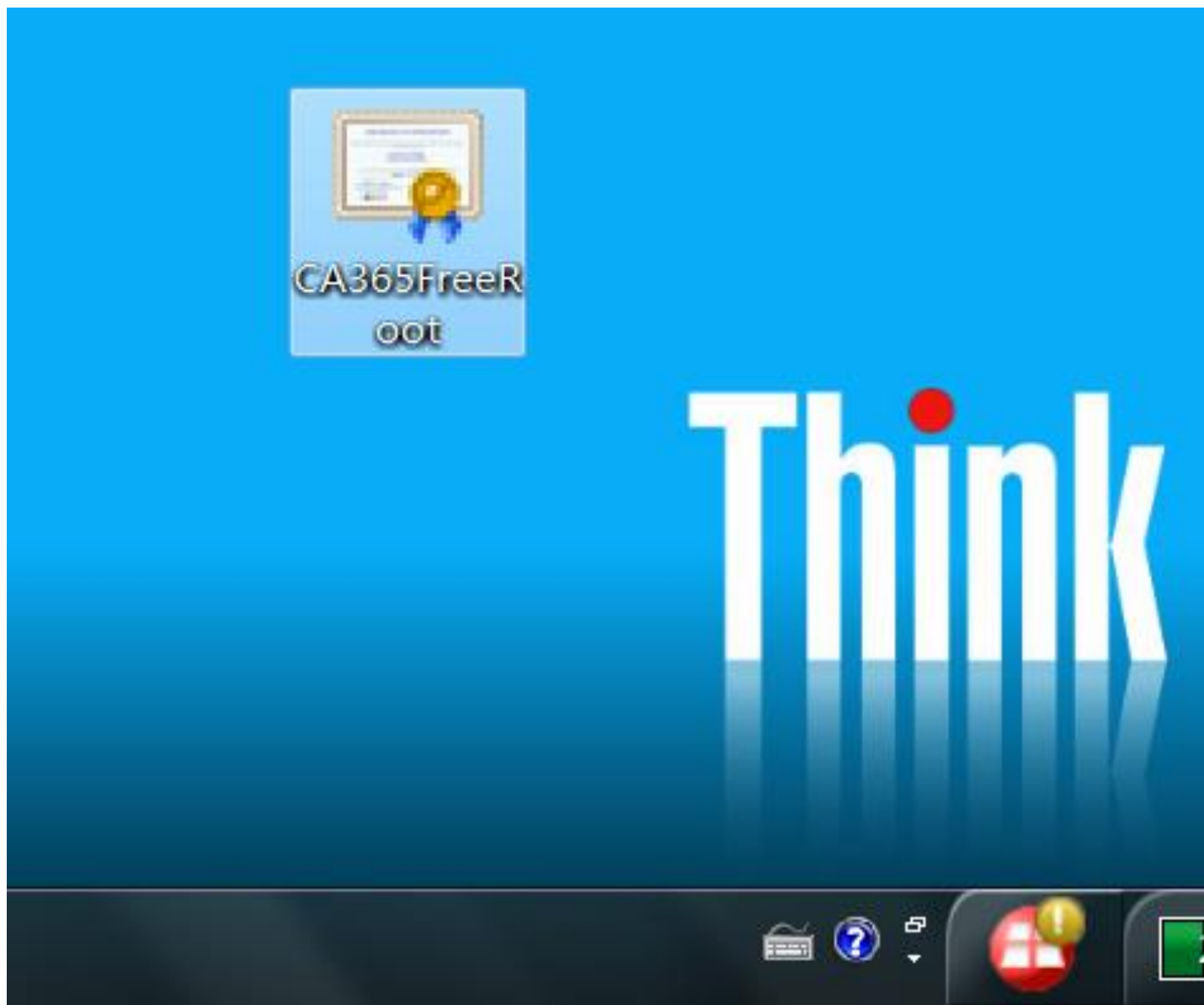
- ▶ 如果您是第一次访问本站点请 [下载并安装根CA证书](#)
- ▶ [用表格申请证书](#)
- ▶ [用PKCS10文件申请证书](#)
- ▶ [证书查询](#)
- ▶ [证书吊销列表](#)
- ▶ [我申请的证书查询](#)

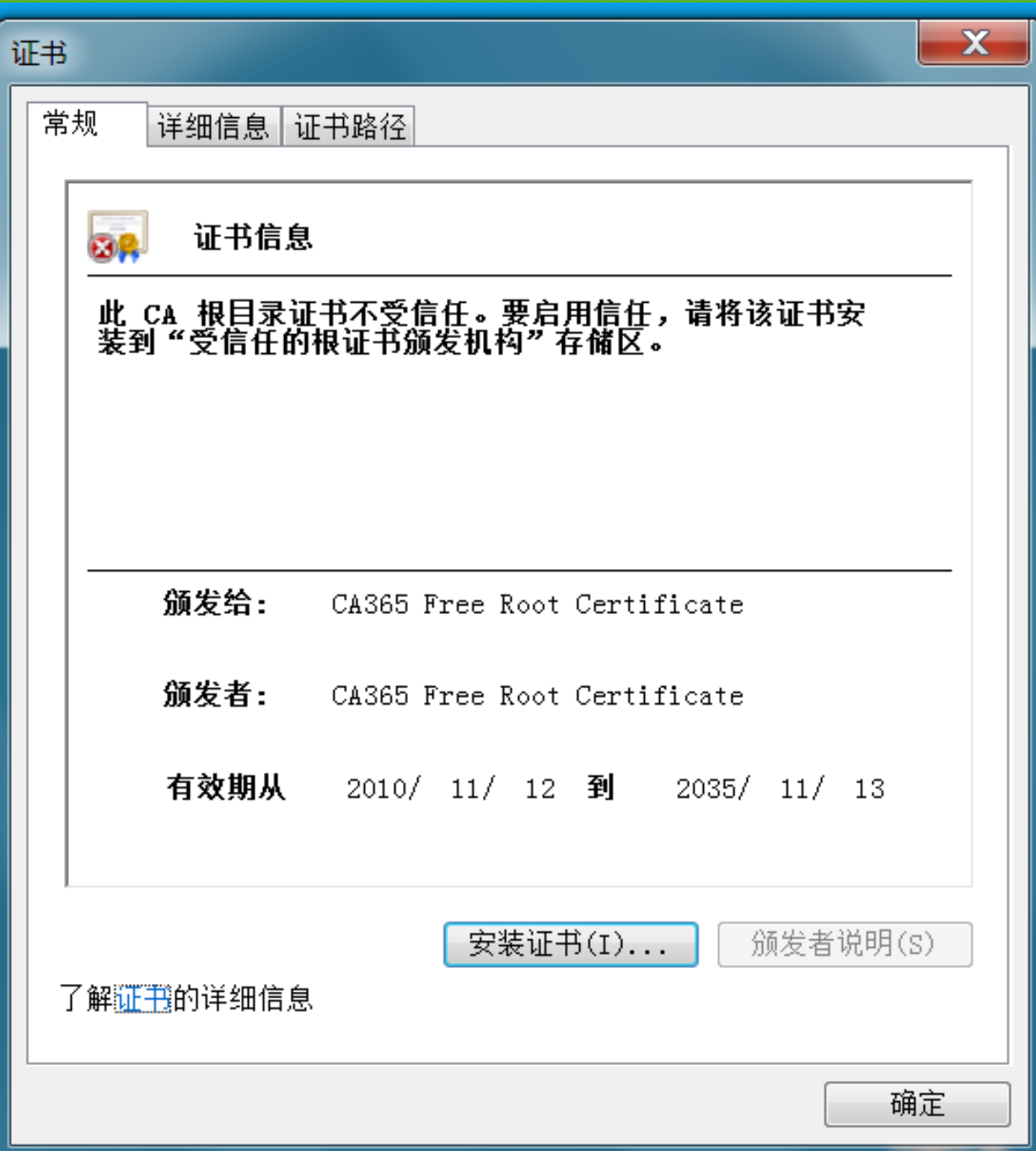
免费证书

- ▶ 如果您是第一次访问本站点请 [下载并安装根CA证书](#)
- ▶ [用表格申请证书](#)
- ▶ [用PKCS10文件申请证书](#)
- ▶ [证书查询](#)
- ▶ [证书吊销列表](#)
- ▶ [我申请的证书查询](#)

测试证书

- ▶ 如果您是第一次访问本站点请 [下载并安装根CA证书](#)
- ▶ [用表格申请证书](#)
- ▶ [用PKCS10文件申请证书](#)
- ▶ [证书查询](#)
- ▶ [证书吊销列表](#)





(2) 在测试证书申请区域，单击“用表格申请证书”链接。这时会出现一个表单，按照上面的提示，输入完整的个人资料，然后单击“提交”按钮。

您当前的位置：测试证书 -> 用表格申请证书

名称：平萍

✔ 输入正确

公司：河海大学

✔ 输入正确

部门：计算机与信息学院

✔ 输入正确

城市：南京

✔ 输入正确

省：江苏

✔ 输入正确

国家(地区)：CN

✔ 输入正确

Email：amazingapple@163.com

✔ 输入正确

网址：

请输入

证书用途：☐ 客户身份验证证书 ☒ 电子邮件保护证书 ☐ 代码签名证书 ☐ 时间戳签名证书 ☐ 通用证书

证书吊销方式：☒ 集中吊销 ☐ 单独吊销

档案：☒ 开放（允许您的证书在网上公开检索） ☐ 不开放（不允许您的证书在网上公开检索）

保存

重置

您当前的位置：测试证书 -> 证书下载

加密服务提供： Microsoft Base Cryptographic Provider v1.0 ▼

密钥大小： 1024 ▼

密钥是否可导出： ☒

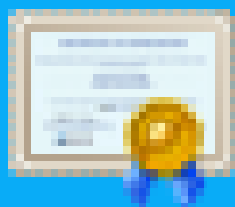
申请证书

加密服务提供： Microsoft Base Cryptographic Provider v1.0

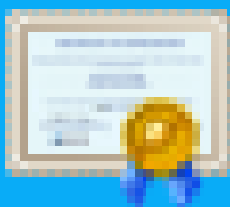
密钥大小： 1024

密钥是否可导出： ☒

下载证书



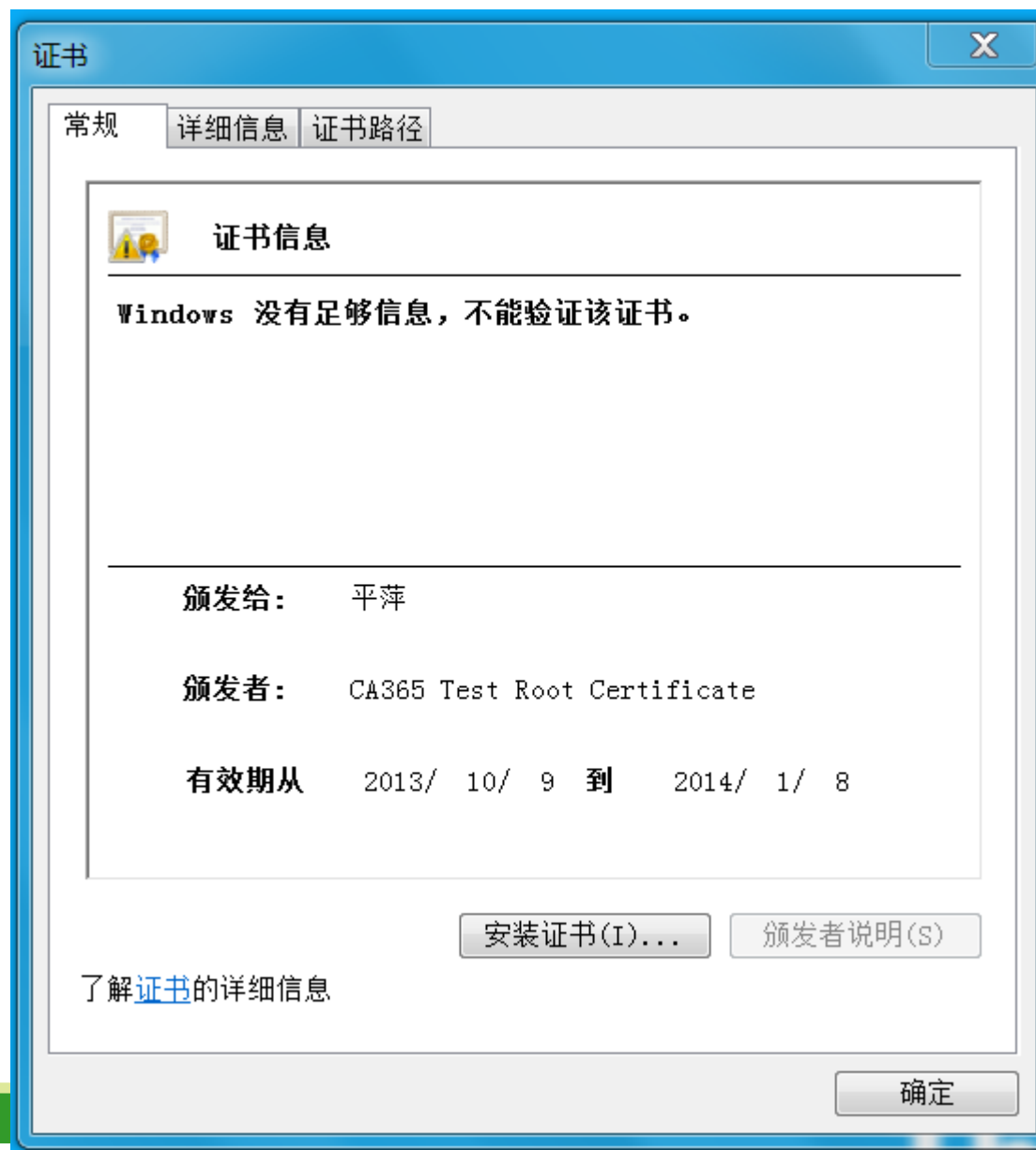
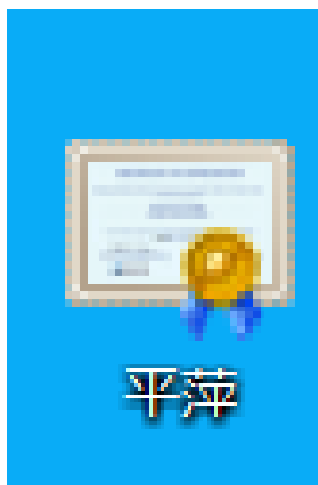
CA365Fre...



平萍

(3) 安装数字证书

双击数字证书
点击安装证书



2. 查看数字证书

首先打开Internet Explorer，执行"工具"菜单中的"Internet选项"命令，在弹出的对话框中，打开"内容"选项卡，单击"证书"按钮，在弹出的对话框中查看用户信任的当前证书的列表。下面是申请的免费数字证书

家长控制



控制可查看的 Internet 内容。

家长控制(P)

内容审查程序



分级系统

证书



使用加密

清除 SSL 状态

自动完成

自动完成的
内容并

源和网页快讯

源和网页
Explore
更新内容

证书

预期目的(N):

<所有>

个人

其他人

中级证书颁发机构

受信任的根证书颁发机构

受信任的发布者

未受信

颁发给

颁发者

截止...

友好名称

平萍

CA365 Test ...

2014...

<无>

导入(I)...

导出(E)...

删除(R)

高级(A)

证书的预期目的

安全电子邮件

查看(V)

了解[证书](#)的详细信息

关闭(C)

数字证书应用操作实例

- ❖ 如何在用Microsoft Outlook Express 发送电子邮件时添加数字签名?
- ❖ 由于越来越多的人通过电子邮件发送机密信息，因此确保电子邮件中发送的文档不是伪造的变得日趋重要。同时保证所发送的邮件不被除收件人以外的其他人截取和偷阅也同样重要。
- ❖ 通过使用 Outlook Express 的“数字证书”，您可以在电子事务中证明您的身份，就像兑付支票时要出示有效证件一样。您也可以使用数字证书来加密邮件以保护个人隐私。

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) (I)☒ 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)。

下载图像

☐ 阻止 HTML 电子邮件中的图像和其他外部内容 (B)。

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)...

要对邮件数字签名或接收加密的邮件, 您必须有数字标识。

获取数字标识 (G)...

☐ 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 (S)

高级 (V)...

确定

取消

应用 (A)

哪里可以获得数字证书？

- ❖ 在想启用此添加数字签名之前，首先要**申请一个数字签名**。
- ❖ 数字证书由**独立的证书颁发机构**发放。在证书颁发机构的网站申请数字证书时，证书颁发机构在发放证书之前将确认您的身份。数字证书有不同的类别，不同类别提供不同的信用级别。

Application for Secure Email Certificate

Your Details

First Name

Last Name

Email Address

Country

United States ▼

Advanced Private Key Options...

Revocation Password

If you believe the security of your certificate has been compromised, it may be revoked. A revocation password is required to ensure that only you may revoke your certificate:

Revocation Password

Re-enter Revocation
Password

Comodo Newsletter

☒ Opt in?

Subscriber Agreement

Please read this Subscriber Agreement before applying for, accepting, or using a digital certificate. If you do not agree to the terms of this Subscriber Agreement, do not apply for, accept, or use the digital certificate.

Secure Email

▶ **Step 1:** Pr
for your ce

Step 2: Co
install your

COMODO

Tel Sales : +1 888 266 6333

Fax Sales : +1.201.963.9633

Your Comodo FREE Personal Email Certificate is now ready for collection!



Dear shui mitao,

Congratulations - your Comodo FREE Personal Secure Email Certificate is now ready for collection! You are almost able to send secure email!

Simply click on the button below to collect your certificate.

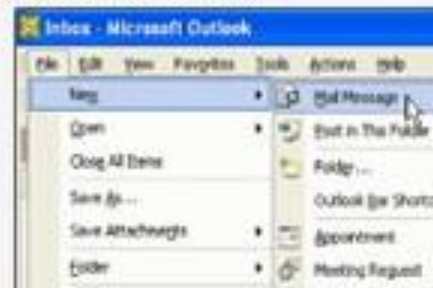
[Click & Install Comodo Email Certificate](#)

Note:- If the above button does not work, please navigate to

How to encrypt mail

Step 1

Create a new Mail



Collection of Secure Email Certificate

Attempting to collect and install your Free Certificate...

Successful



常规 安全 隐私 内容 连接 程序 高级

家长控制



内容审查程序



证书



清除 S

自动完成



源和网页快讯



证书

预期目的(N):

<所有>

个人

其他人

中级证书颁发机构

受信任的根证书颁发机构

受信任的发布者

未受信

颁发给

颁发者

截止日期

友好:

pingping_njust@163.com

COMODO Client Authentic...

2012/12/4

<无>

导入(I)...

导出(E)...

删除(R)

高级(A)

证书的预期目的

安全电子邮件, 1.3.6.1.4.1.6449.1.3.5.2

查看(V)

了解[证书](#)的详细信息

关闭(C)

常规

详细信息

证书路径



证书信息

这个证书的目的如下：

- 保护电子邮件消息
- 1.3.6.1.4.1.6449.1.2.1.1.1

* 有关详细信息，请参考证书颁发机构的说明。

颁发给： pingping_njust@163.com

颁发者： COMODO Client Authentication and Secure
Email CA

有效期从 2011/ 12/ 4 到 2012/ 12/ 4

🔑 您有一个与该证书对应的私钥。

[颁发者说明\(S\)](#)

了解[证书](#)的详细信息

[确定](#)









常规

详细信息

证书路径

显示(S):

<所有>

字段	值
 版本	V3
 序列号	00 aa 58 92 99 2...
 签名算法	sha1RSA
 签名哈希算法	sha1
 颁发者	COMODO Client Au...
 有效期从	2011年12月4日 8:0...
 到	2012年12月4日 7:5...
 使用者	pingping_njust@1...

编辑属性(E)...

复制到文件(C)...

了解[证书详细信息](#)的更多信息

确定

如何在 Outlook 中设置数字证书？



如何在outlook中设置数字证书？

高级安全设置

加密邮件

 邮件加密不足该强度时发出警告 (W):
168 位

☒ 发送加密邮件时始终加密给自己 (M)

数字签名的邮件

 ☒ 发送签名邮件时包含我的数字标识 (I)

☐ 发送前对邮件进行编码 (模糊签名) (S)

☒ 将发件人的证书添加到我的通讯簿中 (A)

撤销检查

 检查已撤销的数字标识:

☒ 只在联机时 (O)

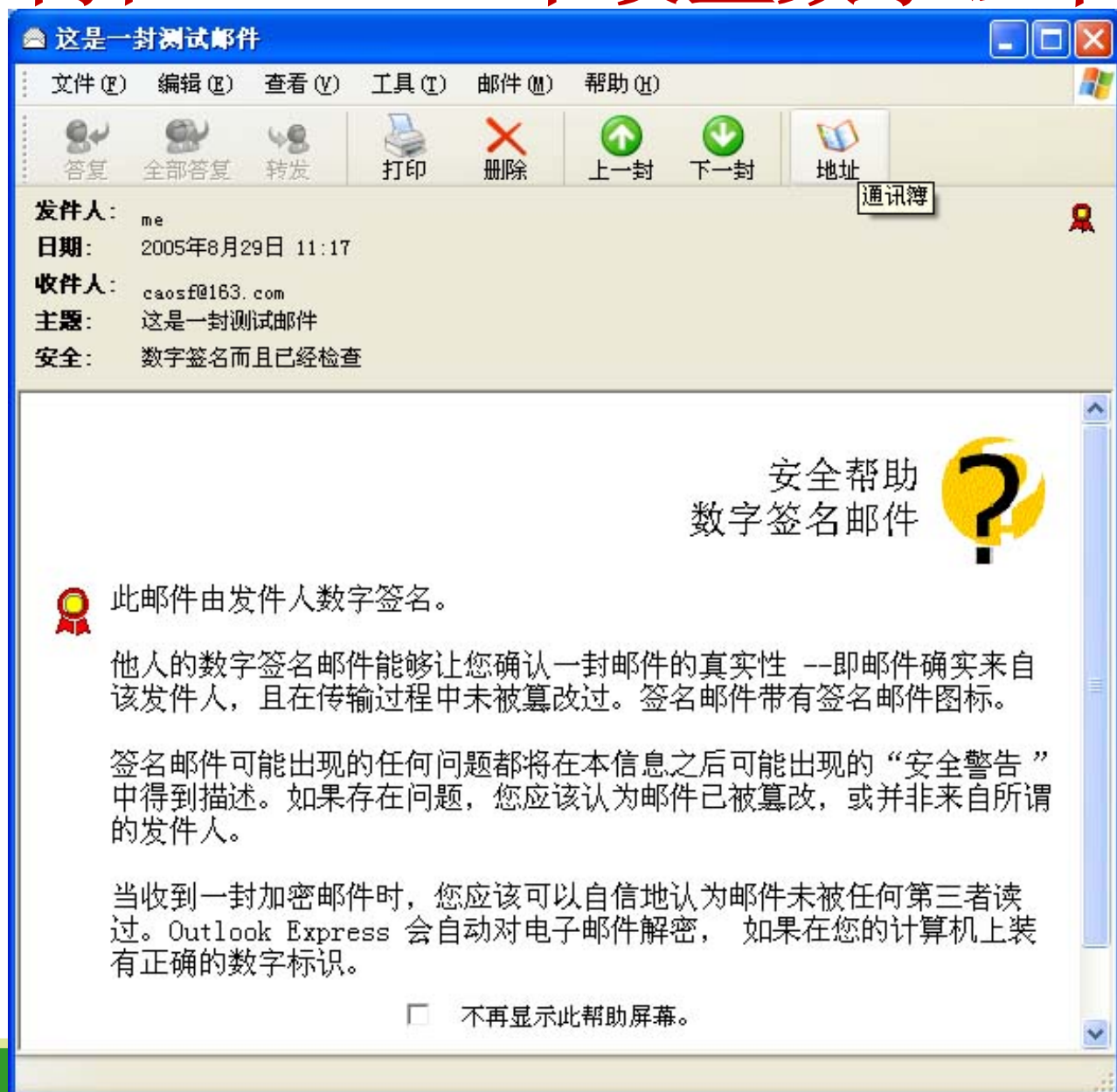
☐ 从不 (N)

确定 取消

如何在outlook中设置数字证书？



如何在outlook中设置数字证书？



如何导出数字证书？



如何导出数字证书？



如何导出数字证书？

证书导出向导

导出私钥

您可以选择将私钥和证书一起导出。

私钥受密码保护。如果要将私钥跟证书一起导出，您必须在后面一页上键入密码。

您想将私钥跟证书一起导出吗？

☒ 是，导出私钥(Y)

☐ 不，不要导出私钥(O)

[了解导出私钥的更多信息](#)

< 上一步(B)

下一步(N) >

取消

如何导出数字证书？



如何导出数字证书？

证书导出向导

密码

要保证安全，您必须用密码保护私钥。

输入并确认密码。

密码(P):

●●●●●●●●

输入并确认密码(必需)(C):

●●●●●●●●

< 上一步(B) 下一步(N) > 取消

如何导出数字证书？

证书导出向导

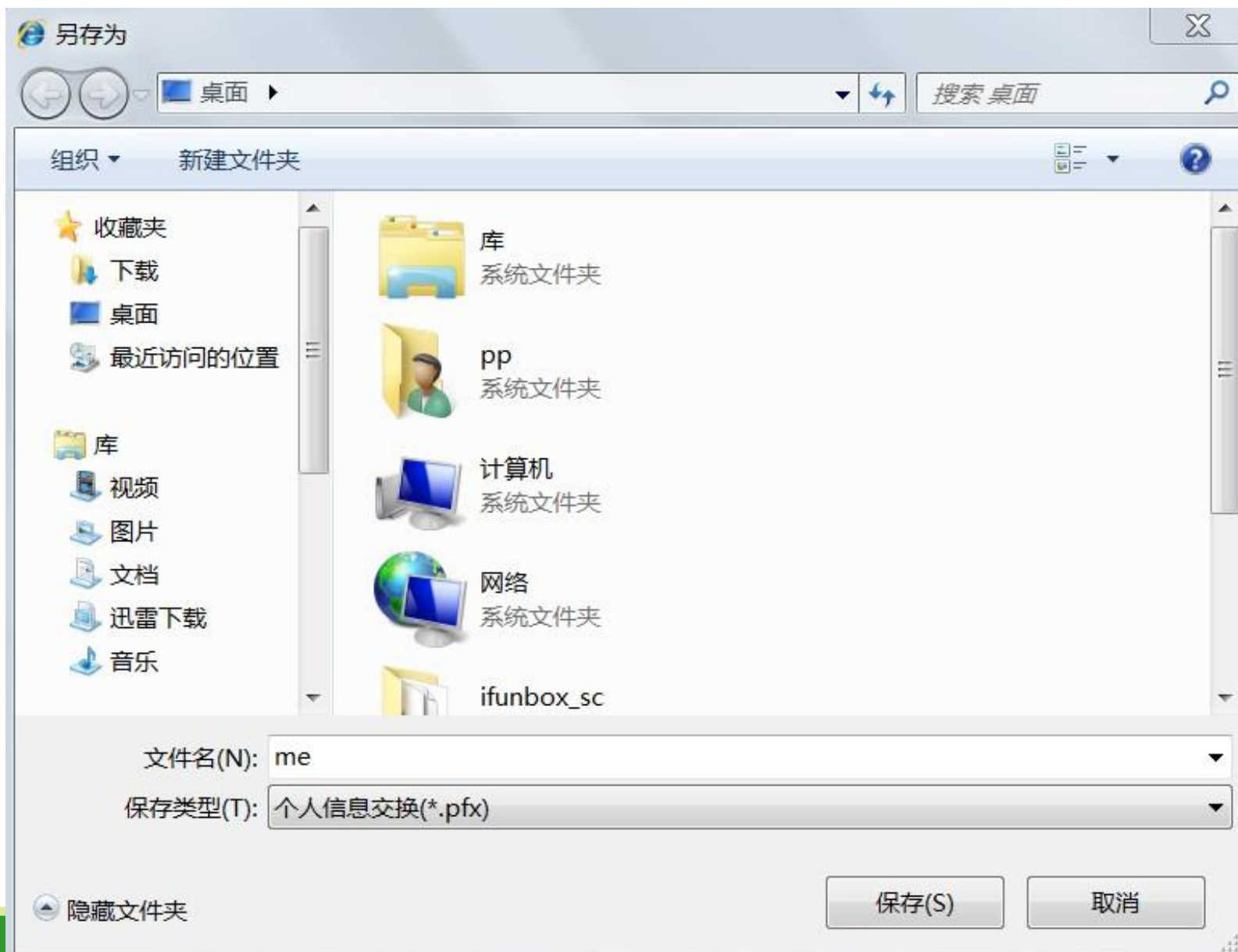
要导出的文件
指定要导出的文件名。

文件名(F):

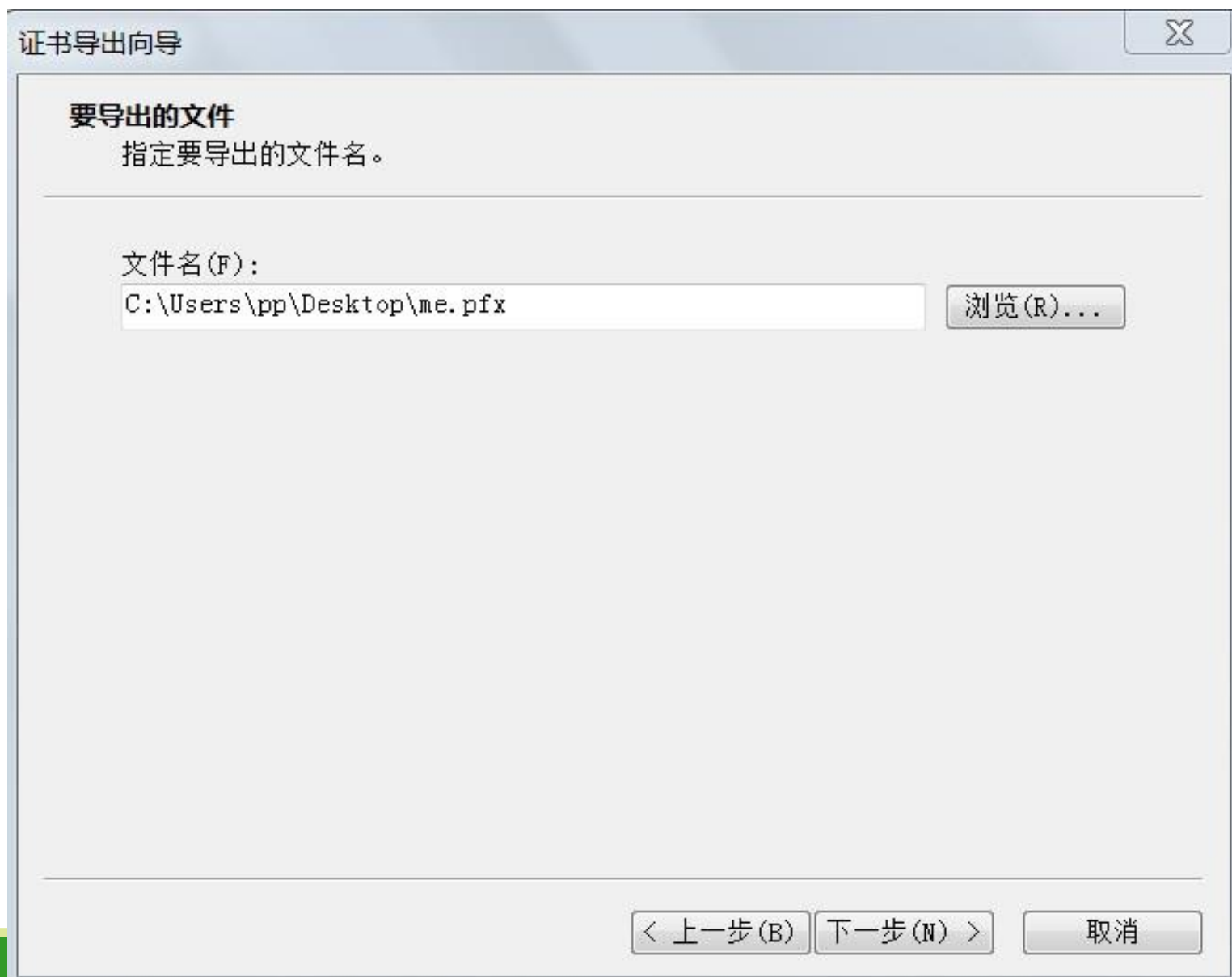
浏览(R)...

< 上一步(B) 下一步(N) > 取消

如何导出数字证书？



如何导出数字证书？

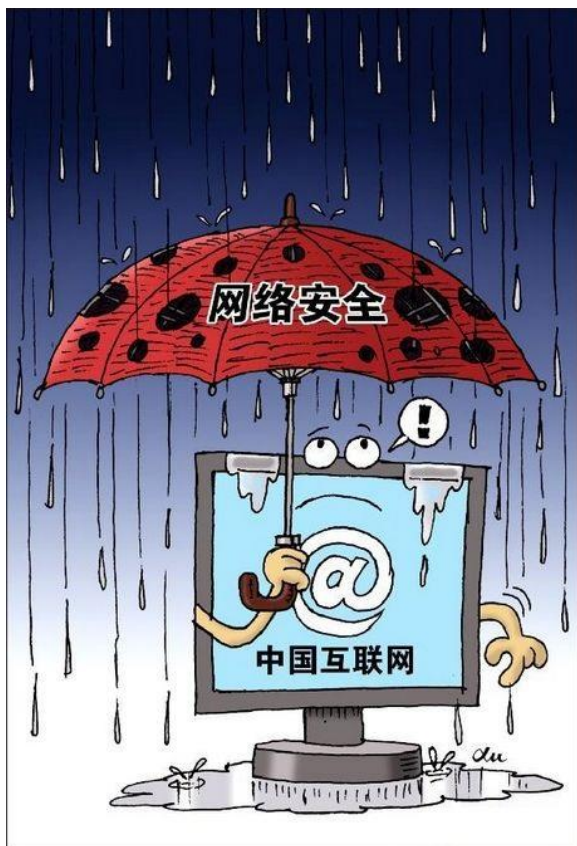


如何导出数字证书？





河海大學



Thank You!