

北京飞天诚信科技有限公司（以下简称“飞天”）尽最大努力使这篇文章中的内容完善且正确。飞天对于由这篇文档导致的任何形式的直接或间接损失不负有责任。这篇文章的内容会跟随产品的升级而有所变化。

修改记录：

日期	版本	修改
2001 年五月	2.00	第一版
2001 年八月	2.10	第二版
2001 年十一月	3.00	第三版
2003 年五月	3.60	第三版第二次修订
2003 年十二月	3.70	第三版第三次修订
2004 年十一月	4.0	第四版

北京飞天诚信科技有限公司

软件开发协议

北京飞天诚信科技有限公司（以下简称飞天）的所有产品，包括但不限于：开发工具包，磁盘，光盘，硬件设备和文档，以及未来的所有定单都受本协议的制约。如果您不愿接受这些条款，请在收到后的 7 天内将开发工具包寄回飞天，预付邮资和保险。我们会把货款退还给您，但要扣除运费和适当的手续费。

1. 许可使用

您可以将本软件合并、连接到您的计算机程序中，但其目的只是如开发指南中描述的那样保护该程序。您可以以存档为目的复制合理数量的拷贝。

2. 禁止使用

除在条款 1 中特别允许的之外，不得复制、反向工程、反汇编、反编译、修改、增加、改进软件、硬件和产品的其它部分。禁止对软件 and 产品的任何部分进行反向工程，或企图推导软件的源代码。禁止使用产品中的磁性或光学介质来传递、存储非本产品的原始程序或由飞天提供的产品升级的任何数据。禁止将软件放在服务器上传播。

3. 有限担保

飞天保证在自产品交给您之日起的 12 个月内，在正常的使用情况下，硬件和软件存储介质没有重大的工艺和材料上的缺陷。

4. 修理限度

当根据本协议提出索赔时，飞天唯一的责任就是根据飞天的选择，免费进行替换或维修。飞天对更换后的任何产品部件都享有所有权。

保修索赔单必须在担保期内写好，在发生故障 14 天内连同令人信服的证据交给飞天。当将产品返还给飞天或飞天的授权代理商时，须预付运费和保险。

除了在本协议中保证的担保之外，飞天不再提供特别的或隐含的担保，也不再对本协议中所描述的产品负责，包括它们的质量，性能和对某一特定目的的适应性。

5. 责任限度

不管因为什么原因，不管是因合同中的规定还是由于刑事的原因，包括疏忽的原因，而使您及任何一方受到了损失，由我方产品所造成的损失或该产品是起诉的原因或与起诉有间接关系，飞天对您及任何一方所承担的全部责任不超出您购买该产品所支付的货款。在任何情况下，飞天对于由于您不履行责任所导致的损失，或对于数据、利润、储蓄或其它的后续的和偶然的损失，即使飞天被建议有这种损失的可能性，或您根据第 3 方的索赔而提出的任何索赔均不负责任。

6. 协议终止

当您不能遵守本协议所规定的条款时，将终止您的许可和本协议。但条款 2, 3, 4, 5 将继续有效。

EC Attestation of Conformity



The equipment complies with the principal protection requirement of the EMC Directive (Directive 89/336/EEC relating to electromagnetic compatibility) based on a voluntary test.

This attestation applies only to the particular sample of the product and its technical documentation provided for testing and certification. The detailed test results and all standards used as well as the operation mode are listed in

Test report No. 70407310011

Test standards: EN 55022/1998 EN 55024/1998

After preparation of the necessary technical documentation as well as the conformity declaration the CE marking as shown below can be affixed on the equipment as stipulated in Article 10.1 of the Directive. Other relevant Directives have to be observed.

USB



This equipment is USB based.

FCC certificate of approval



This Device is conformance with Part 15 of the FCC Rules and Regulations for Information Technoogy Equipment.

目 录

第一章 ePass1000 简介	1
1.1 产品简介	1
1.2 为什么使用ePass1000	2
1.3 ePass1000 开发者	2
1.4 ePass1000 体系结构	7
第二章 安装ePass1000 软件	12
2.1 ePass1000 支持的平台	12
2.2 安装ePass1000 SDK	12
2.3 安装ePass1000 驱动程序和运行库	17
2.4 卸载ePass1000SDK和运行库	18
第三章 使用ePass1000	22
3.1 使用ePass1000 字符界面编辑器	22
3.2 打开ePass1000	24
3.3 打开/关闭指示灯	25
3.4 格式化ePass1000	25
3.5 获取和修改权限设置	26
3.6 管理ePass1000 文件系统	27
3.7 管理员密码与用户密码	29
3.8 关闭ePass1000	29
第四章 ePass1000 管理器使用说明	30
4.1 配置ePass1000	30
4.2 初始化ePass1000	31
4.3 更改用户PIN码	32
4.4 更改令牌名	33
4.5 用户PIN码解锁	34
4.6 改变管理员PIN码	35
4.7 证书管理	36
第五章 ePass1000 的PKI应用	39
5.1 ePass1000 PKI体系	40

- 5.2 ePass1000 PKCS#11 模块 41
- 5.3 ePass1000 的MS CAPI CSP模块..... 46
- 5.4 同时连接多个ePass1000 48
- 5.5 ePass1000 PKI应用指南..... 49
- 5.6 其它应用 101
- 第六章 发布ePass1000 应用程序102**
- 附录 一 常见问题.....103**
- 附录 二 ePass1000 技术及规格表105**

第一章 ePass1000 简介

对于电子商务来说安全是非常重要的。而 ePass1000 则是针对此类问题而开发的产品，对从事电子商务的人来说，提供了极大的便利及可靠性。

本文将向您介绍怎样将 ePass1000 的安全特性与您现有的应用程序，或者您正在开发的一个产品相结合。

本章包括如下主题

- ✓ 产品简介
- ✓ 为什么使用 ePass1000
- ✓ ePass1000 开发者
- ✓ ePass1000 体系结构

1.1 产品简介

ePass1000 是一种低成本、便携的硬件计算机设备，它可以通过 USB 接口与计算机连接。运行 Windows98SE（第二版）以上操作系统的计算机均可使用本产品（ePass1000 也支持 Mac OS 及 Linux，请参见附录 2）。ePass1000 不需要附加电源及类似于 IC 卡读卡器设备，而且其只有拇指般大小，可穿在钥匙链上，极大地方便了使用者随身携带。

对于身份认证及访问权限控制，ePass1000 是一个完美的解决方案。基于 ePass1000 的应用程序，将从内置于 ePass1000 硬件中的 HMAC-MD5 算法中得到收益。这是一种强度很高的冲击响应算法。冲击响应模式与传统用户名加密码模式相比更加安全，因为冲击响应模式中的共享密钥信息绝对不会在认证过程中暴露。

对于存取重要信息的应用来说使用 ePass1000 也是非常完美的方案。数字证书、私钥、密码、信用卡号、或其它安全认证信息如果都存放于 ePass1000 中，并带在您的身边，将更加方便、更加安全。

1.2 为什么使用 ePass1000

使用 ePass1000 的好处在于，它可以为您的组织及应用程序中心提供安全的网络通讯。

单纯的密码并不安全。用户可能会将密码告诉别人，或将它记在纸上。这样一来，仅通过密码认证并不能完全保证使用此账号的人一定就是其本人。另外，通过网络传送的密码会被许多嗅探软件截取到，而这类密码截取器的自由软件往往可以从 Internet 上免费得到。ePass1000 采用了双因子验证，其效果非常惊人。双因子意味着，一个合法的 ePass1000 使用者除了必须掌握 ePass1000 的 PIN 码，还必须持有其自己的 ePass1000 硬件才可能通过身份认证。

ePass1000 可以很容易地与支持 MS-CAPI、PKCS#11 的 PKI 应用相结合，如 Internet Explorer, Outlook, Outlook Express 以及 Netscape Communicator。

信用卡号、银行帐号、证书等安全信息很容易被计算机病毒破坏或被黑客们窃取，因而一个折衷的解决方案是不要将它们存放在计算机中。ePass1000 硬件内置的多级文件访问权限控制保证了存储于硬件中的信息远比在计算机中安全得多。

ePass1000 集成了智能卡的许多优点，同时又没有传统智能卡应用时所需要的读卡器，不但节约了硬件成本，而且也方便了用户的使用。

ePass1000 是一种低成本而又便携的设备，对于经常携带着安全信息往返于家及办公室的人来是再方便不过了，当然这也适用于经常外出办公的人。

1.3 ePass1000 开发者

有两类 ePass1000 开发者：

基于公开密钥体系（PKI）的开发者，这类开发人员将在相应的 PKI 环境中开发他们的应用程序。

系统编程者，这类开发人员更需要底层 ePass1000 API 的支持，以便通过他们的程序完全控制存取、认证、管理存储于 ePass1000 内部的敏感信息

注意：ePass1000 目前提供 Win32、Linux 及 Mac OS 平台下的 API。但 PKI 体系仅有 Win32 平台的实现版本。

对于 PKI 开发者来说他们可以利用公开密钥体系来控制 Web Server、Intranet、VPN (Virtual Private Networks)、加密电子邮件。ePass1000 并不只是低成本的设备，它也集成了十分强大的加密算法。除了内置的 MD5 算法外，ePass1000 还实现了 RSA、DSA、DH、DES、3DES、RC2、RC4 等常用的算法。

ePass1000 目前支持两种工业标准的 PKI 体系：

- ✓ PKCS#11 (Public Key Cryptography Standards from RSA Security Inc)
- ✓ MS CAPI (Microsoft's Cryptographic Applications Programming Interface)

构建于以上两个标准的应用程序将不用作任何修改就可与 ePass1000 无缝结合。Internet Explorer, Outlook, Outlook express, Netscape Navigator 和 Netscape Messenger 等程序就是典型的符合 PKI 标准的程序。

ePass1000 有一个分层的文件系统，这与 PC 上的文件系统相类似，而 ePass1000 的文件系统针对访问的权限及安全方面作了更多的考虑。

每个 ePass1000 硬件都有一个世界唯一的序列号。这个序列号，可以用于 ePass1000 应用中的唯一标识。

ePass1000 使用 MD5 散列算法来保护密码及其它认证信息。ePass1000 内置散列算法，这意味着用户密码及其它的认证信息从不直接从 ePass1000 中读出。ePass1000 将通过算法在硬件的内部用密码或认证信息与一个由外部输入的随机字符串计算的结果来验证一个 ePass1000 用户的有效性。这个过程将在下面的介绍中详细说明。

图 1-1 为一个计算机网络及安装在客户机上的 ePass1000 的简单示意图，此网络可以被假想为一个小型的局域网或 Intranet，也可被假想为现实中的 Internet。

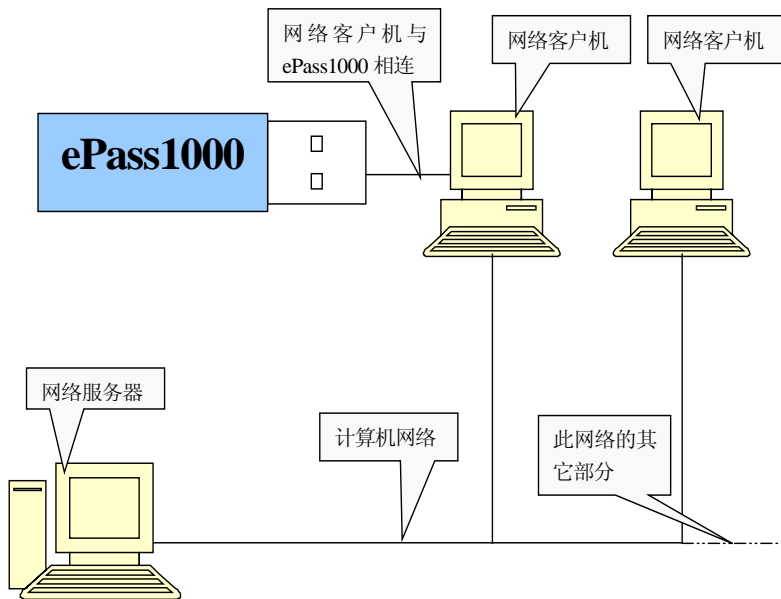


图 1-1

当利用密钥进行身份验证时，客户机首先向服务器发出登录请求。服务器则通过用户名便可从数据库中取出相应用户的密钥，参见图 1-2：

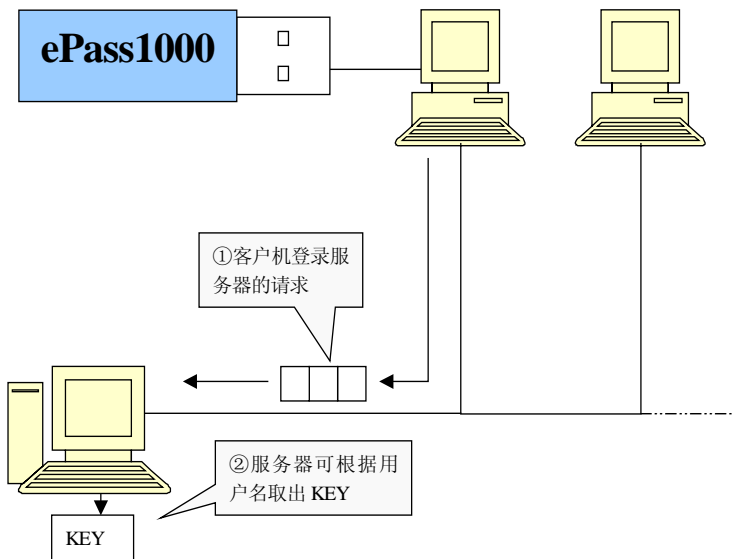


图 1-2

当服务器收到客户的登录请求后,便向客户机发送一个随机字符串 X ,该随机串最终送入客户机的 ePass1000 中用于计算。与此同时,服务器则根据用户名取出对应的密钥并利用发送给客户机的随机串 X ,在服务器上用加密引擎进行运算,得到运算结果 R_h ,如图 1-3 示:

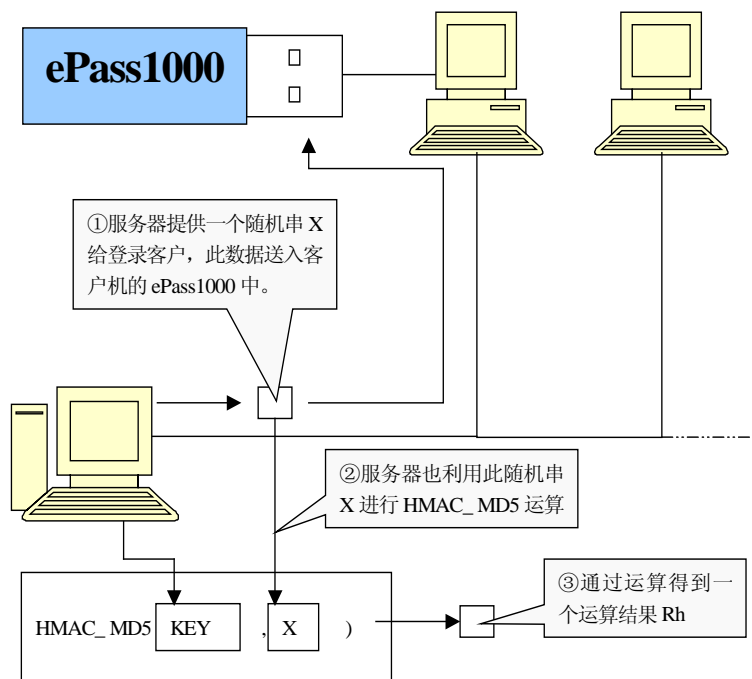


图 1-3

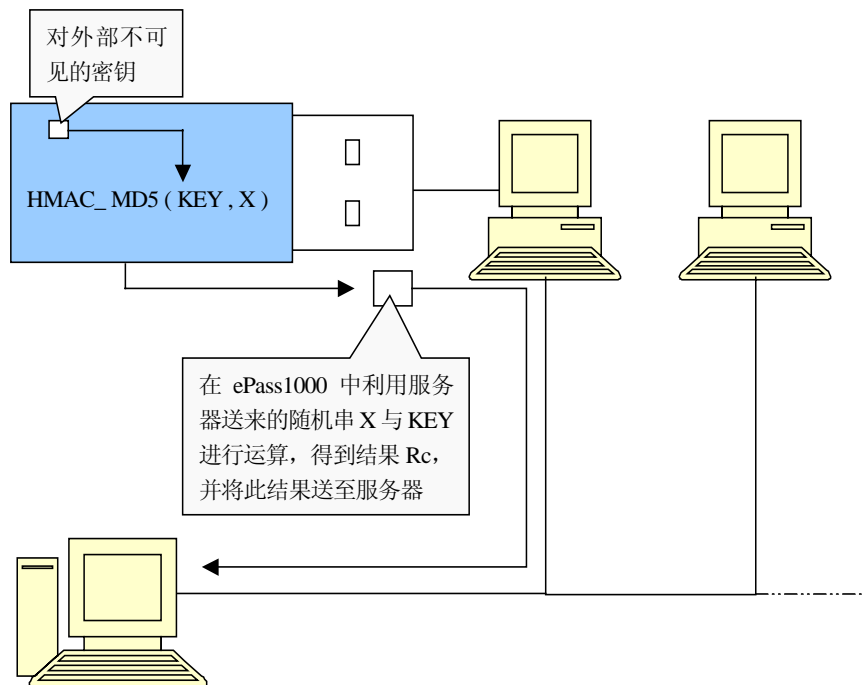


图 1-4

客户机将此随机串 X 传入 ePass1000 (参见图 1-4), ePass1000 则利用此串与内置在其中的密钥文件通过硬件加密引擎进行运算, 也得到一个运算结果, 将此运算结果可直接在网络中发送给服务器。

服务器比较两运算结果 $R_h(\text{服务器})$ 与 $R_c(\text{客户机})$ 是否相同, 便可确定一个网络用户的合法性, 如图 1-5 示。由于密钥存在于 ePass1000 中, 而整个运算过程也是在其中来完成的, 密钥鉴别是通过加密算法来实现的, 随机串作为运算的一个输入因子使其运算结果也随输入的变化而变化, 如果黑客简单截获到认证过程的数据仍无法在网络中冒充 ePass1000 客户端, 所以整个认证体系对现有的网上身份认证作了一个十分有益的补充。

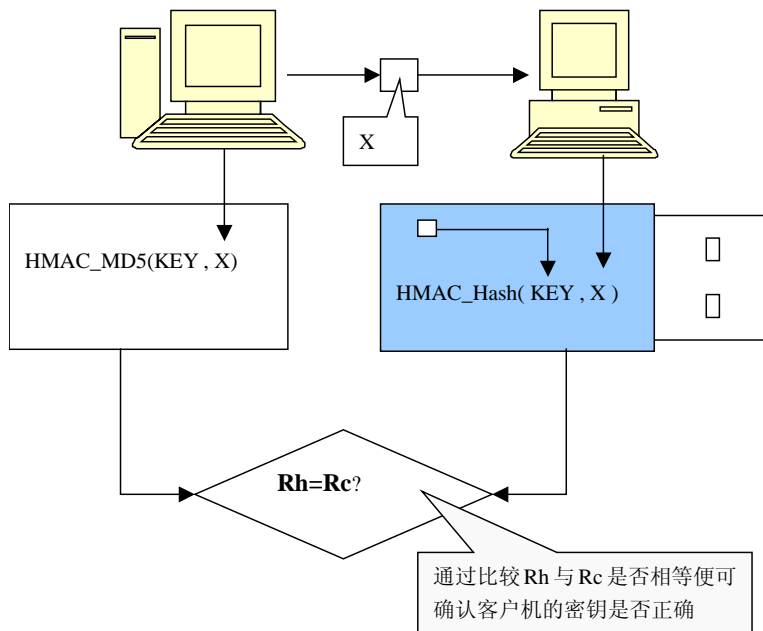


图 1-5

1.4 ePass1000 体系结构

1.4.1 安全状态

ePass1000 在硬件层提供了三种安全状态，超级用户、普通用户、匿名用户。

超级用户（Security Officer）状态

超级用户是拥有最高权限的用户状态。切换到超级用户需要进行超级用户身份识别码（SO-PIN）的验证。在超级用户状态可以修改 SO-PIN 和普通用户的身份识别码，而且在这种状态下允许对硬件的许多重要的参数进行设置，以及初始化 ePass1000。一旦忘记了 SO-PIN，就无法再以此身份操作 ePass1000 了。这种情况下只有将该 ePass1000 送回我公司，对其重新烧制，但原有的数据将全部丢失。

普通用户状态

要切换到普通用户状态，需要进行用户识别码（PIN）的验证。在普

通用户状态下，用户可以修改自己的 PIN 码。存储于 ePass1000 中的私有信息也是在此状态下进行访问的。同时在硬件层实现了一个登录密码计数机制，每当提供的密码不正确时，计数便会减少，而登录成功时计数便会重置为最大值。当此计数减至零时，ePass1000 便会处于锁定的状态。此时只有超级用户才能将此记数值重置，解除锁定的状态。

匿名状态

匿名状态是 ePass1000 加电后的缺省状态。匿名状态允许有限的对公开信息的读取操作。

1.4.2 设备属性

序列号

每个 ePass1000 硬件都有一个全球唯一的硬件序列号。这个序列号是出厂时烧入的，可以用于应用程序的标识依据。

LED

每个 ePass1000 都有一个 LED 指示灯，这个灯可以通过应用程序进行控制，也可以根据刚插在计算机时的状态来得知 ePass1000 的驱动安装是否正常。

存取控制

ePass1000 支持全局的存取控制。全局存取控制将对所有目录及文件生效。全局属性包括创建及删除控制。创建及删除控制可有如下四种属性值：

属性	控制
ALWAYS	无访问的限制
NEVER	不允许访问
PIN	以普通用户或超级用户登录时可访问
SO-PIN	只有超级用户可以访问

注意：超级用户可访问受普通用户 PIN 码保护的信息。

1.4.3 加密服务

随机数产生器

ePass1000 可以由硬件生成随机数。随机数可用作其它算法在创建认证信息码时的种子。

MD5 算法

该算法对输入的不定长度的数据，计算出一个与输入数据相关的 128 位的数据摘要，而这个数据摘要则类似于“指纹”，可以作为一个唯一标识，它是一个国际上认同的标准不可逆加密算法。

HMAC-MD5

MD5 比起简单的校验和算法要可靠得多，不过 MD5 并不提供数据完整性的验证，因此任何人都可以改变输入数据产生和相应的输出数据摘要。很明显，散列运算的值需要被保护。这正是 HMAC (Hash Message Authentication Code) 作用。HMAC 可以与 MD5 散列算法和一个安全密钥结合来验证信息或数据的有效性。HMAC 可以与 MD5 算法(ePass1000 支持这个工业标准的算法)，为最终的用户及应用提供了一种安全的途径来保证认证过程中密钥不被暴露。

1.4.4 文件系统

ePass1000 有一个内置的文件系统，可以通过 API 库来进行完整的控制。文件系统使得存取、保护 ePass1000 中的数据更加便捷。

ePass1000 文件系统有如下属性：

- ✓ 2 级目录结构。
- ✓ 文件的大小是创建时设定的，当文件被创建后其大小将不能被改变。不过可以通过删除已有文件，再创建一个同名新文件的方式达到改变文件大小的效果。
- ✓ 自由空间是相对于整个 ePass1000 而言的。
- ✓ 文件的标识是通过数字 ID，而不是字符串。
- ✓ ePass1000 文件系统支持 32 位及 16 位的目录和文件 ID。
- ✓ 目录 ID 的作用域仅限于当前目录。
- ✓ 文件 ID 的作用域仅限于当前目录。
- ✓ ePass1000 支持最大 32 个字节的字符串方式命名的目录，名字对于整个文件系统来说是全局的，并且区分大小写，不可重复。
- ✓ ePass1000 也支持目录的 128 位（16 字节）的 GUID 标识，GUID 标识对于整个文件系统来说也是全局的，也不允许重复。

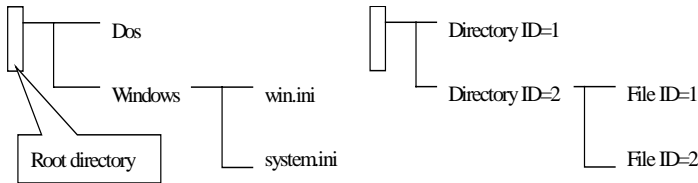


图 1-6

注意：

- ✓ MF 就是根目录使用的 ID，为 0。
- ✓ MF 包含文件及目录。
- ✓ 目录 ID 取值范围为 1...0xFFFFFFFF(0 保留给了根目录)
- ✓ 文件 ID 取值范围为 0...0xFFFFFFFF。

应用程序应使用 16 位的文件 ID (0...0xEFFF) 和 16 位的目录 ID(1...0xEFFF)来保证与新的设备相兼容。应用程序应该尽量不使用 32 位的 ID。

文件类型

ePass1000 文件系统使用两种类型的文件：

类型	描述
数据（DATA）	任何变长的二进制的的数据
密钥（KEY）	用于加密的数据

文件存取控制

ePass1000 的文件有三种存取控制类型，每个文件有它自己的存取控制设置

存取控制	文件类型	
	数据（Data）	密钥（KEY）
读	由属性决定	禁止
写	由属性决定	由属性决定
加密	无意义	由属性决定

注意：读写操作是 ePass1000 的数据传输的功能。加密对于数据（DATA）类型的文件来说是无意义的。对密钥（KEY）文件的加密操作完全在 ePass1000 的内部完成。



文件访问权限

属性	描述
ALWAYS	总是允许访问
NEVER	从不允许访问
PIN	在普通用户及超级用户状态可访问
SO-PIN	仅在超级用户状态可访问

注意：多个应用程序使用同一个 ePass1000 硬件时，应根据情况相应调整其所使用的目录或文件 ID 以免冲突。

1.4.5 支持同时连接多个 ePass1000

同一台计算机中可以同时连接多个 ePass1000 设备，它们可以同时工作，满足了更多的应用需求。

第二章 安装 ePass1000 软件

在使用之前必须在您的计算机上正确安装 ePass1000 的软件。本章提供在 Windows 环境下安装 ePass1000 软件的详细说明。

本章包括如下主题

- ✓ ePass1000 支持的平台
- ✓ 安装 ePass1000 SDK
- ✓ 安装 ePass1000 驱动程序和运行环境
- ✓ 卸载 ePass1000 SDK 和运行环境

2.1 ePass1000 支持的平台

ePass1000 目前支持下列平台：

- ✓ Windows 98 SE
- ✓ Windows ME
- ✓ Windows 2000
- ✓ Windows XP
- ✓ Windows Server2003
- ✓ Linux
- ✓ Mac OS 8/9/10.X

注意：安装 ePass1000 软件之前请以管理员身份登录系统。
硬件缺省的 SO-PIN 是 “rockey”。

2.2 安装 ePass1000 SDK

ePass1000 SDK 会在您的计算机上安装下列组件：

- ✓ ePass1000 字符界面编辑器
- ✓ ePass1000 SDK 文档
- ✓ ePass1000 头文件和库
- ✓ ePass1000 运行环境分发包

✓ ePass1000 例程

注意：安装新版本之前，请卸载旧版本的 ePass1000 SDK。

将安装光盘放入光盘驱动器，然后执行“D:\Setup.exe”（这里假定光盘驱动器盘符为 D），就开始了 ePass1000 SDK 的安装过程。

这时会显示如图 2-1 所示的窗口，在此窗口中请您选择在安装过程中所采用的语言，如图 2-1 所示：



图 2-1

这里我们选用简体中文，即“简体中文”，单击“OK”继续安装，安装程序进入欢迎界面，如图 2-2 所示：

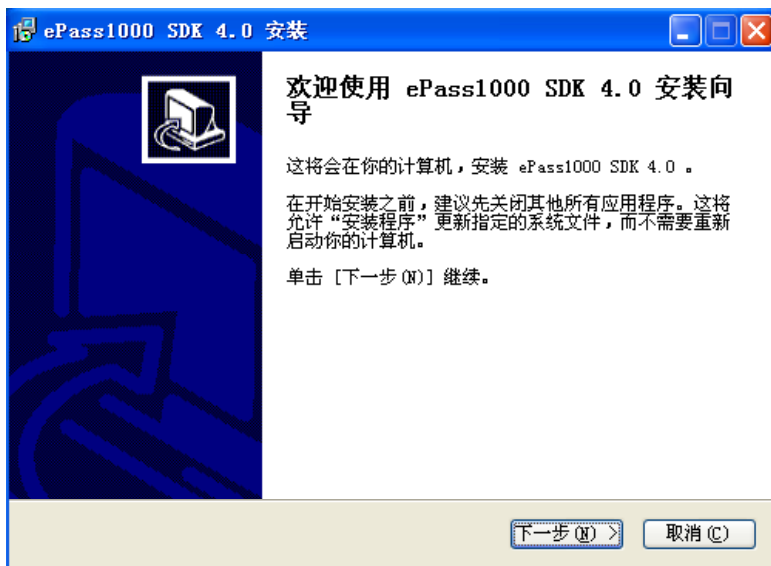


图 2-2

点击“下一步”按钮继续，会显示许可证协议窗口如图 2-3 所示：

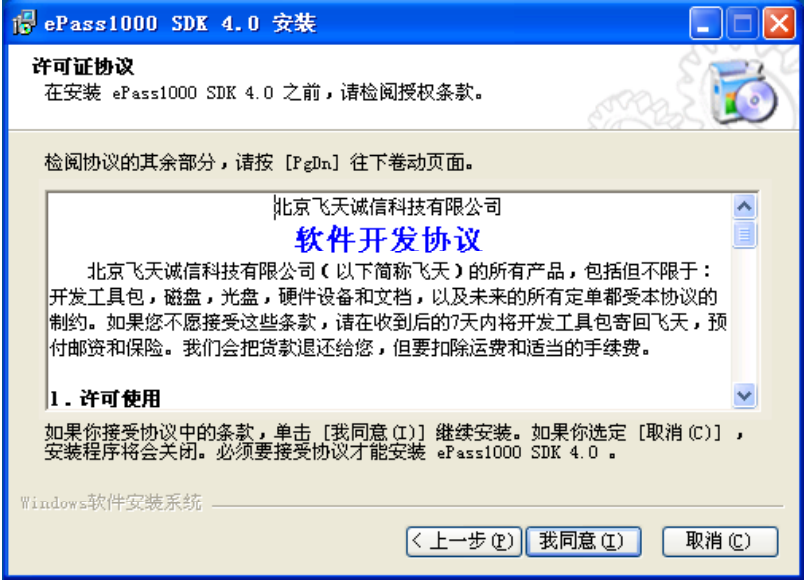


图 2-3

请详细阅读许可证协议。如果您同意这些条款，请选择“我同意”按钮接受许可协议，将进入安装程序的下一步，如图 2-4 所示：

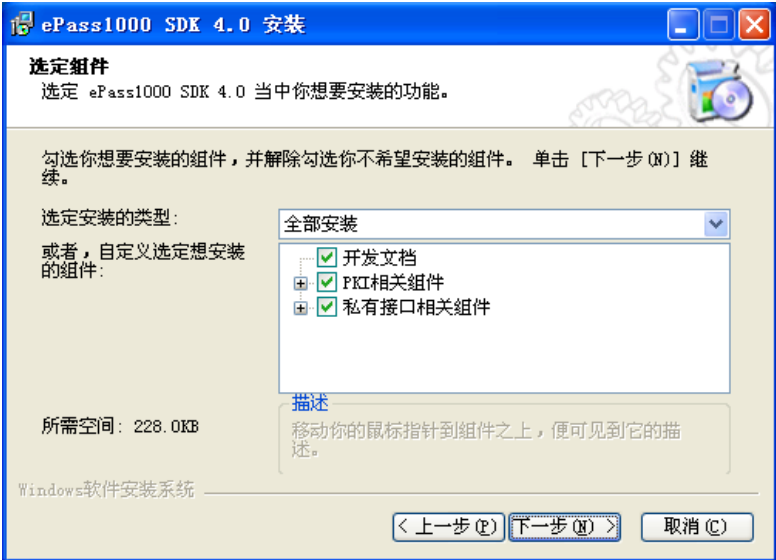


图 2-4

安装程序列出了安装的组件，用户可以进行选择，也可以选择全部安装。选择好以后，点击“下一步”，将进入安装程序的下一步，如图 2-5 所示：

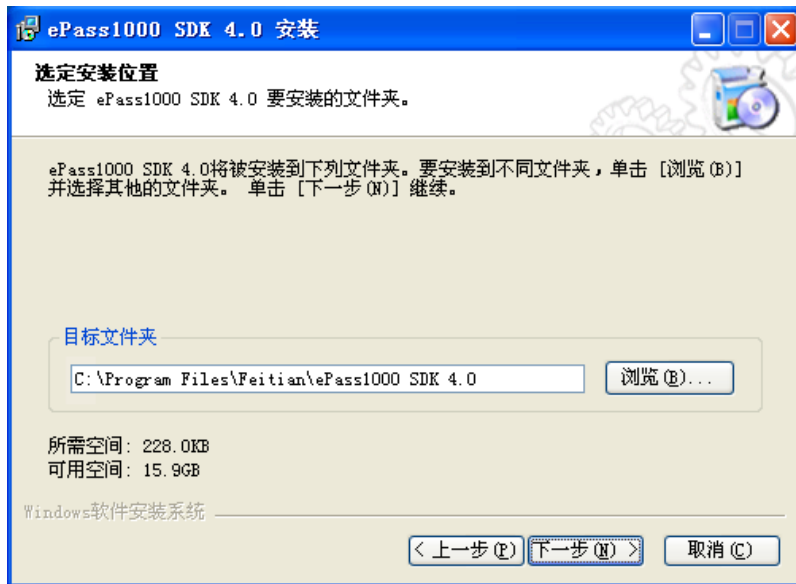


图 2-5

选定要安装的目标文件夹，在这里，您可以使用缺省的安装路径，也可以通过“浏览”按钮来选择自定义的安装路径。在完成路径的设置之后，单击“下一步”。

进入“选择程序文件夹”界面，安装程序会将程序图标安装到指定的“程序文件夹”中，如图 2-6 所示：

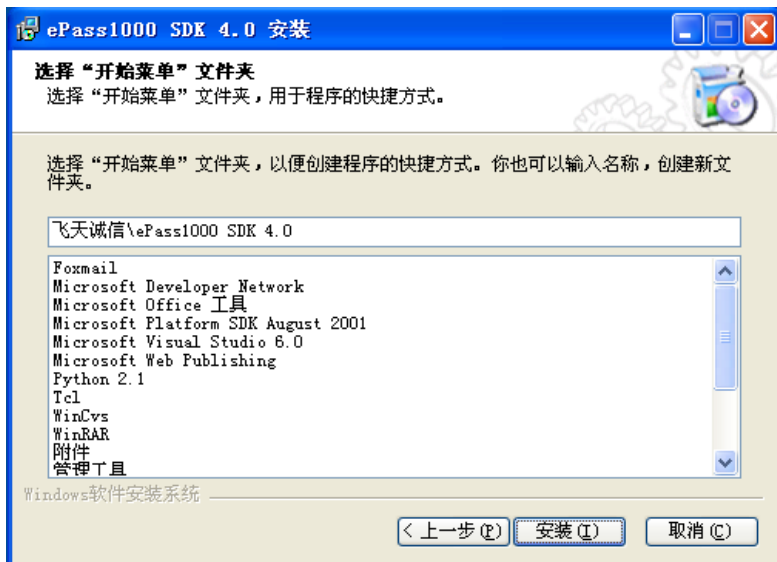


图 2-6

单击“安装”按钮，安装程序自动把 ePass1000 SDK 安装到您的系统中。安装完成如图 2-7 所示：



图 2-7

单击“完成”来完成 ePass1000 SDK 的安装。安装完 ePass1000 SDK 后，用户可以从 ePass1000 SDK4.0 的程序文件夹中安装 ePass1000 驱动程序和运行库，具体的安装过程如 2.3 节。

2.3 安装 ePass1000 驱动程序和运行库

完成 SDK 的安装以后，如果要使用 ePass1000 还必须安装 ePass1000 驱动程序和运行库。用户可以从开始菜单开始，“开始”→“程序”→“飞天诚信”→“ePass1000 SDK4.0”→“浏览安装文件夹”，用户可以看到已经安装好的 SDK 组件。如果是 PKI 用户，则双击“PKI”文件夹，如果是私有用户，则双击“Private”文件夹。这里，我们以 PKI 用户为例。

进入 PKI 文件夹以后，再进入 Redist 文件夹，这时用户可以看到文件夹 CN 和 EN，CN 中是简体中文版，EN 是英文版，这里，我们以简体中文版为例，英文版的安装过程类似。进入 CN 文件夹，双击文件 eps1k_full.exe 进行 ePass1000 驱动程序和运行库的安装。

出现欢迎界面，如下图 2-8：



图 2-8

点击“下一步”进行安装，安装程序会自动进行安装，安装完成如图 2-9 所示：

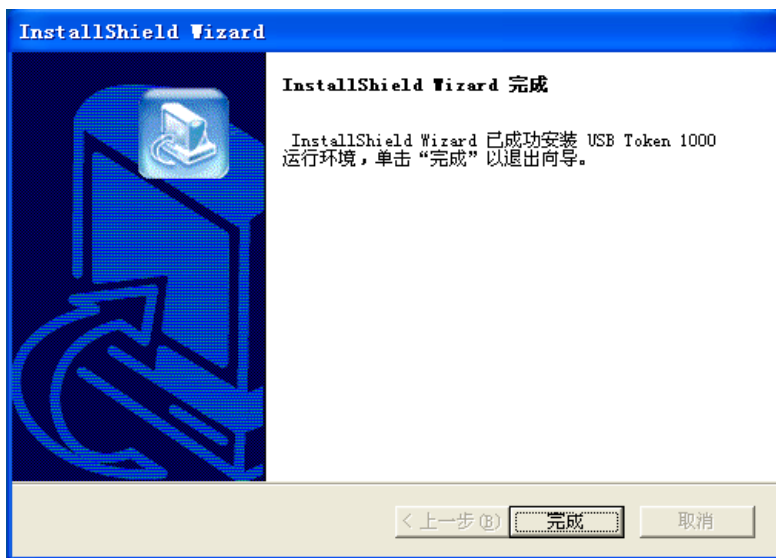


图 2-9

点击“完成”，ePass1000 驱动程序和运行库就完成安装。

如果安装程序检测到您的系统中已经安装了 Netscape Navigator，安装程序会自动向 Netscape Navigator 注册 PKCS #11 所需的组件。

2.4 卸载 ePass1000SDK 和运行库

卸载 ePass1000 SDK 或运行库与卸载其它的应用软件是一样的，您可以在操作系统的控制面板中“添加/删除程序”中进行。如果您只想把运行库卸载掉而保留 SDK，那么从控制面板中“添加/删除程序”中进行，例如，现在要卸载驱动程序和运行库，如图 2-10 所示：



图 2-10

点击“更改/删除”，此时会要求用户确认卸载，如图 2-11 所示：

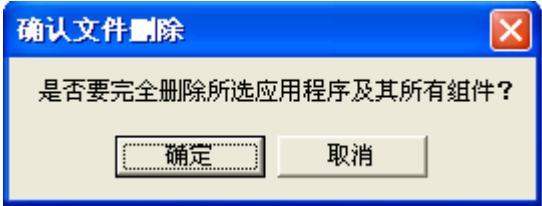


图 2-11

在确认删除之后，运行库将被从系统中完全卸载。同时，需要重新启动计算机，如图 2-12 所示：



图 2-12

卸载 ePass1000SDK 与卸载 ePass1000 的运行库是很类似的。但是也可以从“开始”→“程序”→“飞天诚信”→“ePass1000 SDK4.0”→“卸载 ePass1000 SDK4.0”进行反安装。如图 2-13 所示：



图 2-13

单击“下一步”继续进行卸载。显示卸载的组件和组件所在的文件夹，

如图 2-14 所示：

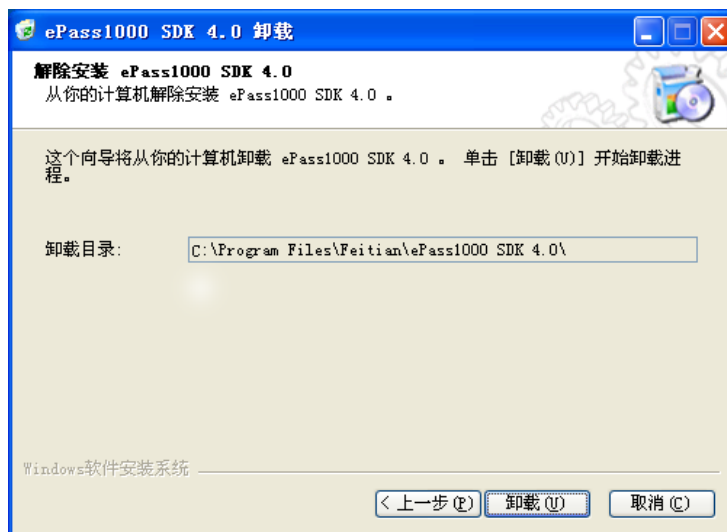


图 2-14

在单击“卸载”之后，ePass1000 SDK4.0 将被从系统中完全卸载。卸载完成以后，系统提示 ePass1000 SDK4.0 已经从计算机中解除安装，如图 2-15 所示：

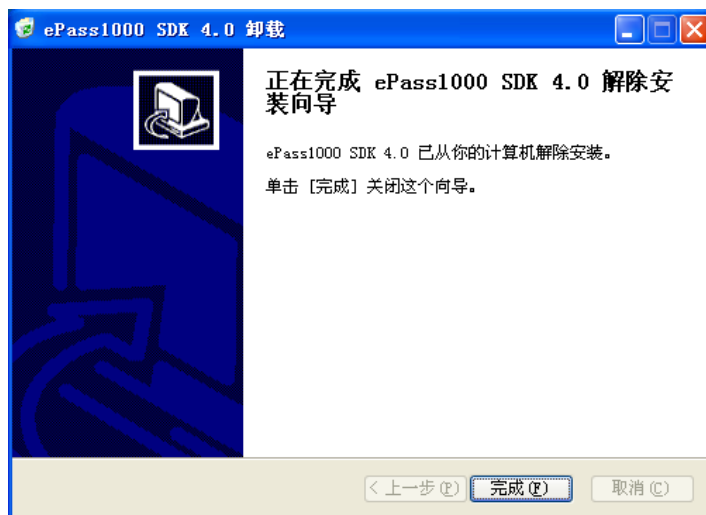


图 2-15

单击“完成”来完成 ePass1000 SDK 的卸载。

第三章 使用 ePass1000

这一章我们将简要介绍一些常用的 ePass1000 函数，并使用 ePass1000 字符界面编辑器演示这些功能。ePass1000 字符界面编辑器使用 ePass1000 的 C 语言编程接口编制而成，开发人员可以使用这个编辑器调用 ePass1000 所有的功能而无需编写代码。

关于 ePass1000 API 的详细信息，请查阅“开发人员手册”，该文档详细阐述了 ePass1000 API 的每一个函数调用。

注意：对于 PKI 应用开发人员，除非要了解 ePass1000 的一些底层功能细节，否则不需要阅读这一章。

本章介绍以下操作：

- ✓ 使用 ePass1000 字符界面编辑器
- ✓ 打开 ePass1000
- ✓ 打开/关闭指示灯
- ✓ 格式化 ePass1000
- ✓ 得到和修改权限设置
- ✓ 管理 ePass1000 文件系统
- ✓ 管理员密码与用户密码
- ✓ 使用加密函数
- ✓ 关闭 ePass1000

3.1 使用 ePass1000 字符界面编辑器

ePass1000 字符界面编辑器是用 ePass1000 的 C 语言编程接口编写而成。使用 C 语言接口可以调用 ePass1000 的所有功能。字符界面编辑器的每一个命令直接对应一个或几个 C 语言接口中的函数。开发人员可以通过使用字符界面编辑器来快速的熟悉 ePass1000 的功能。

字符界面编辑器集成了 ePass1000 编程接口中常用的功能，除非开发人员需要对 ePass1000 作更底层的控制，否则只需使用字符界面编辑器便可完成大部分的工作。

下表列出了字符界面编辑器中的命令对应函数：

ePass1000 操作	ePass1000 C 语言接口函数
打开 ePass1000	epas_OpenDevice: 打开一个连接到计算机的 ePass1000。你可以按照系统列举 USB 设备顺序或者指定硬件序列号等方法来打开特定的 ePass1000。
打开/关闭指示灯	epas_SetProperty: 指示灯可以用来显示 ePass1000 当前的状态。
格式化 ePass1000	epas_DeleteDir: 删除 ePass1000 目录和文件 epas_SetProperty: 设置或改变 ePass1000 的属性。.
得到和修改权限设置	epas_GetProperty: 获取 ePass1000 访问权限设置。 epas_SetProperty: 更改 ePass1000 访问权限设置。
管理 ePass1000 文件系统	epas_CreateDir: 创建目录。 epas_DeleteDir: 删除目录。 epas_ChangeDir: 改变当前目录。 epas_CreateFile: 创建文件。 epas_DeleteFile: 删除文件。 epas_OpenFile: 打开文件。 epas_Read: 从文件中读数据。 epas_Write: 向文件中写数据。 epas_CloseFile: 关闭文件。
管理员密码与用户密码	epas_ChangeCode: 更改管理员密码和用户密码。 epas_Verify: 校验管理员密码和用户密码。
使用加密函数	epas_GenRandom: 使用 ePass1000 的随机数生成器产生一个随机序列。 epas_HashToken: 执行 MD5 散列计算。 epas_MD5_HMAC: 执行 HMAC-MD5 计算。
关闭 ePass1000	epas_CloseDevice: 关闭 ePass1000。

要打开 ePass1000 字符界面编辑器，可以从系统的“开始—>程序—>飞天诚信—>ePass1000 SDK4.0—>使用私有接口”，然后选择控制台编辑

器。编辑器的主界面显示如图 3-1:

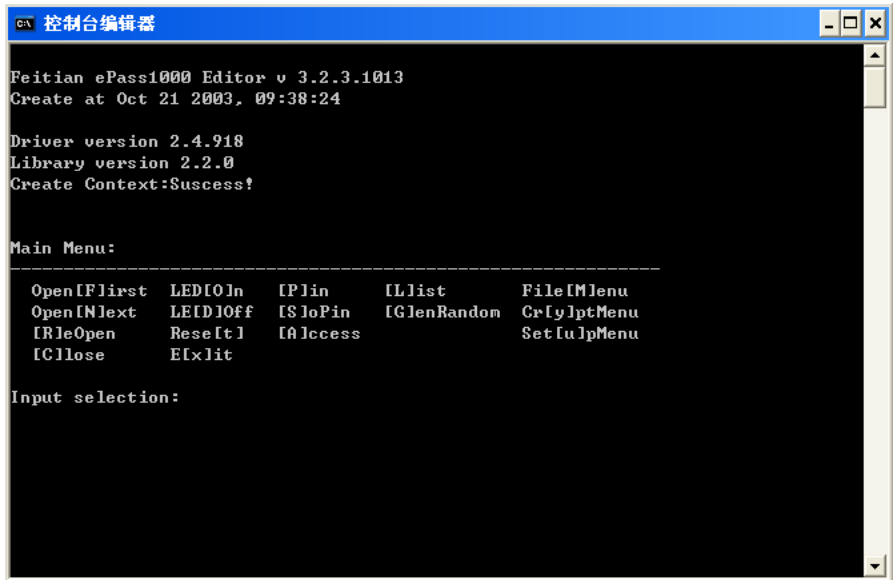


图 3-1

3.2 打开 ePass1000

在使用其他 ePass1000 函数之前，必须先打开 ePass1000。ePass1000 是一个 USB 接口设备，因此系统最多可同时接驳 127 支 ePass1000。ePass1000 的 C 语言接口支持多种方式查找和打开 ePass1000。关于 epas_OpenDevice()函数的细节信息请查阅“开发人员手册”。

打开第一个 ePass1000: 当 ePass1000 插入了计算机的 USB 端口后，按“F”，ePass1000 编辑器便会尝试打开第一个连接到系统的 ePass1000。如果没有 ePass1000 被找到，则“Device not found”错误信息将显示。如果打开操作成功，则编辑器将显示类似图 3-2 的界面：

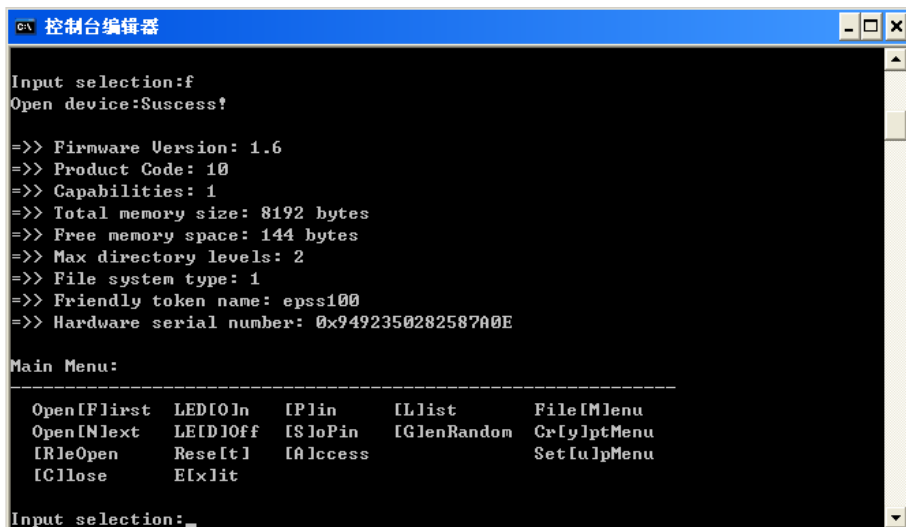


图 3-2

3.3 打开/关闭指示灯

ePass1000 的 LED 指示灯可用来显示 ePass1000 当前的状态。开发人员可使用指示灯来提示用户 ePass1000 正在进行大量数据传输。

打开指示灯：输入“O”。

关闭指示灯：输入“D”。

如果 ePass1000 的指示灯不能正常工作，则说明 ePass1000 可能没有正确连接，或者驱动程序没有正确安装。

3.4 格式化 ePass1000

格式化操作将清空 ePass1000 的存储区并置零。我们建议开发者在发行 ePass1000 前最好先进行初始化操作。格式化操作将删除 ePass1000 中所有的信息，这个操作是不可恢复的，因此在执行此操作前应慎重考虑。

要执行格式化操作必须输入管理员密码。也就是说只有管理员才能够执行格式化操作。

验证 SO-PIN：输入‘S’，然后输入相应的 SO-PIN 并回车。如果成功

则编辑器将显示 “success!” .

格式化 ePass1000: 在 “Setup Menu” 中输入 ‘U’，然后输入 ‘D’。

用户也可为 ePass1000 设置一个易于记忆的名称，类似磁盘分区的标签。

设置 token name: 在 “Setup Menu” 下，输入 ‘T’ 然后输入新的名字即可（最多 31 个字符）。

3.5 获取和修改权限设置

对于 ePass1000，应用权限设置信息是非常重要的。

获得当前的权限设置: 在编辑器的 “Main Menu” 下输入 ‘A’。将显示类似图 3-3 的界面：

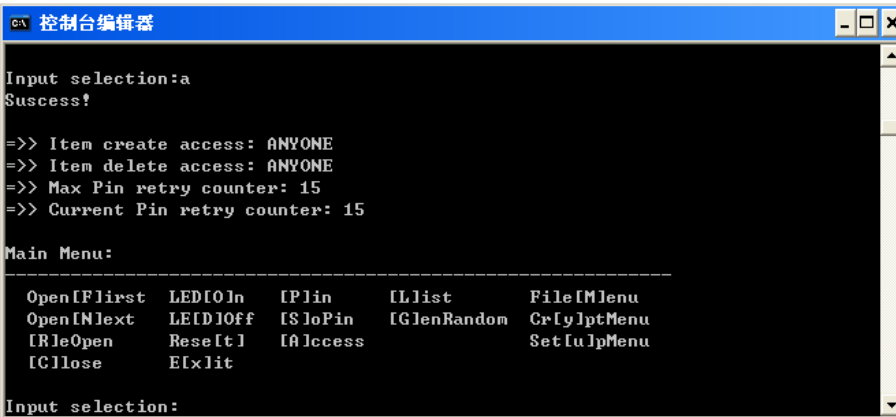


图 3-3

设置访问权限: 在编辑器的 “Setup Menu” 下，输入 ‘A’。然后就可设置权限信息了。如图 3-4 所示：

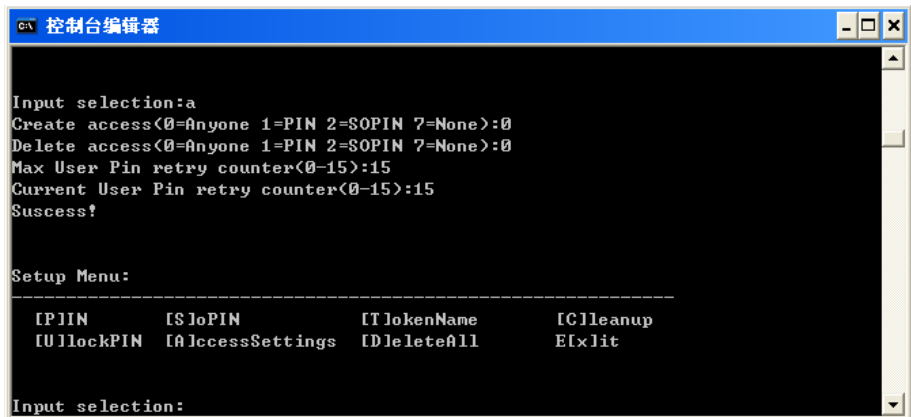


图 3-4

3.6 管理 ePass1000 文件系统

正如我们在前一章所介绍，ePass1000 的文件系统具有两级目录结构。可以创建，删除，读写文件并改变对应的权限设置。要操作目录和文件，先进入编辑器的“File Menu”。

在 ePass1000 的文件系统中，一个目录可以用长 ID (32 位)，短 ID (16 位)，ASCII 字符串和 GUID (128 位) 来标识。应用程序可以选择一种或多种方式来标识一个目录。

使用 ID 创建目录：在 ePass1000 编辑器的“File Menu”下输入 ‘D’，然后输入目录的 ID。

使用字符串或 GUID 创建目录：在编辑器的“File Menu”下输入 ‘A’。然后输入目录名或 GUID，或同时设置。

浏览目录和文件的设置信息：输入 ‘L’。参见下图 3-5：

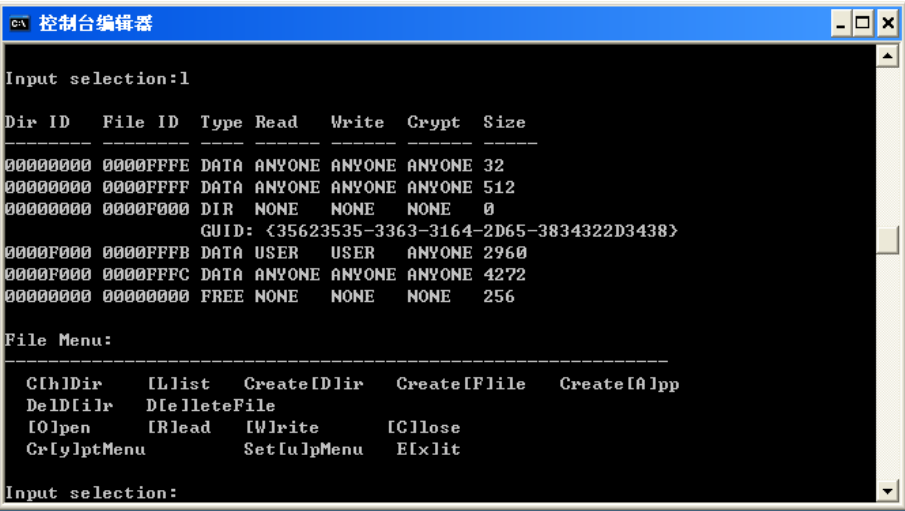


图 3-5

改变当前目录：在编辑器的“File Menu”下输入‘H’。然后输入目录的ID。

对于 ePass1000 的文件系统，同时只能有一个文件被打开。打开一个新的文件（无论打开是否成功）将导致当前已经被打开的文件自动关闭。对于二进制和加密类型文件有三种访问权限设置：读访问权限，写访问权限和加密访问权限。（参见 1.4 中文件访问权限表）

创建文件时，必须同时设置文件的大小。文件被创建后大小就不可改变。文件类型也必须被指定。文件一旦创建，这些信息就不可再更改。

创建文件：要创建一个文件，首先进入要建立文件的目录。然后在编辑器的“File Menu”下输入‘F’，然后输入文件ID，文件大小，文件类型和文件的访问权限设置。我们建议开发人员最好使用短ID。有一些ID是由飞天公司保留，开发人员应避免使用这些目录ID。关于飞天公司保留的ID列表，请查阅“开发人员手册”。

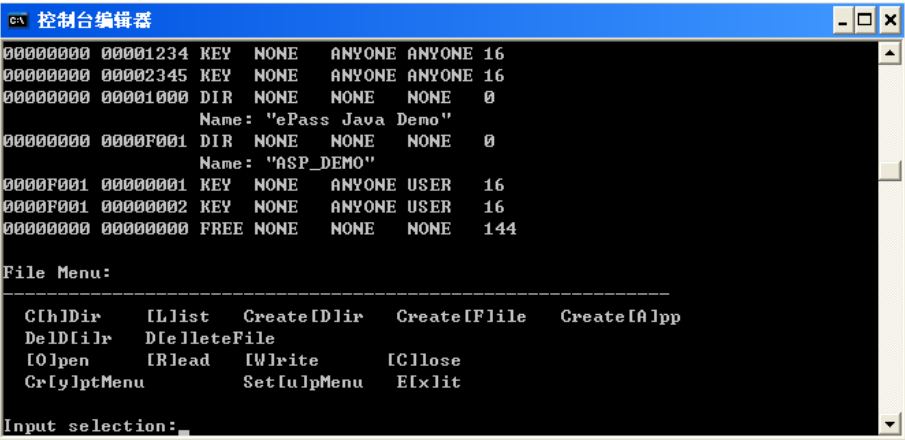


图 3-6

删除文件：在编辑器的“File Menu”下输入‘e’，然后输入文件的 ID。

3.7 管理员密码与用户密码

应用程序应该决定是否需要用户验证 SO-PIN 或 USER-PIN。如果应用程序并不关心某些文件的安全问题可以设置访问权限为不需要 PIN 码验证。

修改 SO-PIN：在编辑器的“Setup Menu”下，输入‘S’。然后输入当前的 SO-PIN 和新的 SO-PIN。ePass1000 出厂时缺省的 SO-PIN 是“rockey”。在开发者发布 ePass1000 前应当修改这个值。

修改 USER-PIN：在编辑器的“Setup Menu”中输入‘P’。然后输入当前的 USER-PIN 和新的 USER-PIN。

3.8 关闭 ePass1000

ePass1000 被设计成进程独占访问方式，也就是说同时只有一个应用程序可以打开 ePass1000。因此当一个应用程序打开 ePass1000 后，其他的应用程序就不能再访问 ePass1000，直到打开 ePass1000 的应用程序关闭 ePass1000。

关闭 ePass1000：在编辑器的“Main Menu”下，输入‘C’。

第四章 ePass1000 管理器使用说明

ePass1000 管理器将初始化 ePass1000、修改 PIN 及证书导入等常用功能均集成了进来，从而用户可以更方便有效地使用 ePass1000，图 4-1 为 ePass1000 Manager 程序管理两个 epass1000 的主界面。

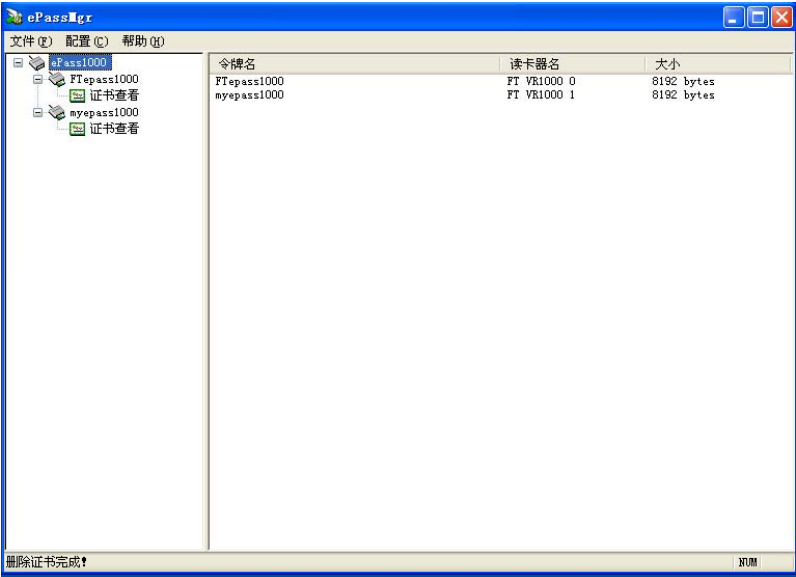


图 4-1

从图 4-1 中我们可以看到，ePass1000 Manager 的功能主要分为两部分：配置 ePass1000 及证书管理。

4.1 配置 ePass1000

在单击 ePass1000 管理器的 ePass1000 的名称，便会见到如图 4-2 所示的界面，此时在管理器主界面下方会出现更多的功能标签，选择不同的标签按钮即可进行不同的管理。

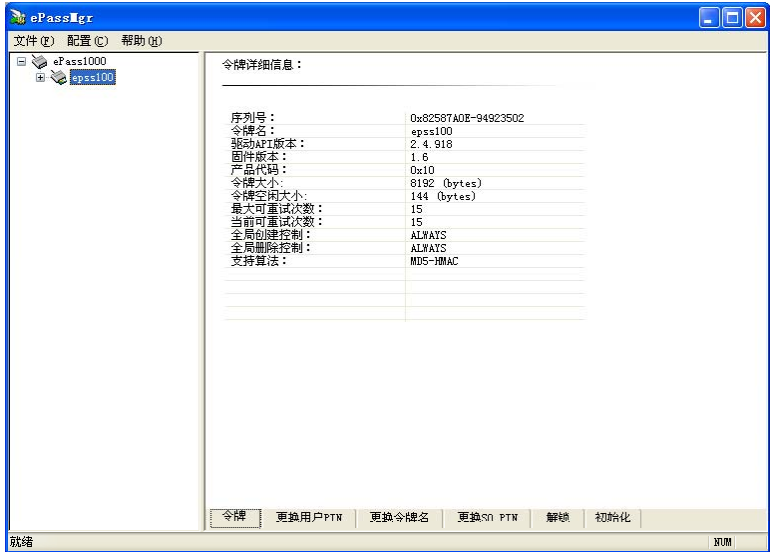


图 4-2

下面依次对这几项功能进行介绍：

4.2 初始化 ePass1000

这对一个基于 ePass1000 的 PKI 应用来说是首先要作的事情。在 ePass1000 初始过程中，将在 ePass1000 硬件的存储空间中划分出一个结构化的区域来存储证书数据，分配合理比例公有存储区及私有存储区的大小。同时要求对 PIN 码及令牌名字进行设定。图 4-3 为单击“初始化”标签按钮后的情况：

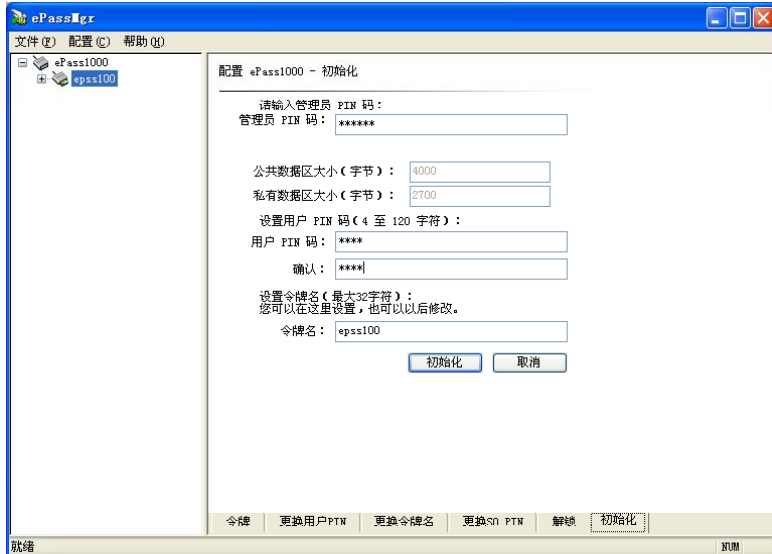


图 4-3

在图 4-3 中的第一个编辑框中必须输入 SO-PIN 即超级用户密码，初始化操作是一个不可逆的操作，此操作将对 ePass1000 进行格式化，原有的数据全部被删除，所以只有超级用户才可进行此操作。

第二个及第三个编辑框将用于设置 ePass1000 公有数据和私有数据的大小，管理器会帮助您预先设定默认值，第四个及第五个编辑框将用于设置 USER-PIN(普通用户密码)，最后一个编辑框输入所要设置定的令牌名；在此操作的过程中，需要注意数据域的长度。

在完整而正确地输入各个数据域之后，便会看到处于最下方的“初始化”按钮处于可用状态，单击此按钮开始初始化过程。

4.3 更改用户 PIN 码

为了 PIN 码的安全性更高，我们可以不定期地更改 PIN 码，此操作保证已有数据的完整性的同时更改 ePass1000 的用户 PIN 码。单击“改变用户 PIN 码”标签按钮时会见到如图 4-4 示的界面：

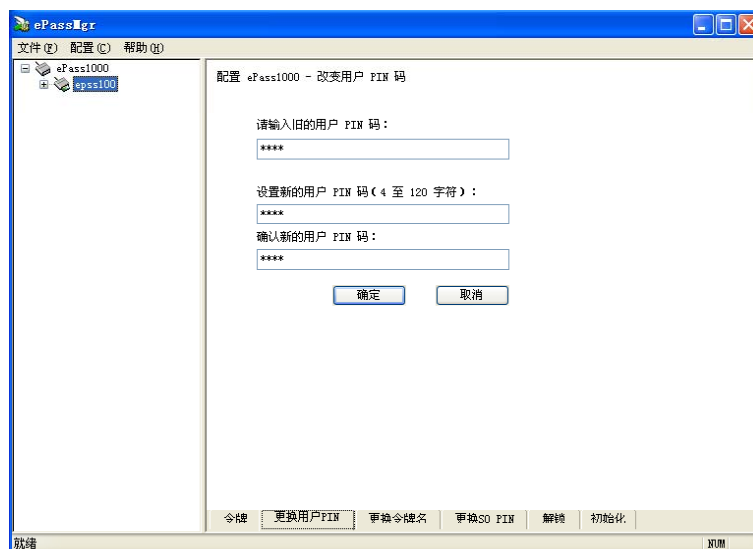


图 4-4

在第一个输入框中输入原来的 PIN，并在第二个及第三个输入所要设定的新的 PIN 码，单击“确定”按钮便执行设定新 PIN 功能，“取消”按钮取消此操作。

4.4 更改令牌名

此功能可用来更改令牌名，单击“改变用户 PIN 码” 标签按钮见图 4-5:

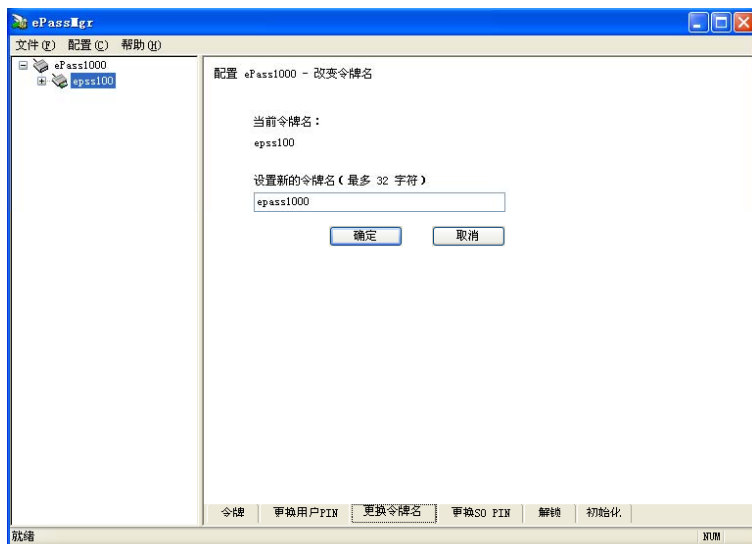


图 4-5

图 4-5 中显示了当前的令牌名并要求用户输入新的令牌名，当用户在编辑框中输入新的令牌名后可按“确定”键确认此操作。

4.5 用户 PIN 码解锁

ePass1000 中的私有数据对于用户来说是非常重要的，因而对其进行有效的保护是十分必要的，ePass1000 中的私有数据存放在受 USER-PIN 保护的区域，并且硬件内部实现了对 PIN 重试次数的限制，一旦用户重试输入错误的 USER-PIN 超过内置设定的重试上限时，ePass1000 便会处于锁定状态，这时即便提供正确的 USER-PIN 也无法正常使用证书，此时只有用超级密码才可解除 ePass1000 的锁定状态。单击“解锁”标签按钮后，便会要求输入超级密码及最大可重次数及当前可重试次数。当前可重试次数决定了用户目前可以重试几次，最大可重试次数用来在用户输入正确的 PIN 码时重置当前可重试次数。同样，单击“确定”确认此操作，“取消”按钮取消操作，参见图 4-6：

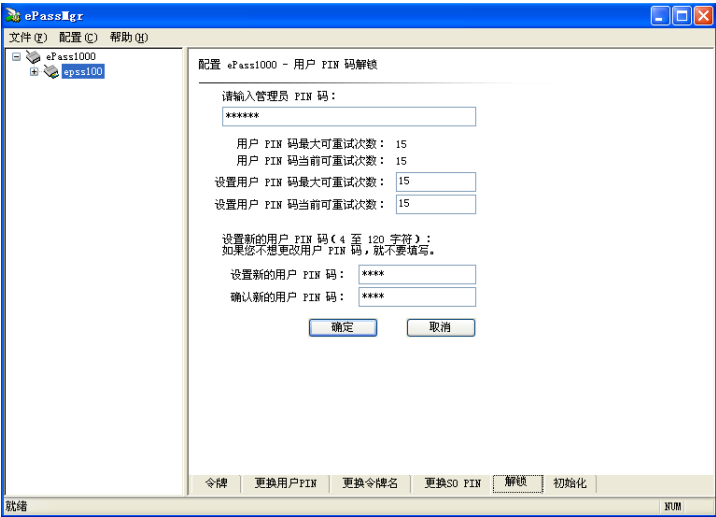


图 4-6

4.6 改变管理员 PIN 码

超级密码一般由基于 ePass1000 应用的发放机构来设定，通过 ePass1000 Manager 也可对此密码进行更改，不过要知道原先的 SO-PIN 才可能更改成功。点击”更换 SO-PIN”标签按钮后如图 4-7 所示：

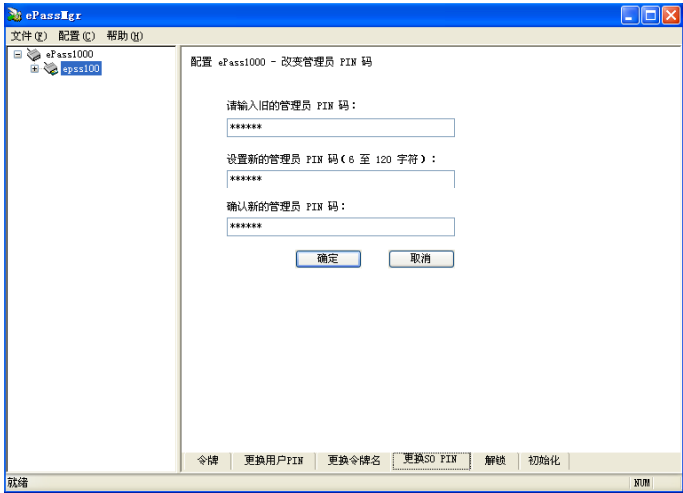


图 4-7

4.7 证书管理

单击“证书查看”标签按钮便会见到如图 4-8 所示的界面：



图 4-8

由于证书中包含受保护的私钥信息，因而只有先登入后才能查看完整的证书信息。输入正确的 USER-PIN 后单击“登入”按钮后便可进入如图 4-9 的界面：

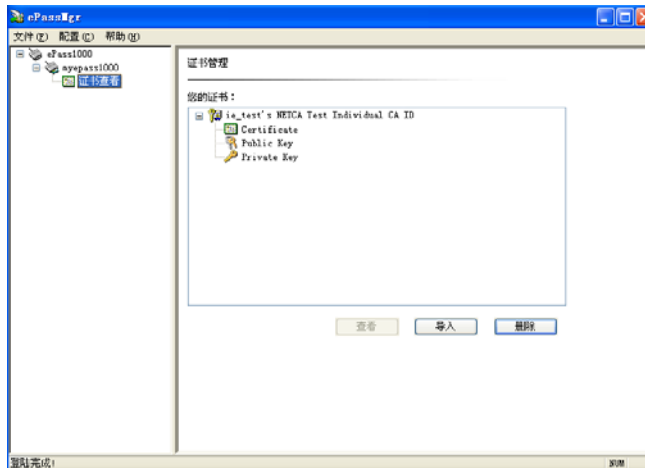


图 4-9

此窗口的右下方的两个按钮“导入”及“删除”按钮分别用于将存于磁盘上的证书文件导入到 ePass1000 硬件中，删除不完整的证书项（由于证书申请过程被异常中断而产生），点击“查看”按钮或双击证书可以查看证书的详细信息，如果是无效数据，则会提示是否删除当前无效数据。

当单击“导入”按钮时的界面如图 4-10 所示：

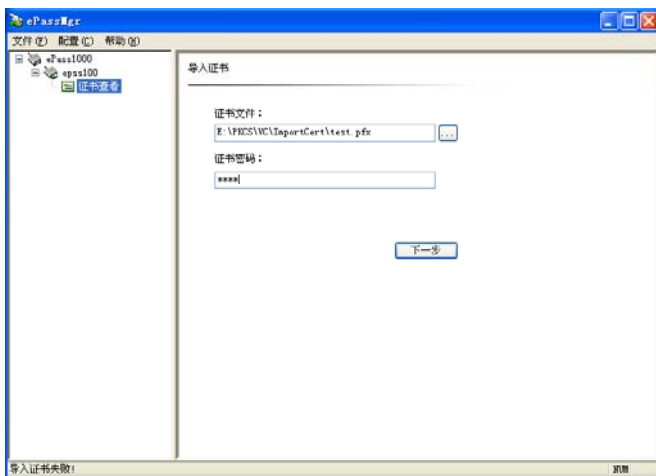


图 4-10

可在“证书文件”处输入证书文件所在的完整路径名或通过单击其右按钮时所弹出的对话框来选择证书所在的位置。在“证书密码”处输入保护此证书的密码，然后单击“下一步”按钮便可完成导入操作。所要注意的是导入的证书格式必须是*.pfx 或*.p12。

进行删除操作时，必须先选择“对象标签”结点后才能进行此操作。如图 4-11：

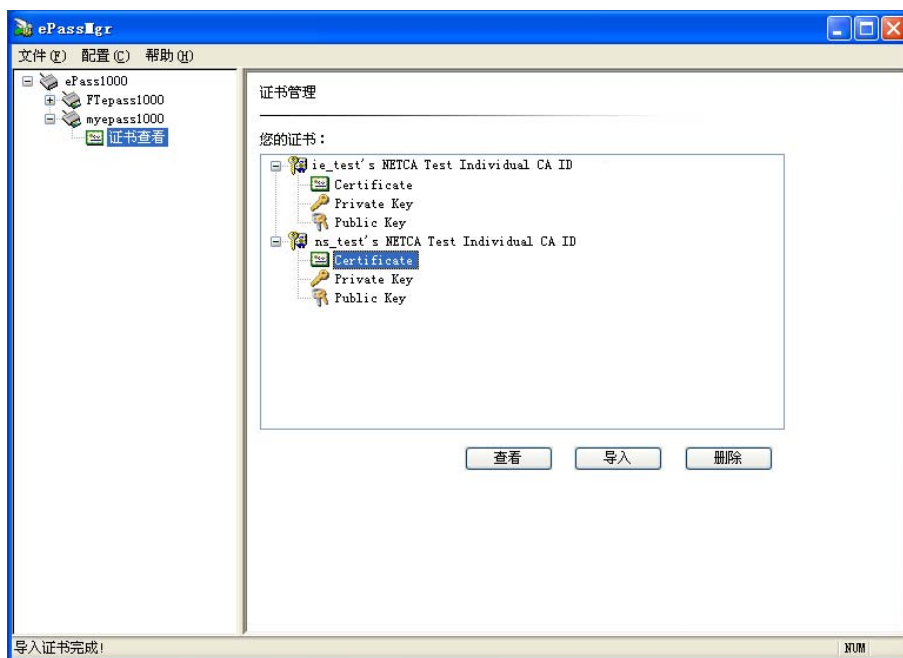


图 4-11

第五章 ePass1000 的 PKI 应用

基于 ePass1000 的诸多优势，PKI 安全体系的开发人员可以轻易的通过集成 ePass1000 到其 PKI 应用中来提高应用的安全性与易用性。例如，企业内联网，虚拟专用网，SSL 加密站点，加密/签名电子邮件等等。

注意：ePass1000 当前仅支持 Win32 平台的 PKI 应用。

本章我们会介绍：

- ✓ ePass1000 PKI 体系
- ✓ ePass1000 PKCS#11 模块
- ✓ ePass1000 的 MS CAPI CSP 模块
- ✓ ePass1000 PKI 应用指南

5.1 ePass1000 PKI 体系

ePass1000 支持两种业界 PKI 标准：RSA Lab 的 PKCS#11 和微软的 CAPI。任何基于这两个标准的 PKI 应用程序都可以轻易的集成 ePass1000，而无需任何编程开发。兼容 MS CAPI 或 PKCS#11 的应用程序可以使用 ePass1000 来存储证书和私钥，生成 RSA/DSA 密钥对，进行数字签名与认证，加密解密数据。如图 5-1 显示了 ePass1000 的 PKI 接口体系：

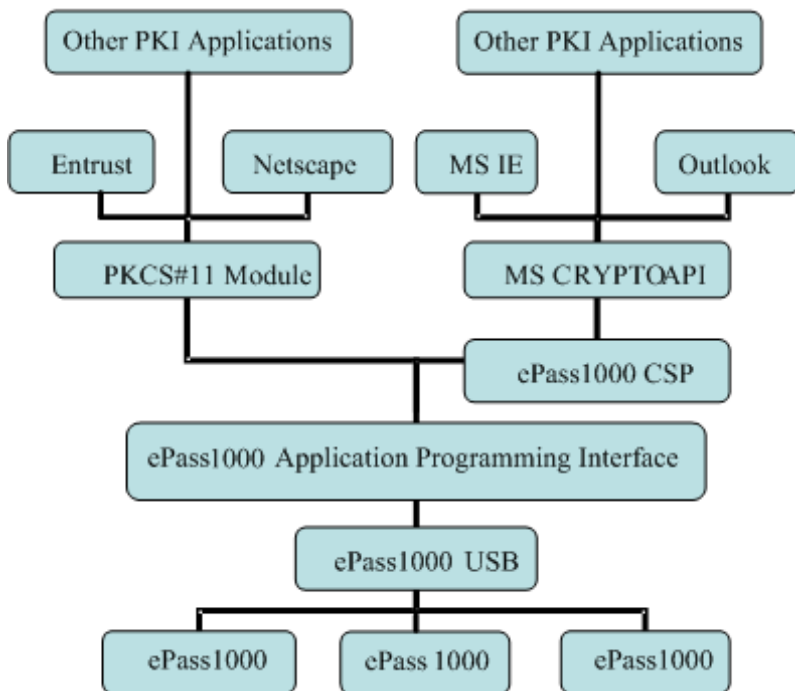


图 5-1

ePass1000 的驱动程序负责管理 ePass1000 与计算机之间所有的通讯。应用程序不直接与驱动程序打交道，而是通过应用程序接口访问 ePass1000。应用程序接口层负责与 USB 驱动通讯。使用哪一层接口对 ePass1000 进行编程取决于应用程序的要求。高层的接口提供更复杂的功能，而底层的接口提供更多的细节控制。但是我们不建议开发人员在一个应用程序中使用不同层次的接口。



5.2 ePass1000 PKCS#11 模块

由于 Internet 全球范围内的爆炸式增长，应用程序对英特网领域中安全事务和通讯的要求也日益迫切。而加密安全产品的迅猛增长也导致了应用程序之间交互性的需求。因此 RSA 公司创立了公开密钥加密标准（PKCS）来满足这一要求。

PKCS#11 是 PKCS 系列标准中的一个。PKCS#11 标准（也称为“Cryptoki”）被设计用来解决不同厂商与开发者的公开密钥加密应用之间交互与兼容的问题。它定义了一个通用的编程接口模型 Cryptoki tokens，ePass1000 正是符合这种模型的产品。

在使用ePass1000 的PKCS#11 接口开发应用程序前，开发人员必须熟悉PKCS#11 标准。这个标准的文档可以在 <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html> 处免费获取。

ePass1000 Cryptoki 模块支持 PKCS # 11 版本 2.10。此模块的实现是一个 Win32 动态连接库。下表列出了开发基于 ePass1000 PKCS#11 接口应用程序需要的文件：

文件	SDK 路径
cryptoki.h	\Include\pkcs(RSA 公司提供)
pkcs11.h	\Include \pkcs(RSA 公司提供)
pkcs11f.h	\Include \pkcs(RSA 公司提供)
pkcs11t.h	\Include \pkcs(RSA 公司提供)
ep1pk111.lib	\Lib
ep1pk111.dll	\Lib (运行时应位于系统目录下)
ep1kdl20.dll	\Lib (运行时应位于系统目录下)

ep1pk111.dll 是 ePass1000 的核心库文件，它实现了 RSA PKCS#11 标准中定义的所有接口函数。如果开发人员需要使用这个接口，必须在工程项目中包含 cryptoki.h 这个头文件。

5.2.1 PKCS#11 类对象

ePass1000 的 PKCS#11 模块支持创建下列类型的对象：

类对象	描述
-----	----

CKO_DATA	应用程序定义数据对象
CKO_SECRET_KEY	对称加密密钥
CKO_CERTIFICATE	X.509 V3 证书
CKO_PUBLIC_KEY	RSA/DSA 公钥
CKO_PRIVATE_KEY	RSA/DSA 私钥

应用程序可以在 ePass1000 中创建和存储上述对象，或者只在运行时创建这些对象。开发人员应当考虑到 ePass1000 存储空间的限制来决定如何处理对象的存储问题。只有需要持续的关键对象才有必要在 ePass1000 内部存储。

5.2.2 ePass1000 支持的 PKCS#11 算法

下表列出了所有 ePass1000 PKCS#1 模块支持的算法：

算 法	加解密	签名 校验	散 列	密钥对 生成	封 装
CKM_RSA_PKCS_KEY_PAIR_GEN				√	
CKM_RSA_PKCS	√	√			
CKM_DSA_KEY_PAIR_GEN				√	
CKM_DSA		√			
CKM_RC2_KEY_GEN				√	
CKM_RC2_ECB	√				
CKM_RC2_CBC	√				
CKM_RC2_CBC_PAD	√				
CKM_RC4_KEY_GEN				√	
CKM_RC4	√				
CKM_DES_KEY_GEN				√	
CKM_DES_ECB	√				
CKM_DES_CBC	√				
CKM_DES_CBC_PAD	√				
CKM_DES3_KEY_GEN				√	
CKM_DES3_ECB	√				
CKM_DES3_CBC	√				
CKM_DES3_CBC_PAD	√				



CKM_MD2			√		
CKM_MD5			√		
CKM_SHA_1			√		
CKM_DH_PKCS_KEY_PAIR_GEN				√	
CKM_DH_PKCS_DERIVE				√	

注：如果是对称密钥，则**密钥对生成**应为**密钥生成**

下表显示了 ePass1000 PKCS#11 库支持的密钥长度：

算法	密钥长度
CKM_RSA_KEY_PAIR_GEN	512-2048 bits
CKM_DSA_KEY_PAIR_GEN	508-1024 bits
CKM_DH_PKCS_KEY_PAIR_GEN	128-2048bits
CKM_RC2_KEY_GEN	1-128 bytes
CKM_RC4_KEY_GEN	1-256 bytes
CKM_DES_KEY_GEN	8 bytes
CKM_DES3_KEY_GEN	24 bytes
CKM_DH_PKCS_DERIVE	1-128bytes

5.2.3 ePass1000 PKCS#11 库函数

开发人员和硬件厂商要集成ePass1000 的PKCS#11 模块就必须熟悉 PKCS#11 标准。（标准见RSA 公司的网站<http://www.rsasecurity.com>。）

PKCS#11 是针对 Cryptoki 硬件的通用模型定义。不同厂商的 PKCS#11 会有一些细节上的不同。

ePass1000 的 PKCS#11 接口也有一些不同于标准的地方：

- ✓ 有极少数 PKCS#11 标准中的函数没有被实现，调用这些函数只会返回 CKR_FUNCTION_NOT_SUPPORT 错误。

注意：ePass1000 就相当于 PKCS#11 标注中所指的“token”。

PKCS#11 标准中将读卡器称为“slot”，但是由于 ePass1000 并不需要读卡器，因此 ePass1000 PKCS#11 实现中的 slot 只是个虚拟的设备。

下表列出了 PKCS#11 定义的函数：

名称	描述
一般功能函数	

C_Initialize	这个函数初始化库。在调用其它库函数前必须调用此函数。唯一的例外是 C_GetFunctionList 函数。
C_Finalize	当应用程序结束对库的访问时应调用此函数。
C_GetInfo	得到 cryptoki 库的信息。
C_GetFunctionList	得到库导出的函数指针列表
Slot 和 Token 管理函数	
C_GetSlotList	得到 slot 列表。
C_GetSlotInfo	获取 slot 的信息。
C_GetTokenInfo	获取 slot 中 token 的信息。
C_WaitForSlotEvent	等待 slot 事件的发生，如 token 被插入或删除。
C_GetMechanismList	获取库支持算法的列表。
C_GetMechanismInfo	获取算法详细信息。
C_InitToken	初始化 token。
C_InitPIN	初始化 USER-PIN。
C_SetPIN	修改当前登录用户的 PIN 码。
会话管理函数	
C_OpenSession	在应用程序和 token 之间建立会话。
C_CloseSession	关闭会话。
C_CloseAllSessions	关闭应用程序打开的所有会话。
C_GetSessionInfo	获取会话的信息
C_GetOperationState	获取当前加密操作的状态
C_SetOperationState	使用从 C_GetOperationState 调用功能返回的状态恢复库的操作状态。.
C_Login	登录用户到 token。
C_Logout	登出用户。
对象管理函数	
C_CreateObject	创建新的 Cryptoki 对象。
C_CopyObject	创建对象的拷贝。
C_DestroyObject	删除一个对象。

C_GetObjectSize	获取对象的大小。
C_GetAttributeValue	获取对象一个或多个属性。
C_SetAttributeValue	修改对象的一个或多个属性。
C_FindObjectsInit	初始化一次对象查找操作。
C_FindObjects	查找对象。
C_FindObjectsFinal	结束一次对象查找操作。
加密函数	
C_EncryptInit	初始化一次加密操作
C_Encrypt	加密数据
C_EncryptUpdate	继续加密数据
C_EncryptFinal	结束数据加密操作。
解密函数	
C_DecryptInit	初始化一次解密操作。
C_Decrypt	解密输入数据。
C_DecryptUpdate	继续解密操作。
C_DecryptFinal	结束一次解密操作。
消息散列函数	
C_DigestInit	初始化一次散列操作。
C_Digest	散列输入的数据。
C_DigestUpdate	继续散列操作。
C_DigestKey	继续散列一个密钥。
C_DigestFinal	结束散列操作。
签名与消息鉴别函数	
C_SignInit	初始化一次签名操作
C_Sign	签名输入数据
C_SignUpdate	继续一次数据签名操作
C_SignFinal	结束数据签名操作
C_SignRecoverInit	初始化一次数据可恢复的签名操作。
C_SignRecover	继续签名操作。
校验签名和消息鉴别函数	
C_VerifyInit	初始化一次校验操作。
C_Verify	校验一个签名。

C_VerifyUpdate	继续校验签名。
C_VerifyFinal	结束一次校验操作。
C_VerifyRecoverInit	初始化一次数据可恢复校验操作。
C_VerifyRecover	校验数据可恢复的签名。
双功能加密函数	
C_DigestEncryptUpdate	继续一次散列并加密操作。
C_DecryptDigestUpdate	继续一次解密并散列操作。
C_SignEncryptUpdate	继续一次签名并加密操作。
C_DecryptVerifyUpdate	继续一次解密并校验操作。
密钥管理函数	
C_GenerateKey	生成密钥并创建新的密钥对象。
C_GenerateKeyPair	生成密钥对并创建新的公私钥对象。
C_DeriveKey	派生一个私钥或密钥。
C_WrapKey	包装一个私钥或密钥。
C_UnwrapKey	解包一个私钥或密钥。
随机数生成函数	
C_SeedRandom	加入随机种子到生成器中。
C_GenerateRandom	生成随机数。
并行功能管理函数	
C_GetFunctionStatus	这个函数已经废弃。
C_CancelFunction	这个函数已经废弃。

5.3 ePass1000 的 MS CAPI CSP 模块

微软的 CryptoAPI 是 Win32 应用程序的通用加密接口。这个标准包括了数据编码解码，散列，加密解密，数字签名，证书存储等功能。

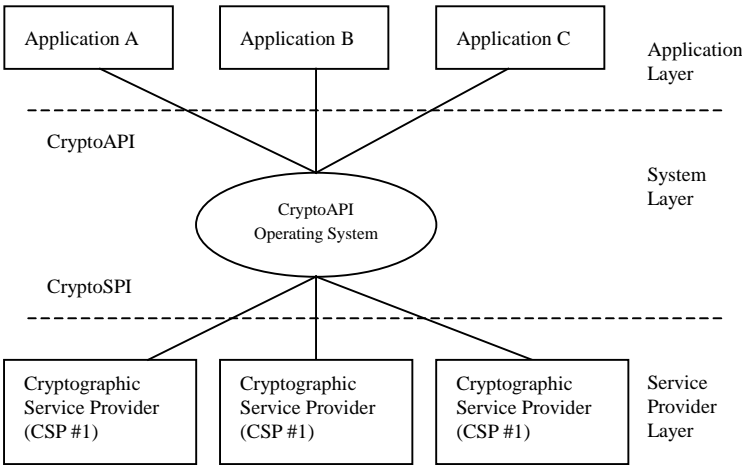


图 5-2

图 5-2 显示了 CAPI 的体系结构。

从图 5-2 中可以看出 CSP 是加密功能的实际提供模块。应用程序不直接与 CSP 打交道而是通过 CryptoAPI 来协调应用程序与 CSP 之间的交互。在一个 CryptoAPI 环境中，应用程序可通过 CSP 来访问 ePass1000。

要获得更多关于微软CAPI的信息可浏览微软软件开发者网络MSDN网站：<http://www.microsoft.com>。

ePass1000 的 CSP 是一个 PROV_RSA_FULL 类型的 CSP。应用程序应当调用 CAPI 来建立与 ePass1000 之间的通讯。CAPI 将为应用程序与 ePass1000 交互。不同厂商的 CSP 实现模块都有可能因为 token 的特性而有所不同。

下表列出了 ePass1000 的 CSP 函数：

名称	描述
连接函数	
CPAcquireContext	创建上下文，初始化对 CSP 的访问，这里可以且必须指定要使用的 CSP。
CPGetProvParam	返回 CSP 相关的信息
CPReleaseContext	释放 CPAcquireContext 中创建的上下文，并作其他释放资源等操作
CPSetProvParam	设置 CSP 的参数操作

密钥生成和交换函数	
CPDeriveKey	从一个数据散列中生成一个会话密钥，它保证生成的密钥互不相同
CPDestroyKey	释放一个密钥句柄；释放后句柄将无效，密钥将无法再被访问
CPDuplicateKey	创建密钥的一个拷贝
CPExportKey	从 CSP 容器中导出密钥
CPGenKey	生成密钥或密钥对
CPGenRandom	产生随机数据
CPGetKeyParam	得到加密操作密钥的属性
CPGetUserKey	获取 CSP 容器中的持久密钥对
CPImportKey	从一个 blob 中导入密钥到 CSP 容器中
CPSetKeyParam	设置密钥的属性
数据加密函数	
CPDecrypt	解密已加密的数据
CPEncrypt	加密明文
散列和数字签名函数	
CPCreateHash	创建一个散列对象并进行初始化
CPDestroyHash	删除一个散列对象句柄
CPDuplicateHash	创建一个散列对象的拷贝
CPGetHashParam	获取散列对象的计算结果
CPHashData	散列输入的数据
CPHashSessionKey	这个函数散列一个会话密钥而不向应用程序暴露密钥的值
CPSetHashParam	这个函数设置一个散列对象的属性
CPSignHash	这个函数签名一个散列对象
CPVerifySignature	这个函数校验一个数字签名

5.4 同时连接多个 ePass1000

ePass1000 中间件支持在同一台计算机上同时连接多个 ePass1000 设

备, PKCS#11 或者 MS CSP 在 PKI 应用当中可以有选择地使用某一个 ePass1000 来存储、管理证书或者保存其它的数据。比如在申请证书时, 可以选择不同的 ePass1000 来存放证书; 在浏览器中可以看到多把 ePass1000 中已存放的证书。

注意, 由于 Windows 平台中智能卡子系统的限制, 最多只能安装 10 个读卡器设备!

5.5 ePass1000 PKI 应用指南

ePass1000 的设计目标之一就是与现有的 PKI 体系应用无缝的集成。PKI 应用开发商无需对 ePass1000 进行任何形式的编程就能通过配置相关服务而开始将 ePass1000 集成于 PKI 应用当中。本节主要讲述如何利用 ePass1000 进行一些 PKI 应用。

- ✓ 配置证书颁发机构
- ✓ 配置 SSL 加密站点
- ✓ 使用 ePass1000 申请数字证书
- ✓ 使用 ePass1000 访问 SSL 加密站点
- ✓ 使用 ePass1000 收发签名与加密邮件
- ✓ 使用 ePass1000 进行 Win2000 智能卡登录
- ✓ 使用 ePass1000 进行 VPN 远程登录

5.5.1 配置证书颁发机构

证书颁发机构亦即通常所说的 CA 中心, 是 PKI 应用的核心。任何 PKI 应用都需要 CA 中心的支持。Windows 2000/XP/2003 系统内建了很多对 PKI 应用的支持, 通过适当的配置可实现智能卡登录, 锁定工作站, VPN 远程登录, SSL 加密站点访问等功能。下面我们将以 Windows Server 2003 自带的证书颁发机构为例, 讲解配置证书颁发机构的一般步骤。

安装证书颁发机构

Windows Server2003 缺省情况下并不会自动安装证书服务。这是由于安装完证书服务后, Windows Server 2003 计算机就无法再更改计算机名称了, 为了提高系统管理灵活性, Windows Server 2003 不会自动安装证

书服务。如果要设置一台证书服务器，就必须手工安装证书服务。

若要在 Windows Server 2003 计算机上安装证书颁发机构(CA), 请按照下列的步骤进行操作:

1. 以系统管理员权限的帐号本地登录服务器。
2. 请依序打开“开始”菜单→“设置”→“控制面板”选项，以启动 Windows Server 2003 控制面板。
3. 接着，选择“添加/删除程序”，启动添加/删除程序，如图 5-3 所示。

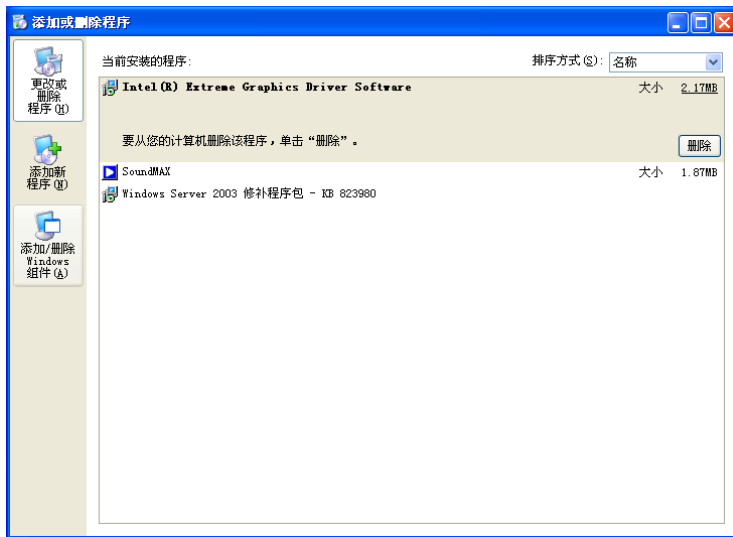


图 5-3 添加/删除程序

4. 接着，请选择“添加/删除 Windows 组件”选项，这时候，系统会启动 Windows 组件向导，让用户选择想安装的 Windows Server 2003 操作系统的相关服务或工具的组件。如图 5-4 所示。

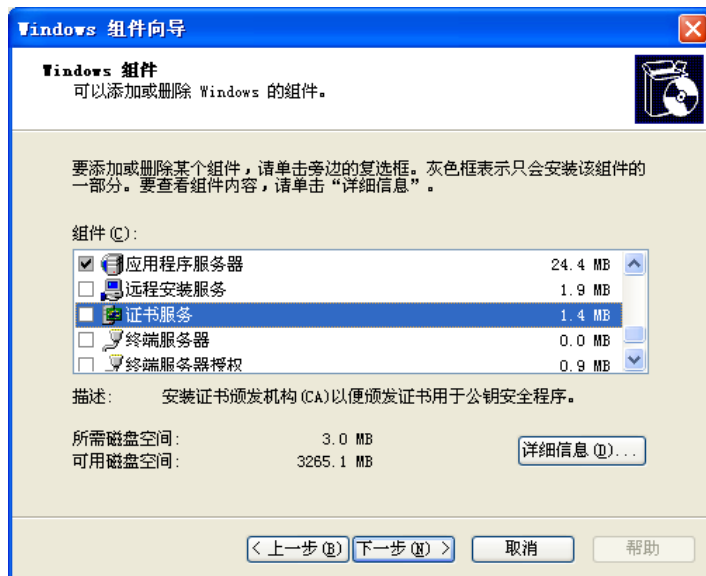


图 5-4 添加/删除 Windows 组件向导

5. 请在 Windows 组件向导的“组件”列表里，选择“证书服务”的选项，以便在 Windows Server 2003 计算机上安装证书服务。

当在 Windows Server 2003 计算机上安装了证书服务后，这台机器就会成为证书颁发机构的证书服务器，因此，就无法对其重新命名，也无法加入其他的域、或者由现存的域中删除。

6. 当勾选“证书服务”的选项后，请接着按“下一步”按钮。接下来，系统会出现证书授权类型的设置过程。只需要按照需要，选择要安装的证书颁发机构 (CA) 的类型即可。用户可以选择设置的各种证书颁发机构的类型以及用途如下 (参见图 5-5)：

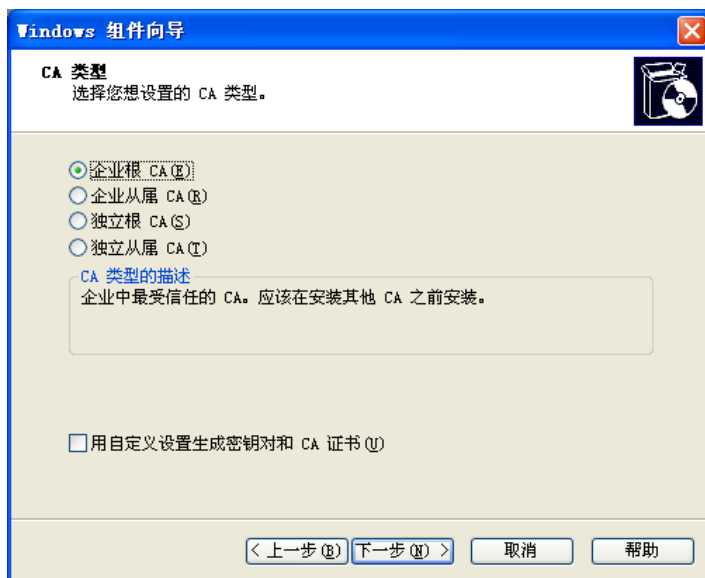


图 5-5 选择证书颁发机构类型

企业根证书颁发机构(Enterprise Root CA): 如果本证书颁发机构要将证书发行到企业 Active Directory 域内所有的个体上, 用户就必须选择此选项。请注意, 本证书颁发机构将会登记在 Active Directory 域内。如果企业的硬件资源足够时, 建议只将企业根证书颁发机构(Root CA)用在发行授权(证书)给企业从属证书颁发机构(Subordinate CA)的用途上, 因为这样可以确保较好的安全性。如果企业域内部目前并没有任何的证书颁发机构, 也必须选择安装主要证书颁发机构(Root CA)。

企业从属证书颁发机构(Enterprise Subordinate CA): 如果本证书颁发机构要将证书发行到企业 Active Directory 域内的每一个个体上, 而且企业域上已经有一个企业根证书颁发证书机构, 就可以选择此选项。请注意, 本证书颁发机构将会登记在 Active Directory 域内。

独立根证书颁发机构(Stand-alone root CA): 如果本证书颁发机构将要发行证书给企业域外部的个体使用时, 就必须选择这种证书颁发机构方式。选择了这种方式的证书颁发机构, 将会成为一个

证书颁发机构层次架构的独立根证书颁发机构。

独立从属证书颁发机构 (Stand-alone subordinate CA)：如果要将本证书颁发机构设置为一个已经设置好的证书层次架构里的一员，就应该选择此选项。证书层次架构组织可以是用户之前所安装的独立证书系统，也可以是存在于企业外部的一个商用证书颁发机构。

在图 5-5 中显示选择了企业根证书颁发机构。

在 Windows Server 2003 操作系统的证书服务器上已经采用了默认的加密系统，提供证书的安全机制。若要设置证书颁发机构一些高级设置值(例如证书颁发机构所使用的密码编译服务提供者(CSP)、数字签名或信息完整性检查所使用的散列算法、证书所使用的密钥长度、所使用的密钥类型等)，可以勾选下方的“高级选项”复选框。若勾选了此选项的话，当按下“下一步”按钮时，接下来会出现“公钥/私钥对”的设置窗口。如图 5-6 所示：



图 5-6 公钥/私钥对高级设置

在这里可以更改系统默认的加密功能，例如使用哪一种密码编译

服务提供者（CSP）、使用哪一种散列算法等等。

用户可以在“密钥长度”的选择框里调整加密数据时所使用的密钥长度。一般来说，密钥长度越长，加密结果越安全，但是所需要的加密/解密时间越长。如果选择“默认”的密钥长度，系统会根据所选择的 CSP 来自动设置所需要的密钥长度。我们建议用户在许可的范围内，尽量选择较长的密钥长度。有些硬件可能无法支持较长的密钥长度（例如基于存储区容量限制、加密/解密速度限制等因素）。

如果要使用已经存在的密钥，请选择下方的“使用现有密钥”框以及“导入”按钮来设置此证书颁发机构所使用的密钥。

完成上述的设置后，请按“下一步”按钮，继续证书颁发机构的安装设置。

7. 接下来，向导会出现“CA 标识信息”的设置窗口。用户必须在此窗口里设置此证书颁发机构的标识信息，如图 5-7 所示：

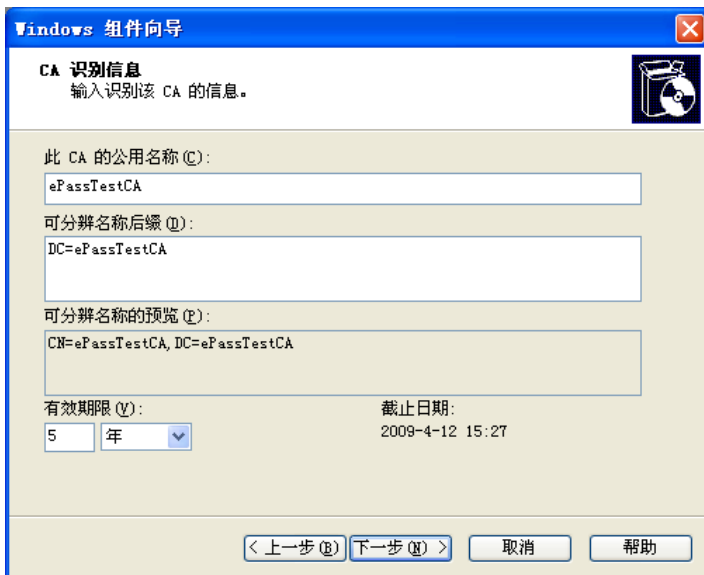


图 5-7 证书颁发机构标识信息

在这里请用户要特别注意，在“CA 名称”的字段上，用户务必为此证书颁发机构命名一个名称，因为稍后将会使用此名称来标识建立在证书服务器上的证书颁发机构对象。

如果用户建立的是企业型的证书颁发机构，此名称将会使用来标识建立在 Active Directory 域内的证书颁发机构对象，如果用户建立的是独立证书颁发机构，此名称将会使用在标识此证书颁发机构上。在这里，还需要注意另外一点，如果所设置的是根证书颁发机构(Root CA)，那证书颁发机构的“有效期限”需要比较长的时间，至少都需要比从属证书颁发机构的有效时间长。如果设置的根证书颁发机构，请将“有效期限”设置在一个合理的时间内。当然用户必须考虑到安全以及系统管理的负担，从两个不同的角度考虑，获取一个平衡点。当根证书服务器的有效期限过期时，系统管理人员就必须重新刷新一次所有的信任关系。

当完成上述的设置后，请按“下一步”按钮，继续下一个证书颁发机构的设置过程。

8. 接下来，向导会出现“数据储存位置”的窗口（参见图 5-8），这里主要是设定证书数据库的储存位置、证书服务器设置信息的储存位置、储存证书撤销列表的位置以及证书数据库记录文件的位置。



图 5-8 指定相关数据储存位置

如果所设置的证书颁发机构类型为企业型的证书颁发机构，则企业型的证书颁发机构会将它的一些设置信息以及属性信息存储在域里（域控制器上）。

如果不是在域控制计算机上设置证书服务器，请选择“共享文件夹”选项，并输入一个本地共享文件夹路径，用来指定证书颁发机构设置信息的存储位置（用户可以指定在共享文件夹里，这样即使没有加入到域的客户端机器，也能够获取证书吊销列表的相关信息）。

完成上述的设置后，请按“下一步”按钮，继续下一个证书颁发机构的设置步骤。

9. 如果安装的是一个从属证书颁发机构，用户将会看到“CA 证书申请的设置窗口（如果您安装的不是从属证书颁发机构，请跳到步骤 10）。之前，我们曾经提到过，从属证书颁发机构会直接向根证书颁发机构获取证书信息，在这里，就要指定这个根证书颁发机构。用户可以选择采用网络直接传输的方式，或者以文件形式

的方式，来获取证书颁发机构的证书信息。若采用网络直接传输的方式，需要指定根证书颁发机构计算机名称、以及证书颁发机构的名称。若采用文件形式来获取根证书颁发机构的证书信息，需要指定存储证书信息的文件位置（参见图 5-9）。

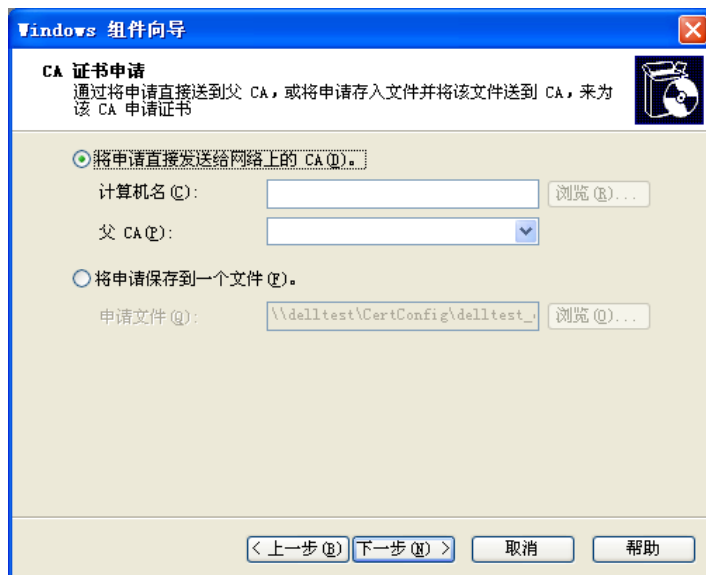


图 5-9 选择获取证书授权的主要证书颁发机构

用户可以选择“将申请直接发送给网络上的 CA”选项，并按下“浏览”按钮，选择一台可以获取证书授权的根证书服务器以及证书颁发机构。如果必须由特定的商用证书颁发机构获取授权证书信息，或者需要获取授权的证书颁发机构无法由网络上获取授权信息时，用户可以选择“将申请保存到一个文件”的选项，并将此文件带到指定的主要证书颁发机构上处理，获取发行证书的授权。

当完成上述的设置后，请按“下一步”按钮，继续下一个证书颁发机构的设置过程。

10. 因为 Microsoft 的证书服务需要 IIS(Internet Information Server，因特网信息服务)服务的支持，因此，如果这时候 IIS 正在运行，系统会提示停止 IIS，以便顺利安装证书服务器(参见

图 5-10)。



图 5-10 要求停止 IIS 的执行

11. 按下“确定”按钮，证书服务安装向导便开始安装证书服务器相关的组件以及程序，如图 5-11 所示。

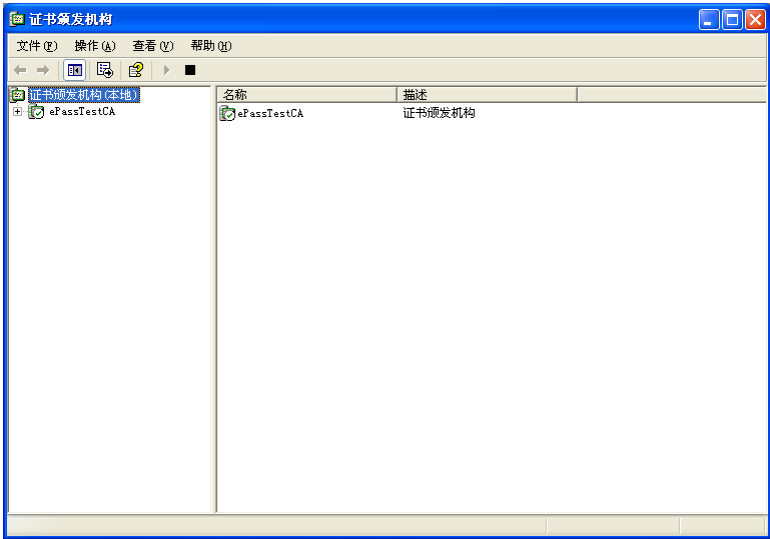


图 5-11 证书服务器组件安装

请注意一下%SystemRoot%\system32\CerSrv\CertEnroll 文件夹是共享的。因为证书服务的客户端计算机会需要获取此文件夹下的信息，以便核对吊销的相关信息。如果此文件夹没有处于共享状态，证书服务客户端计算机可能会无法正常运行。

12. 这时候证书服务已经成功地安装在服务器上了。可以由“开始”菜单→“程序”→“管理工具”→“证书颁发机构”选项，启动

证书颁发机构系统管理工具(见图 5-12)，来管理证书颁发机构。



5-12 证书授权系统管理工具

5.5.2 安装根证书

客户端开始向证书颁发机构申请证书前，必须先安装该证书颁发机构的根证书，没有证书颁发机构的根证书，就无法正确验证由该证书颁发机构颁发的证书的有效性。另外，如果没有证书颁发机构的根证书，将无法从该证书颁发机构申请证书。

下面我们说明如何由证书颁发机构获取并安装根证书。

1. 启动IE浏览器，并连接到证书服务器（例如http://证书服务器的DNS名称/certsrv, 例如，假设在delltest这台服务器上安装了根证书颁发机构，用户就可以用 http://delltest/certsrv 进行访问）。此时就进入到证书颁发机构的证书发行网页，如图 5-13 所示。

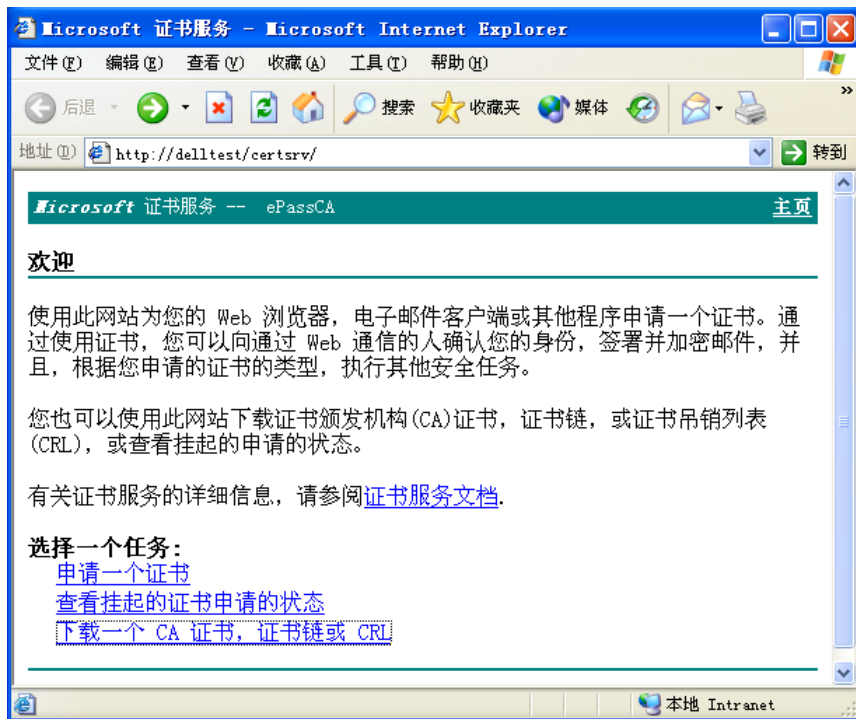


图 5-13 证书授权网页

因为现在需要先获取该证书颁发机构的根证书，因此，请选择“下载一个 CA 证书，证书链或 CRL”的选项。

2. 当按下“下载一个 CA 证书，证书链或 CRL”后，页面上会列出一系列安装或者下载 CA 证书的链接，如图 5-15 所示。

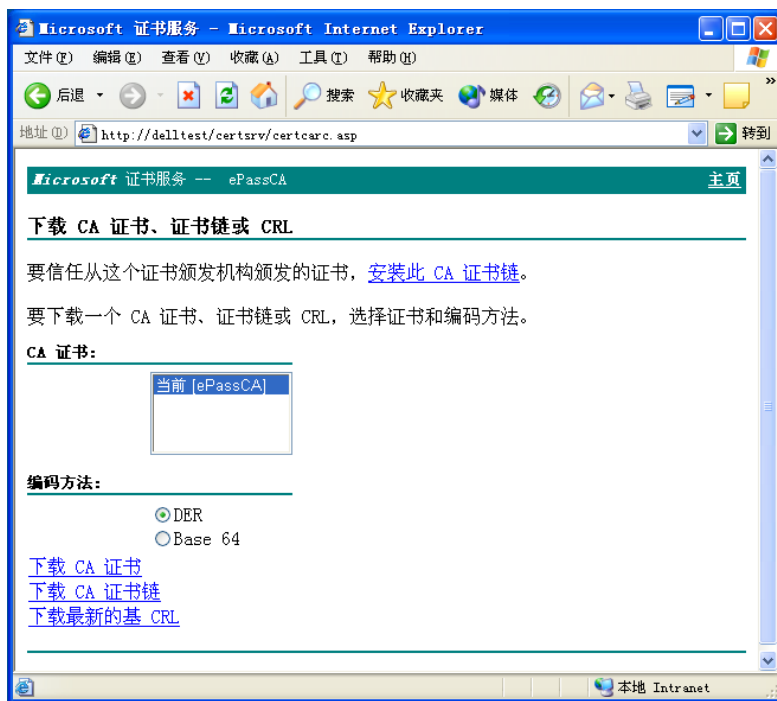


图 5-15 证书颁发机构的证书下载安装窗口

可以直接选择“安装此 CA 证书路径”的链接，当按下此链接后，系统会自动将该证书颁发机构的证书路径(证书信任关系)安装到客户端计算机上，这时候，用户就可以使用该证书颁发机构所发行的证书，来完成身份验证或其他安全性的处理(参见图 5-16)。



图 5-16 自动安装 CA 证书路径

除了选择上述的“安装此 CA 证书路径”的链接方法以外，用户还可以选择下方的“下载 CA 证书”的链接，以手动的方式获取证书颁发机构所发出的证书信息。可以采用 DER 编码的方式、或者以 Base 64 编码的方式，证书颁发机构会将数字证书进行编码，用户可以通过浏览器下载证书文件，供以后导入只用。

3. 选择编码形式后，直接按下“下载 CA 证书”的链接，这时候系统就会以用户所选择的证书编码形式，将证书下载到客户端系统中，如图 5-17 所示。

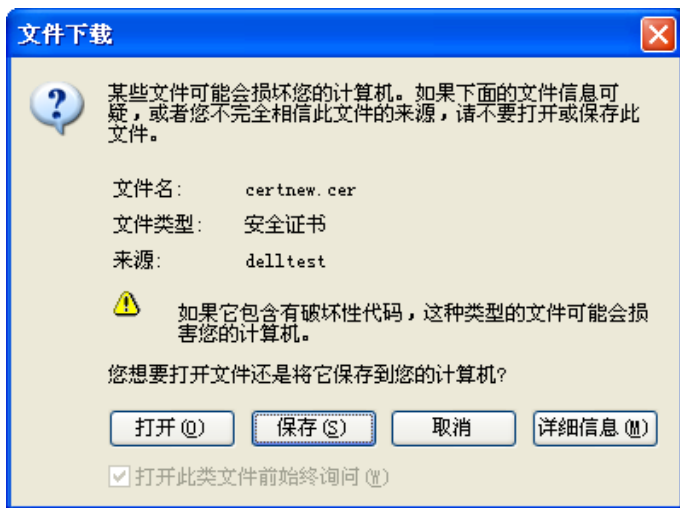


图 5-17 下载 CA 证书

4. 如果要查看此证书，可以选择“打开”选项。这时候，系统便会立即下载并打开这个证书文件，如图 5-18 所示。

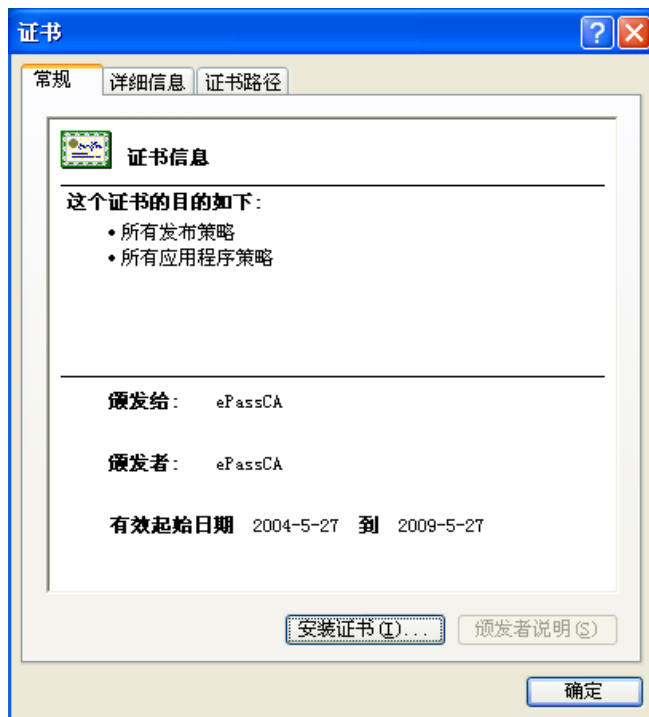


图 5-18 打开证书

5. 用户可以查看此证书的相关信息，若确定无误后，可以按下“常规”页面下方的“安装证书”按钮，系统会启动证书导入向导以便将此证书安装到客户端系统中。如图 5-19 所示。

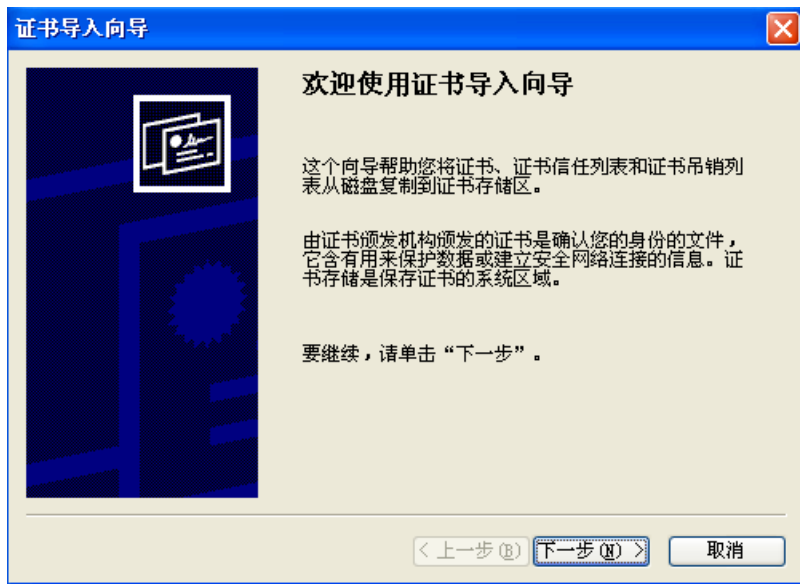


图 5-19 证书导入向导

用户只需要按照证书导入向导的提示步骤，依序进行操作，即可将证书顺利安装到用户计算机的运行环境上。

用户还可以通过这种方式下载该证书颁发机构发行的证书吊销列表。

5.5.3 配置 SSL 加密站点

IIS(Internet Information Service)是 Windows 平台上提供的因特网信息服务，主要提供了 HTTP、FTP 等因特网上的重要服务。安装 Windows Server 2003 操作系统时，Windows Server 2003 操作系统的安装程序默认不会将 IIS 的相关组件安装到计算机上。

如果还没有安装 IIS 组件，用户可以由“配置服务器向导”来完成安装。如图 5-23 所示。

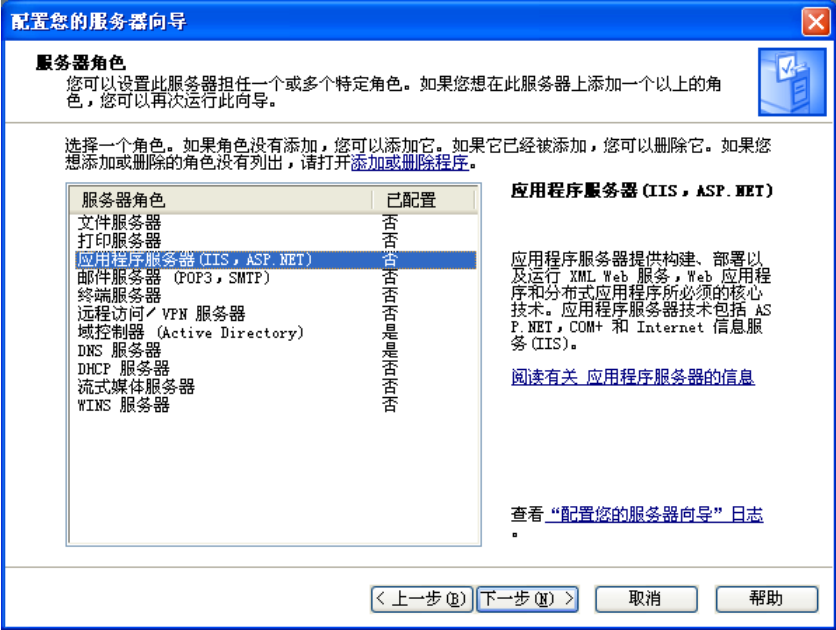


图 5-23 安装 IIS

假设用户已经安装了 IIS，而且目前 IIS 已经开始启动运行了，可以由“开始”菜单→“控制面板”→“管理工具”→“Internet 服务管理器”选项，来启动 IIS 服务管理工具，如图 5-24 所示。

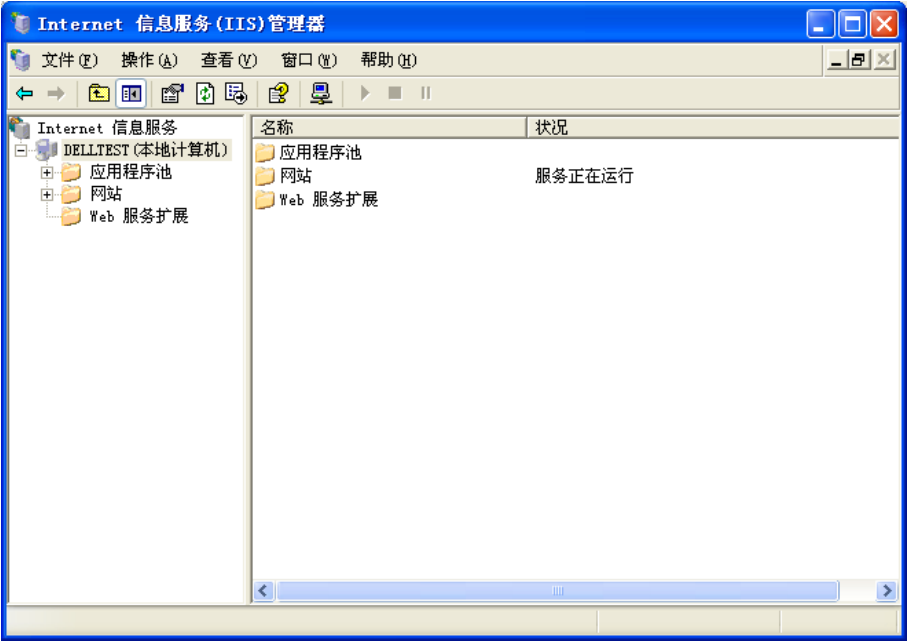


图 5-24 IIS 管理界面

因为 Windows Server 2003 上默认是 ASP 服务是没有启动的。如图 5-25 所示：

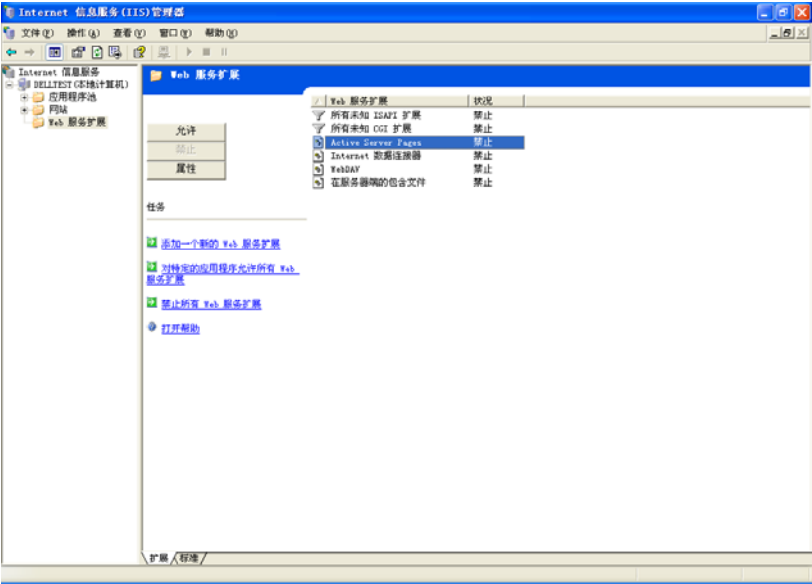


图 5-25 禁止 ASP 界面

选择 Active Server Page 后选择启动按钮来启动 ASP 支持，启动后的界面如下：

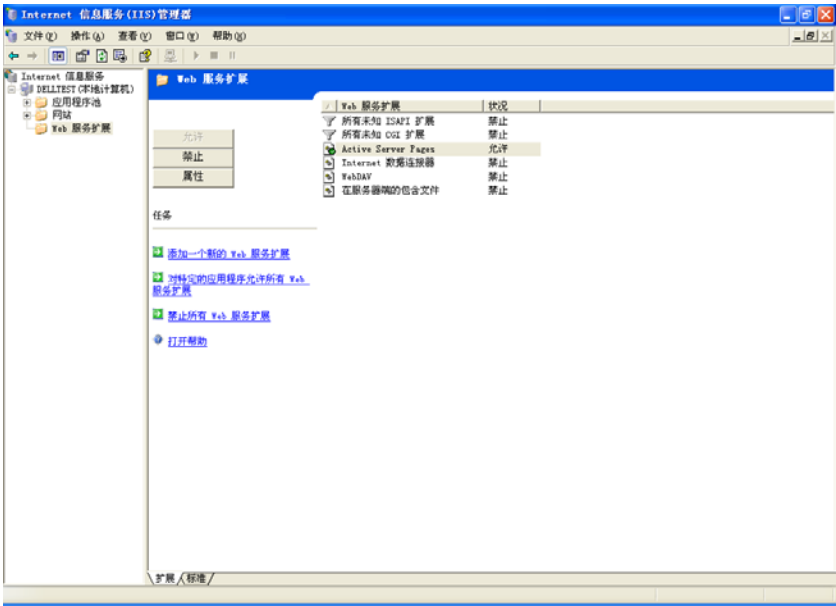


图 5-26 启动 ASP 界面

我们的目的是要设置 IIS 系统，让用户 IIS 系统内的 Web 站点能够具备使用 SSL 通讯协议的能力。

下面详细讲解如何配置使用 SSL 安全通讯协议：

1. 以系统管理员权限的账户本地登录 WEB 服务器。
2. 通过“开始”菜单→“程序”→“管理工具”→“Internet 服务管理器”选项，来启动 IIS 服务管理工具。如图 5-24 所示。
3. 展开控制台里的“Internet 信息服务”节点，点击想要设置的服务器计算机名称。展开节点。如图 5-24 所示。
4. 右键点击“网站”，选择属性。如图 5-27 所示。请选择“目录安全性”页面。

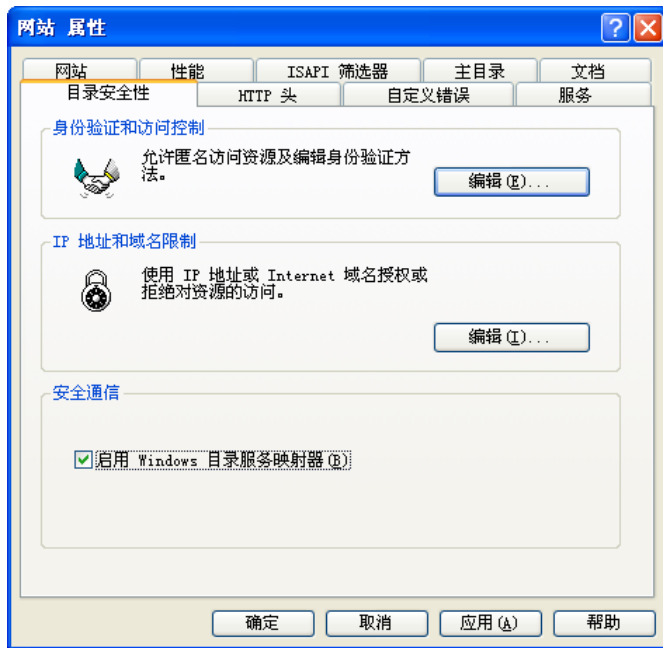


图 5-27 目录安全性设置

接着，请勾选“安全通信”部分的“启用 Windows 目录服务映射器”的复选框选项。

如果在这里勾选“启用 Windows 目录服务映射器”的选项，那么 IIS 将会要求 Active Directory 域控制器来负责处理证书与帐号的映射关系。请注意，只有在 IIS 主要属性里，才可以设置此选项。

如果使用 Windows Server 2003 Active Directory 域控制器的映射方式，用户就可以使用由在企业内部的证书颁发机构所发给的登录证书来连接上企业的 Web 站点。因为根据默认的状态，Windows Server 2003 会自动完成一对一的证书与用户账户的映射关系，所以用户目前就可以采用此映射关系来连接 Web 网站。

5. 我们来看看如何设置一个单一的 Web 站点的安全功能。若用户不希望使用到 Windows Server 2003 Active Directory 域的映射功能(也就是用户在前一个操作步骤里没有勾选“启用 Windows 目

录服务映射器”的复选框选项)，直接跳到这一小节来操作即可。

在 IIS 里，可以同时设置管理多个国际互联网信息服务器（包括多部的 WWW Server、多部的 FTP Server、抑或是其他的国际互联网上的信息服务器），前面所说明的部分是针对整个 IIS 的安全性控管的设置（称为主 IIS 目录安全设置），接下来，我们便要说明如何针对 IIS 内部的一个站点做安全性的设置与管理。

在想设置的服务节点上（例如“默认的 Web 站点”），按下鼠标右键，并选择“属性”选项。

系统会打开该服务节点的属性设置窗口，请选择“目录安全性”的页面，如图 5-27a 所示。



图 5-27a 目录安全性页面

当要开始启用 IIS 功能时，必须先获取一个服务器证书，以提供基础的证书身份验证服务。

注意：在“安全通信”组中，若用户还未获取并安装 Web 服务器证书，这时候“编辑”按钮为不可用的状态。用户必须先安装服务器证书，才能继续编辑安全通信的属性。要安装服务器使用的证书，请按“服务器证书”按钮。

6. 当按下“服务器证书”按钮后，接着会出现 Web 服务器证书向导，指导用户进行服务器证书的安装过程，如图 5-28 所示。

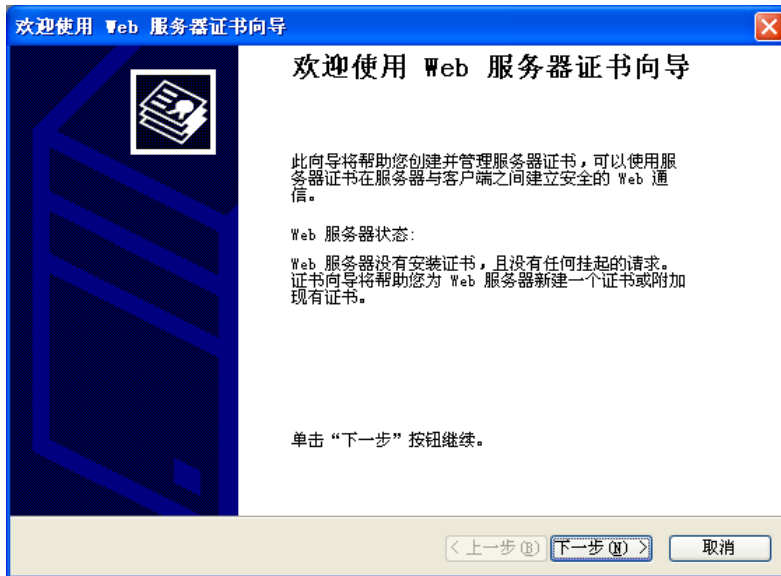


图 5-28 Web 服务器证书向导

7. 继续按“下一步”按钮，系统会要求用户选择指定服务器证书的来源方式，如果尚未安装过服务器证书，这时候用户必须选择“创建一个新证书”选项。若之前已获取过 Web 服务器证书，而且想要重新利用这些已有的证书，请选择“分配一个已存在的证书”、或者“从密钥管理器备份文件导入一个证书”选项，将原有的 Web 服务器证书安装到 IIS 系统上。

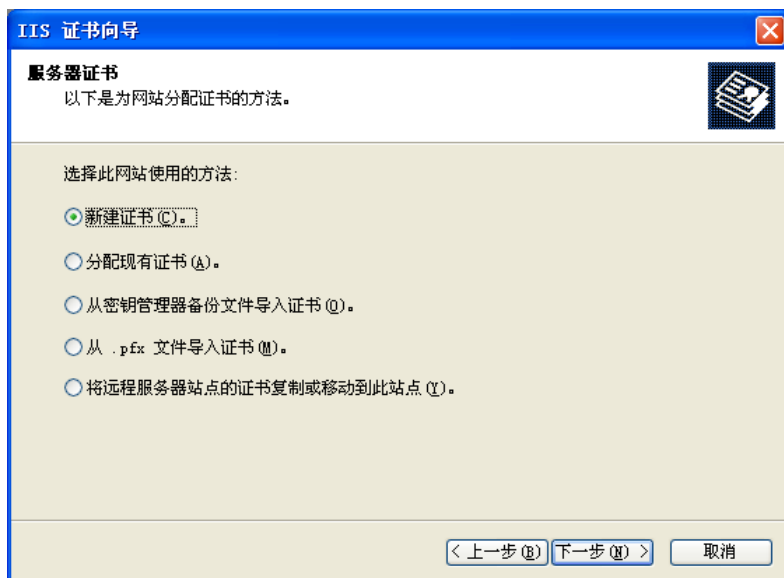


图 5-29 选择指定服务器证书的来源方式

如图 5-29 所示。以下的步骤假设用户选择“创建一个新证书”选项。

8. 设置好上一个设置步骤后，按“下一步”按钮。系统会要求您选择证书申请的时机，您可以按照您的需要来选择是否要先准备好证书要求，稍后再将此证书要求发送到证书颁发机构上，以获取适当的证书信息；或者立即将证书要求传递到您在稍后指定的证书颁发机构上，立即向证书颁发机构要求获取证书信息。

在这个步骤里，可以选择在线上直接连接证书颁发机构，直接获取证书信息（“立即发送一个请求到一个在线证书颁发机构”选项）；或是将证书要求储存成文件（选择“现在准备请求，但稍后发送”选项）再将此证书要求的文件发送到证书颁发机构上，以获取需要的证书。

9. 如果目前需要由企业外部商用性质的证书颁发机构获取所需要的证书，那么可能需要使用文件方式的证书要求方式，产生要求证书的文件（一般是提供给该部商用证书颁发机构处理身份验证过程使用的信息），并由该商用证书颁发机构确认核对后，再发行用

户证书，这时候，用户就可以获取需要的证书。一般来说，联机获取的证书颁发机构通常是本地的证书颁发机构，以及企业内部（域内）的证书颁发机构。

这里，我们选择“现在准备请求，但稍候发送”。

当设置好这一个设置步骤后，请继续按“下一步”按钮，进行下一个步骤的服务器证书安装设置过程。

10. 接下来，系统会出现“命名和安全设置”的设置窗口。系统会要求用户设置此证书的名称以及此证书安全设置项目。此时需要为请获取的服务器证书定义一个易于标识的证书名称，并设置此证书要使用的密钥长度。根据应用的需要，设置适当的密钥长度。并注意，若密钥长度设置太短，可能导致安全性的降低；若密钥长度设置太长，可能导致系统运算处理时间过长，导致系统效率不佳、或者软硬件系统无法配合等现象。一般来说大约 1024～2048 Bits 会是比较好的选择。
用户还可以设置是否要将此证书设置成为“服务器网关加密(SGC)证书”，此种类型的证书只是用于导出型的证书。如图 5-30 所示。

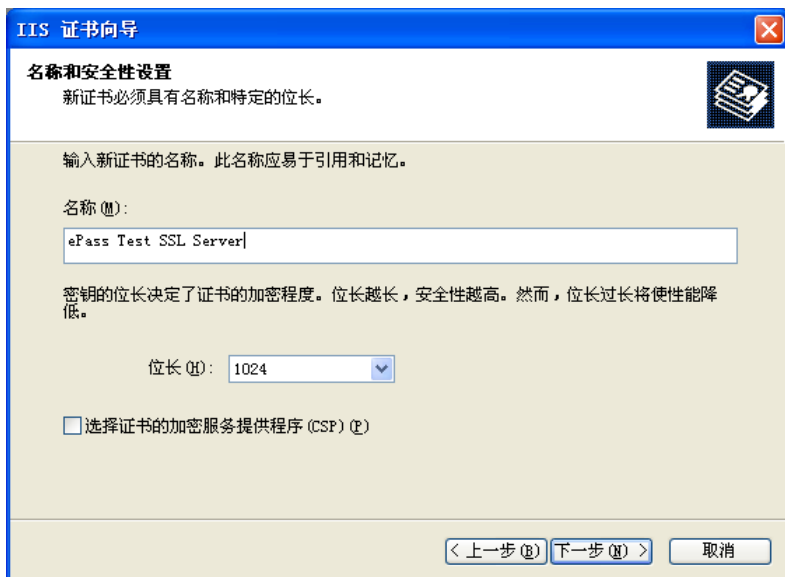
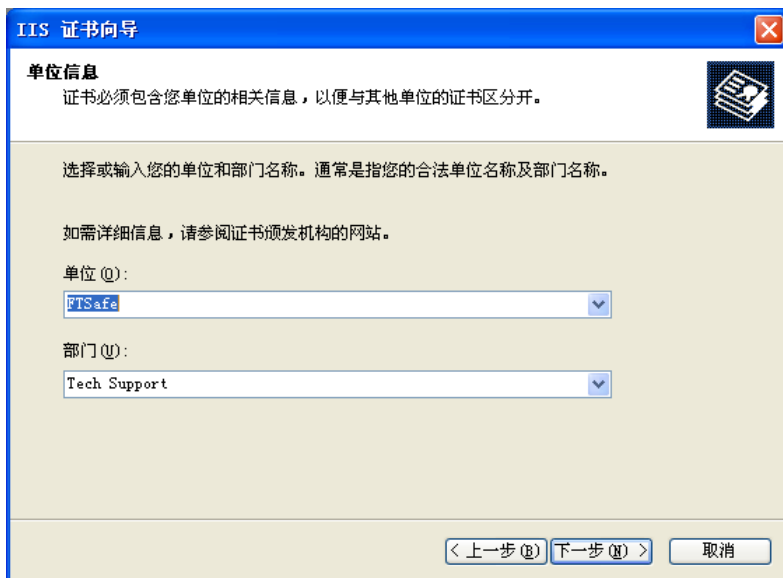


图 5-30 命名及安全设置

完成此设置步骤后，按“下一步”按钮，进行下一个步骤的服务器证书安装设置过程。

11. 接下来，用户需要输入企业组织的一些相关信息，以便让系统将企业以及目前所处的单位等相关信息记录在想颁发的用户证书内。如图 5-31 所示。输入完毕后，按“下一步”按钮。



The image shows a Windows dialog box titled "IIS 证书向导" (IIS Certificate Wizard). The current step is "单位信息" (Unit Information). The text inside says: "证书必须包含您单位的相关信息，以便与其他单位的证书区分开。" (The certificate must contain information about your organization to distinguish it from certificates of other organizations.) Below this, it says: "选择或输入您的单位和部门名称。通常是指您的合法单位名称及部门名称。" (Select or enter your organization and department names. Usually, these are your legal organization name and department name.) It then says: "如需详细信息，请参阅证书颁发机构的网站。" (For more information, see the website of the certificate authority.) There are two dropdown menus: "单位 (O):" (Organization) with "FTSafé" selected, and "部门 (OU):" (Department) with "Tech Support" selected. At the bottom, there are three buttons: "< 上一步 (B)" (Previous Step), "下一步 (N) >" (Next Step), and "取消" (Cancel).

图 5-31 组织信息设置

12. 命名安装服务器证书的国际互联网服务器的标识公用名称。输入这台服务器的 DNS 名称。若服务器在企业内部网络（Intranet），可以输入这台服务器的 NetBIOS 名称，如图 5-32 所示。

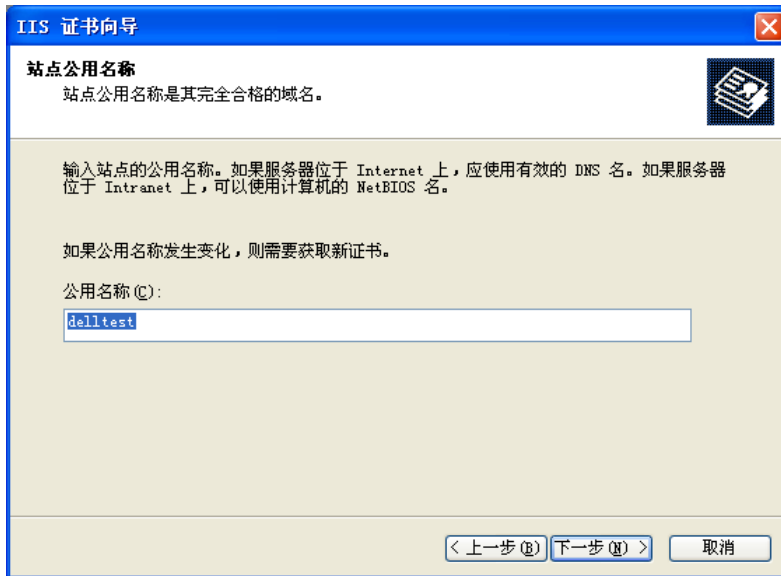


图 5-32 站点公用名称

设置好这一个设置步骤后，请按“下一步”按钮。

13. 填入目前此国际互联网服务器所在的地理位置信息，以便为证书信息提供更详细的数据。如图 5-33 所示。



图 5-33 地理信息

完成这一个设置步骤后，继续按“下一步”按钮。

14. 现在进行到设置证书请求文件名的步骤，在这里指定保存证书请求文件的文件名，如图 5-34 所示。

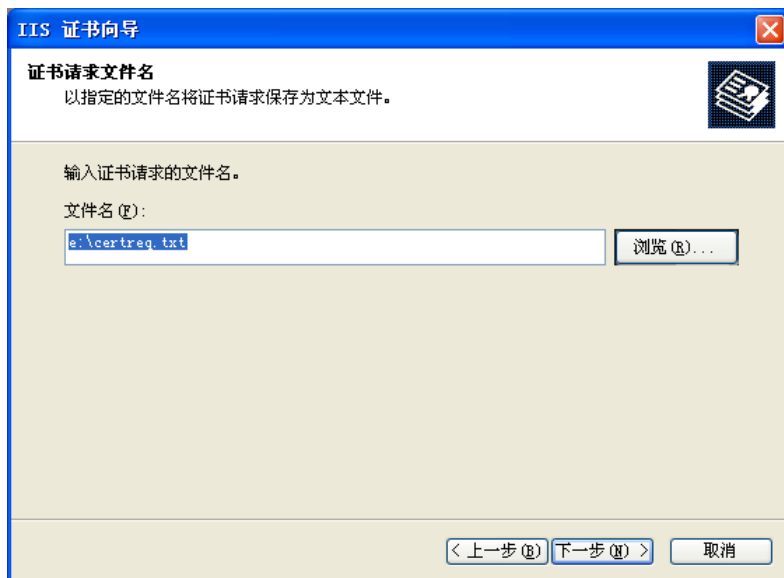


图 5-34 将证书请求存储成文件

15. 当设置完成后，系统会显示刚刚所设置的证书申请条件，如图 5-35 所示。用户可以检查看看是否有错误，若无错误，可以继续按“下一步”按钮。



图 5-35 请求文件摘要

16. 按“完成”按钮，这时计算机已经把证书请求文件存储下来了。现在，就可以去证书颁发机构去获取证书了。
17. 打开 IE 浏览器，连接证书服务器（这里以上面刚刚搭建的 CA 为例），进入证书颁发网页，勾选“申请证书”选项，如图 5-36 所示。并按“下一步”按钮，继续证书申请的下一个步骤。

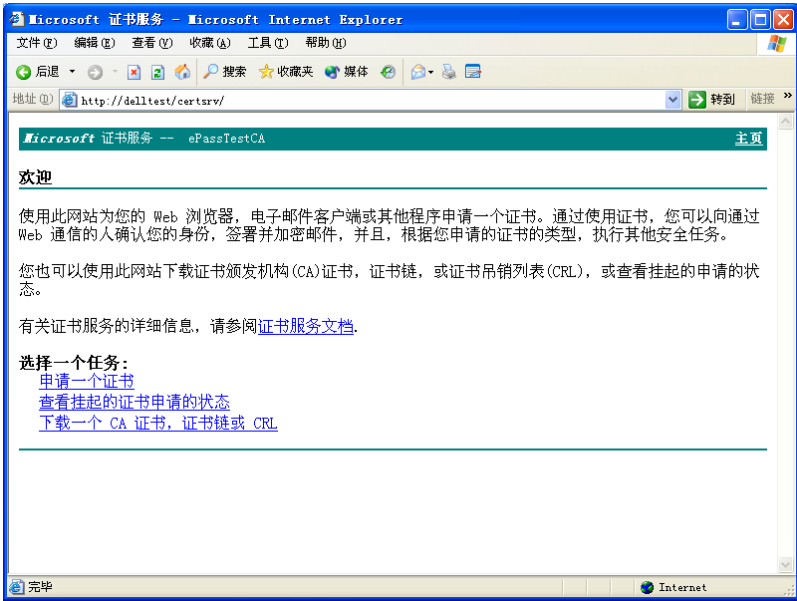


图 5-36 由 IE 获取证书

18. 接下来，进入选择证书申请类型页面，在这里我们勾选“高级申请”选项，然后按“下一步”按钮。

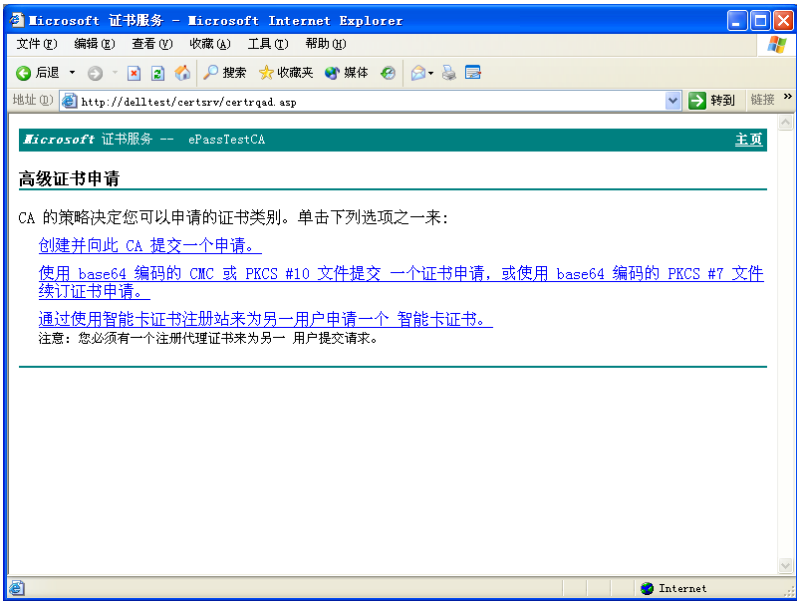


图 5-37 证书高级申请

19. 如图 5-37 所示，这里要选择文件形式的证书获取方式，即利用刚刚得到的证书请求文件来申请证书。按“下一步”按钮，继续证书的申请过程。
20. 进入如图 5-38 所示的界面，用户需要将存储起来的证书请求文件的内容拷贝到“存储的请求文件”一栏中。然后按“下一步”按钮。

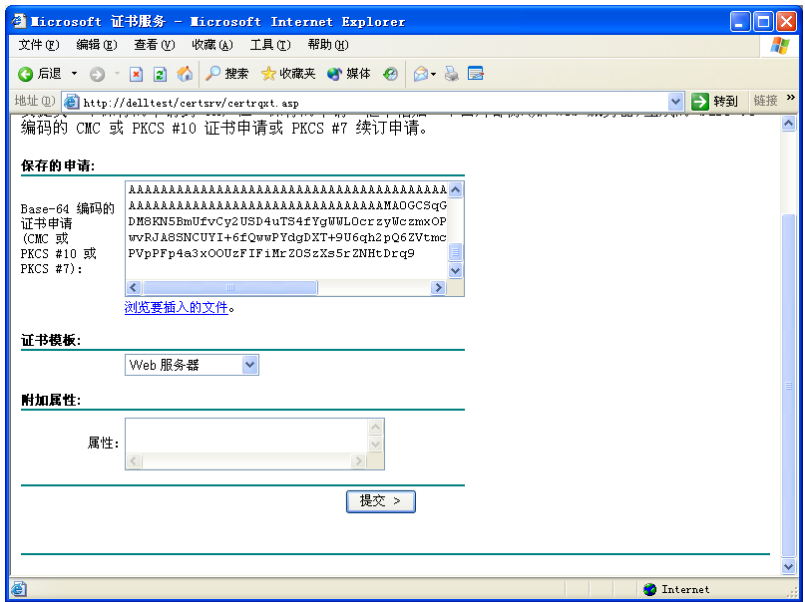


图 5-38 提供证书请求文件

21. 提交完证书请求文件后，会进入图 5-39 所示的页面中。这里可以看到，请求的证书被挂起，要等待颁发机构确认身份并发行证书后才能去领取。



图 5-39 证书挂起

22. 等待证书颁发机构确认身份并通知用户去领取证书后，用户就可以再次进入颁发机构去领取证书了。打开颁发证书页面，选择检查挂起的证书选项。如图 5-40 所示。

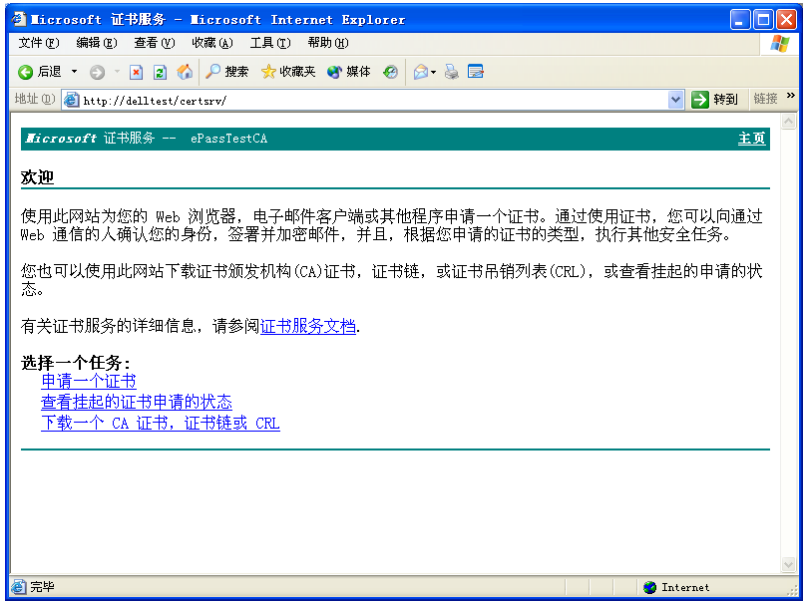


图 5-40 用 IE 获取被挂起的证书

23. 选中与申请日期一致的证书申请请求，按“下一步”按钮，去领取证书，如图 5-41 所示。

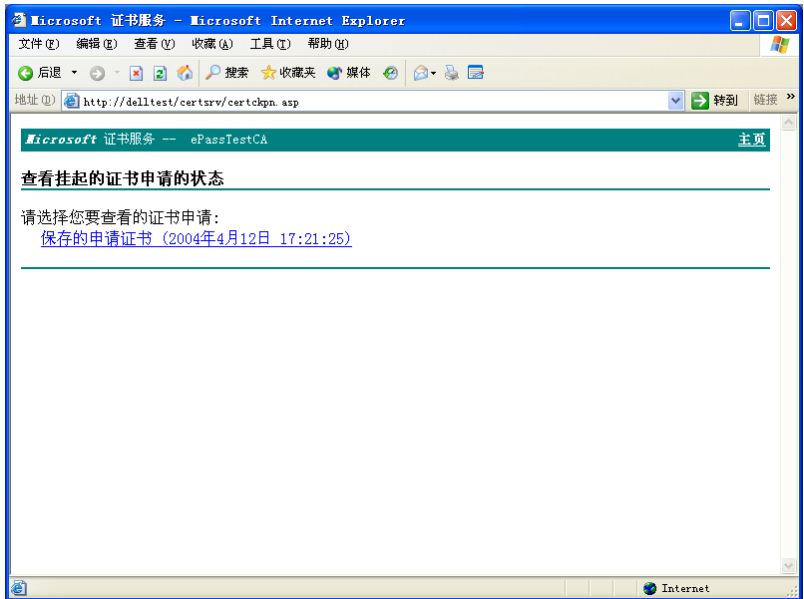


图 5-41 检查挂起的证书请求

24. 这时能看到，用户所申请的证书已经发行了，如图 5-42 所示。单击“下载 CA 证书”，就开始了证书下载过程。

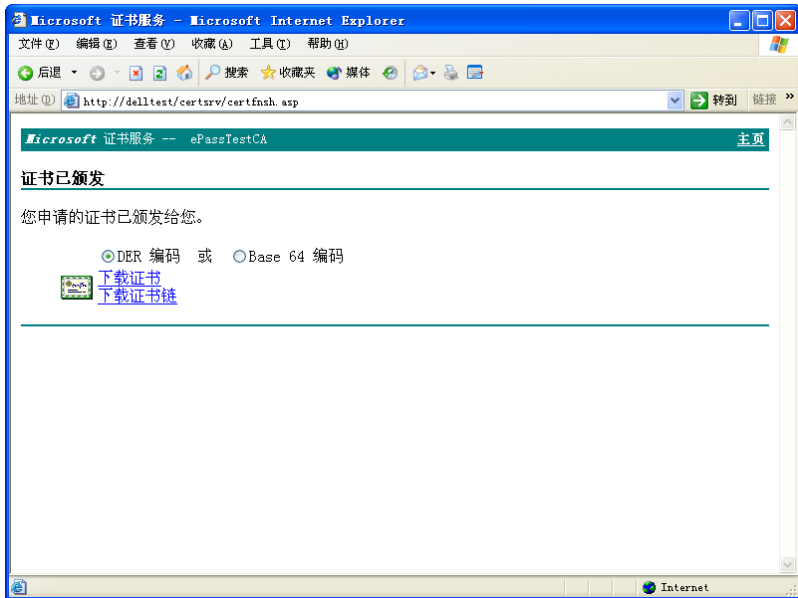


图 5-42 证书下载

25. 完成了证书下载，用户还必须启动证书安装向导来把证书安装在 WEB 服务器系统中。有关如何打开证书安装向导请参照第 8、9 步骤。完成证书导入如图 5-43 所示。

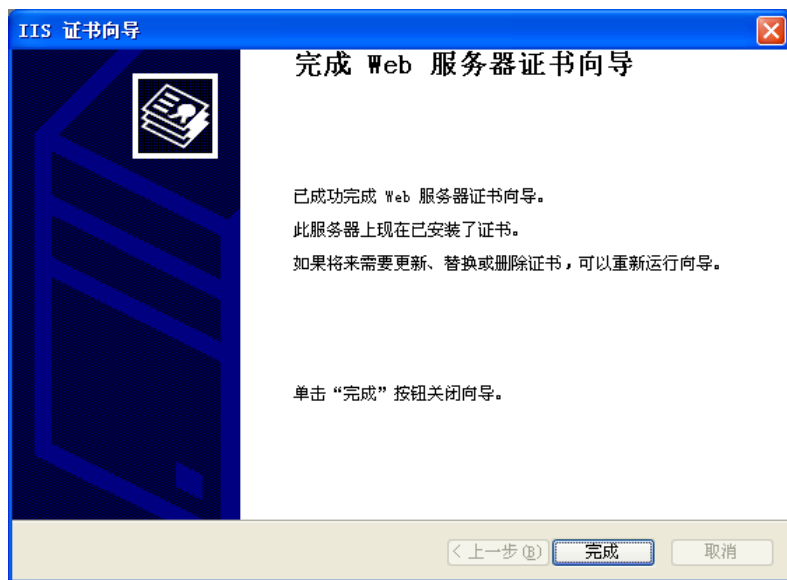


图 5-43 完成服务器证书导入工

如果采用直接连接上证书颁发机构的方式来获取证书，那么这时候向导会向用户所指定的证书颁发机构发出一个获取证书的要求信息，当该证书颁发机构身份验证通过时，就会发给用户一个证书，此证书会自动安装在用户的 WEB 服务器系统中。

在安装了服务器的证书后，接下来，用户就可以回到原来所打开的 WEB 站点属性设置窗口上，这时 SSL Port 变为可填写状态。用户要为该 WEB 站点填写一个安全通道端口（SSL Port），推荐填写默认值 443。如图 5-44 所示。

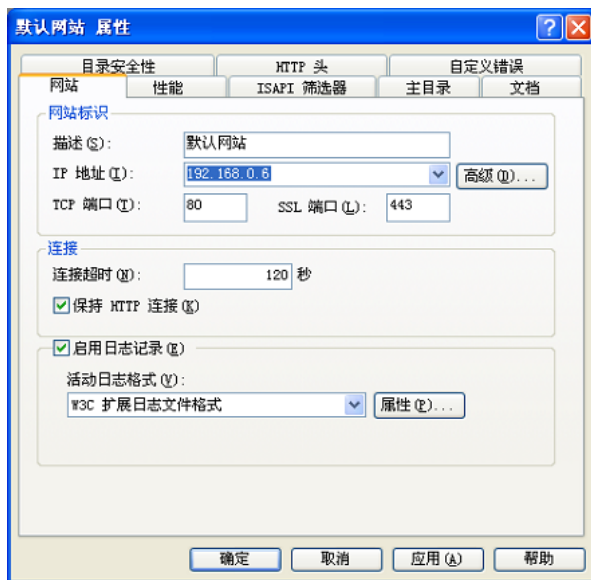


图 5-44 填写 SSL Port

现在展开“目录安全性”页面，用户可以看到在“安全通信”部分里的“查看证书”以及“编辑”按钮已经可以使用，表示这时候就可以开始配置 WEB 服务器的 SSL 设置了。如图 5-45 所示。



图 5-45 安装服务器证书后的服务器属性设置窗口

要设置此国际互联网服务器使用的安全性协议功能的操作时，按照下列的过程进行设置：

1. 回到该国际互联网服务器的属性设置窗口，并选择“目录安全性”页面，如图 5-45 所示的画面。
2. 这时候，按下在“安全通信”部分里的“编辑”按钮，来进行该国际互联网服务器的安全设置。当按下“编辑”按钮后，会出现安全通信编辑窗口。
3. 勾选位于窗口上方的“申请安全通道 (SSL)”的复选框。在客户证书中选择“申请客户证书”选项，如图 5-46 所示。以下是关于这些选项的说明。

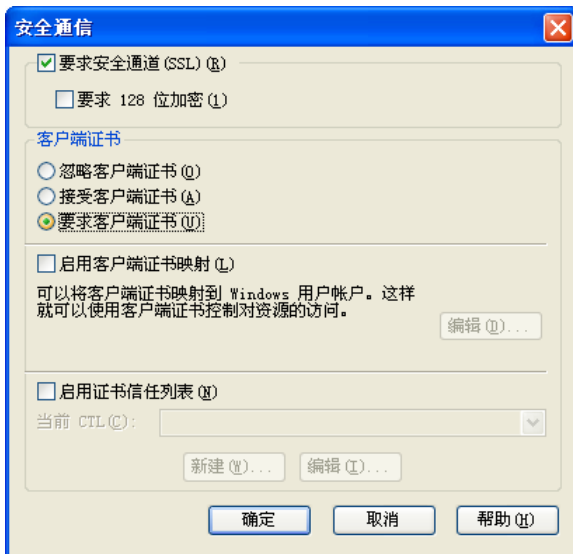


图 5-46 设置安全通信页面

- 申请安全通道 (SSL)：若没有启动此选项的话，Web 服务器默认都会以 HTTP 的通讯协议来提供 WWW 服务。启动了此选项后，WEB 服务器会要求客户端浏览器使用 SSL 的通讯协议进行访问。也就是当启用此选项后，系统就会关闭使用 http: 的连接，仅能使用 https: 连接来访问 WEB 服务器。
- 申请客户证书：用户必须提供一个证书才能够获得访问权限，这种方

式具有较高的安全。当设置完成后，单击“确定”按钮。

这时，已经完成了安全 Web 站点的设置工作，并已经启用了安全通道，如果再通过 http:连接来连接该 Web 站点，会出现如下图所示的情况：

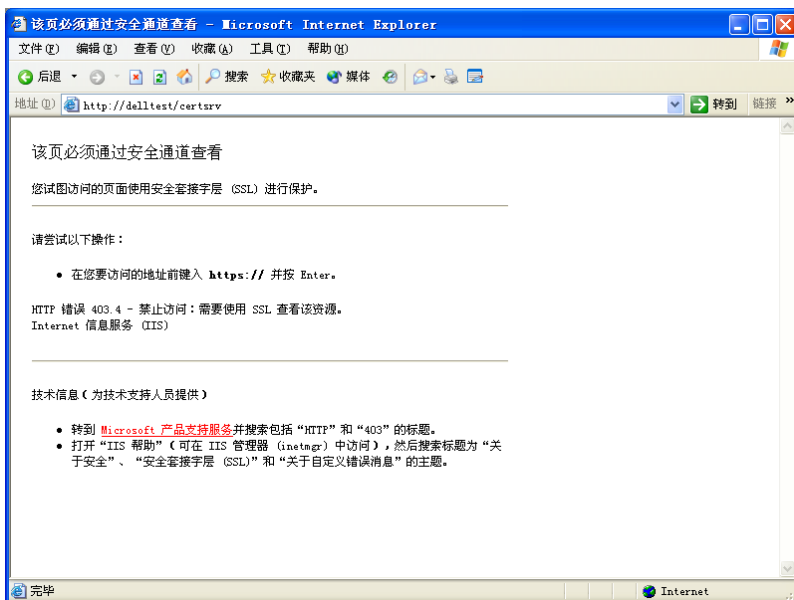


图 5-47 用 http:访问安全站点

系统提示必须要通过 https:连接来连接上要访问的站点。用户再通过 https:连接来连接上刚刚设置的安全 Web 站点。会看到系统有如下图所示的安全提示。

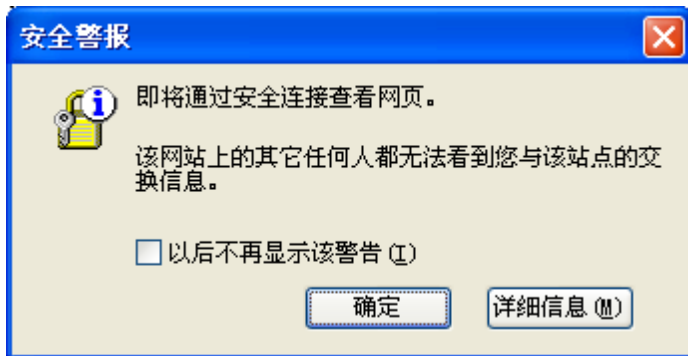


图 5-48 安全提示信息

单击“确定”按钮后，会有客户认证提示，要求选择用户要使用的证书。此时用户还没有申请客户认证证书，所以证书列表框为空。

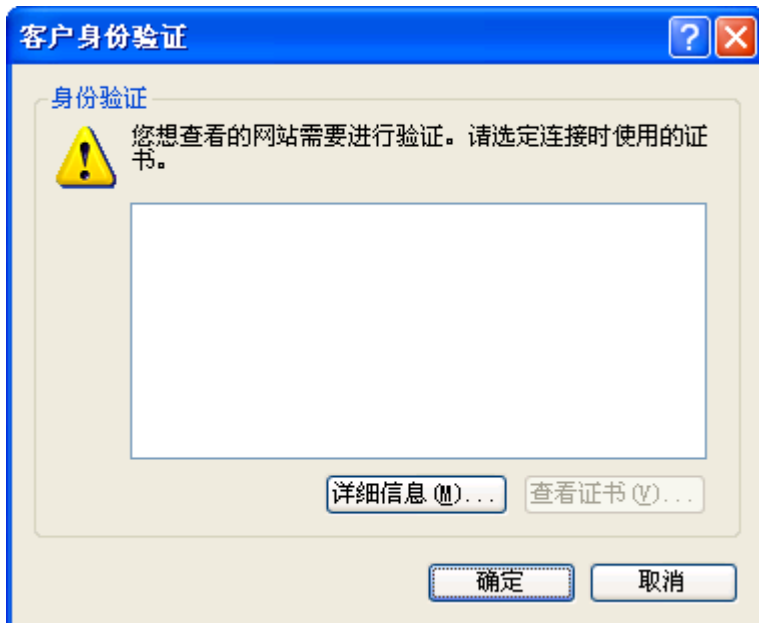


图 5-49 客户证书选择

下面，我们就介绍如何利用 ePass1000 进行客户证书的申请。

5.5.4 使用 ePass1000 申请数字证书

确认插入了一支已经完成 PKI 应用初始化的 ePass1000，然后通过 IE 浏览器打开证书颁发机构的网页，选择申请证书。这里我们用 Verisign 公司的测试证书服务器为例。如图 5-49 所示：

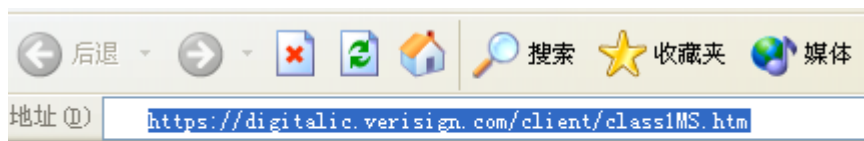


图 5-49 Verisign 测试网址

请按照提示信息完成证书申请过程中基本信息的填写。在“CSP”（加

密服务提供程序) 选项中选择“FTsafe ePass1000 RSA Cryptographic Service Provider”，如图 5-50 所示：



图 5-50 选择 CSP

选择了“FTsafe ePass1000 RSA Cryptographic Service Provider”意味着证书所使用的密钥对是由 ePass1000 生成，确保了密钥的安全，为此，ePass1000 的合法用户必须登入 ePass1000，如下图 5-51 所示：



图 5-51 校验 PIN 码

当合法的 ePass1000 持有者正确登入后，申请操作继续。至于证书申请过程的后继操作，请参考具体的证书申请网页上的提示。

当申请工作结束之后，您可以通过 ePass1000 的管理工具来查看证书，具体操作请参考“第四章 ePass1000 管理器使用说明”中相关内容。

5.5.5 使用 ePass1000 访问 SSL 加密站点

假设 SSL 加密站点已经配置好，这里介绍如何使用 ePass1000 去访问此 SSL 加密站点。

利用 ePass1000 申请一个“Web 浏览器证书”或者具有相当功能的数字证书。在申请这些证书时所采用的 CSP 类型亦为“FTsafe ePass1000 RSA Cryptographic Service Provider”，此过程类似于“使用 ePass1000 申请数字证书”中所描述的。

若客户端拿到了“Web 浏览器证书”数字证书，即证书已经妥善保存到了 ePass1000 里，客户端就可以去访问 SSL 加密站点了。

5.5.6 使用 ePass1000 收发签名与加密邮件

在开始设置 Outlook Express 中收发签名与加密邮件之前，假设已经将 Outlook Express 设置好，可以连接上电子邮件服务器以及电子邮件帐号的相关设置，换句话说，用户已经可以使用 Outlook Express 以一般的方式发送/接收电子邮件。要设置 Outlook Express 的安全设置，必须先获取具有电子邮件安全处理能力的证书（在 Outlook Express 里称为“数字 ID”），当获取用户的数字标识后，用户才可以发送具有数字签名或者信息加密的电子邮件。

我们先进行获取数字标识的操作过程，来获取数字标识。由于电子邮件的应用是属于公开性的，因此，用户必须通过专门负责提供证书服务的企业，来获取适当的证书信息，以确保该证书的有效性。为此，我们所要采用的数字证书必须为“电子邮件安全证书”。

申请电子邮件安全证书的方式可以参考“使用 ePass1000 申请数字证书”的内容，要注意的二点是：第一、要将该选择证书类型为“电子邮件安全证书”；第二、在填写证书信息中的电子邮件地址时一定要是 Outlook Express 中您所将要用来收发安全邮件的那个帐号。如果已经拥有了一个电子邮件安全证书（此证书必须包含有私钥），并且保证此证书是有效的，也可以通过 ePass1000 的管理工具来导入这个证书；

在获取了电子邮件安全证书之后，我们就要对 Outlook Express 内的帐号进行设置。

启动 Outlook Express，在其菜单中选择“工具”选项→“帐号”选项，如图 5-52 所示：

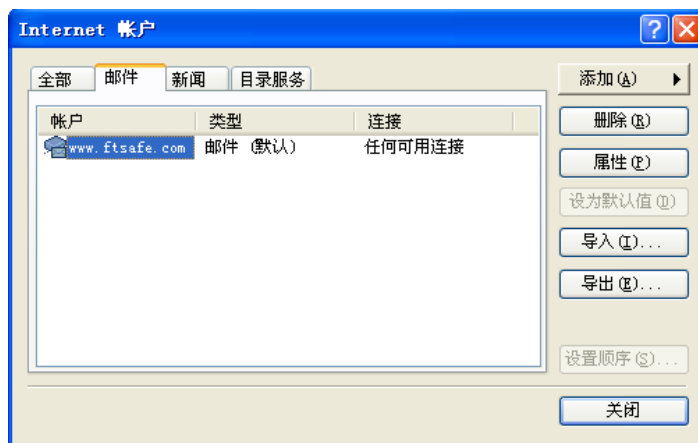


图 5-52 设置邮件帐号

当打开“Internet 帐户”窗口后，请点选“邮件”页面。我们假设用户已经设置好电子邮件信箱了，请选择想设置的电子邮件帐号，接着，请按旁边的“属性”按钮；打开此电子邮件帐号的属性设置窗口后，先选择“常规”页面，检查目前的“电子邮件地址”是否有设置错误，如图 5-53 所示：



图 5-53 设置邮件帐号

选择“安全”页面，以显示关于此电子邮件帐号的安全性相关设置，若让此 Email 帐号能够具有数字签名的能力，在“签署证书”的部分里，按下“选择”按钮，并选择一个刚刚获取的证书（数字 ID）。若要让此 Email 帐号能够具有电子邮件加密的能力，在“加密首选项”的部分里，按下“选择”按钮，并选择一个刚刚获取的证书（数字 ID），以便让 Email 帐号具有处理电子邮件加密的功能，用户还可以选择想使用算法规则，如图 5-54 所示：

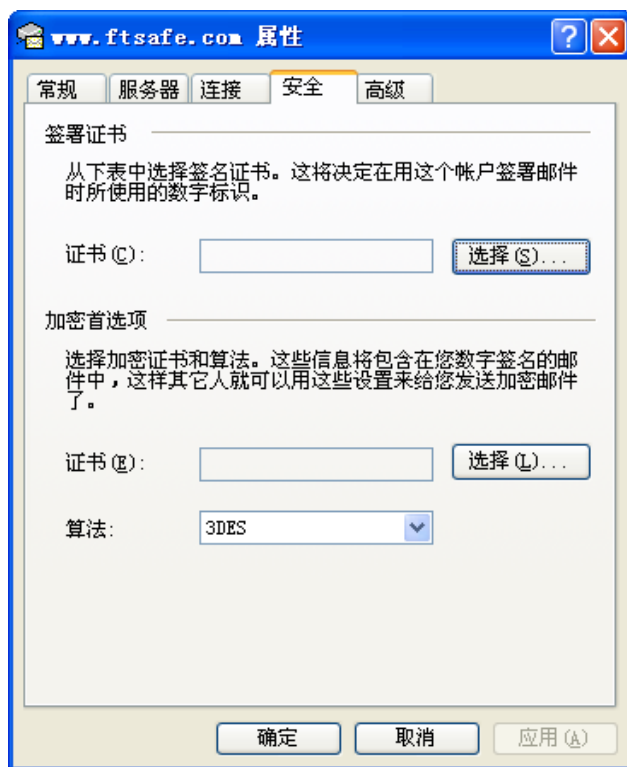


图 5-54 安全属性

当按下此按钮后，用户会看到下列的画面。Outlook Express 将只会使用用户信箱里所设置的证书来辨识 S/MIME 信件。此证书是记录在 Email 信箱的证书的主题字段里的证书。这些证书都会显示在图 5-55 所示的选择窗口里，选择一个要使用的证书。

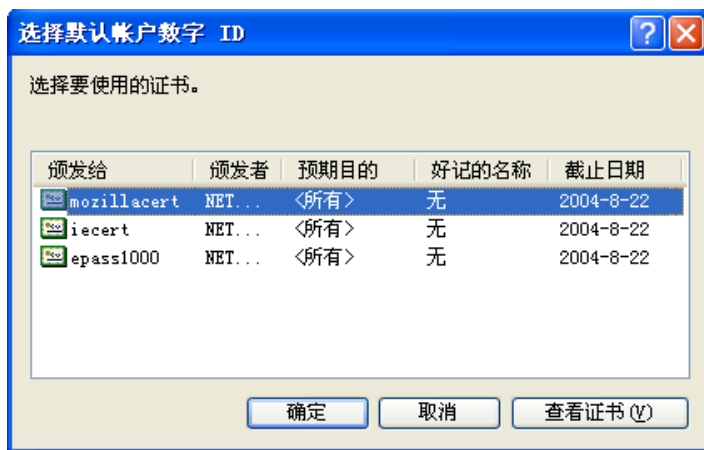


图 5-55 选择证书

这里要注意的是，如果系统连接了 ePass1000，那么 ePass1000 内的证书会被枚举出来，所以也可以选择此证书。

按“确定”完成设置，回到 Outlook Express 的主要界面。

由下拉式菜单的“工具”选项里，选择“选项”设置。点选“安全”设置页面。这时候会显示关于安全设置的一些设置项目，如图 5-56 所示：

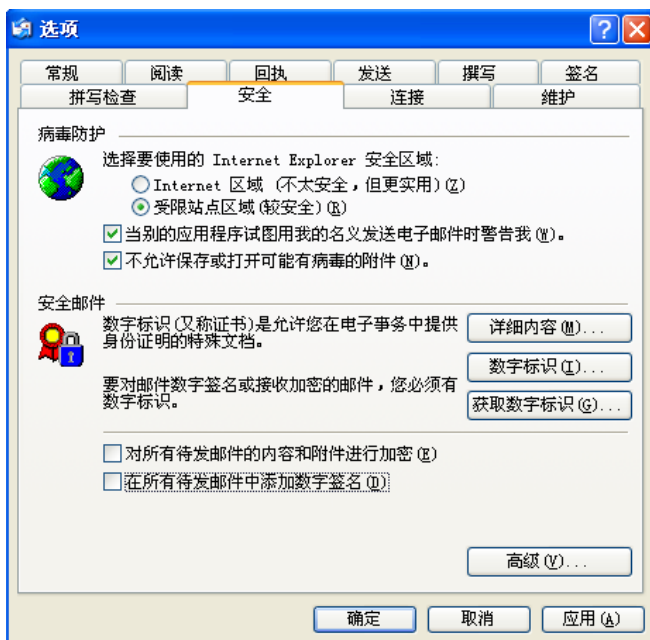


图 5-56 安全邮件设置

如果想要让送出去的每一份电子邮件上都附加上数字签名，勾选“对所有待发邮件中添加数字签名”选项，也可以用稍后所说明的方法，为特定的电子邮件加上数字签名。

如果要将所发送出去的每一份电子邮件的属性都加密，请勾选“对所有待发邮件的内容和附件进行加密”的选项，也可以用稍后所说明的方式，为特定的电子邮件加密。

按下方的“高级”按钮，这时候会启动“高级安全设置”对话框，如图 5-57 所示。

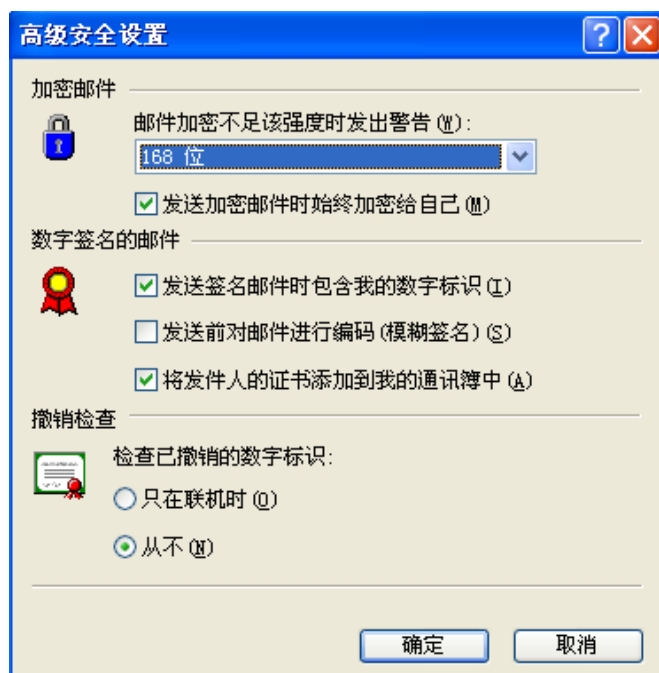


图 5-57 高级安全设置

确定已经勾选了“发送加密邮件时始终加密给自己”的复选框选项（位于加密邮件部分下的选项）。

确定也勾选了位于“数字签名的邮件”框下方的“发送签名邮件时包含我的数字标识”以及“将发件人的证书添加到我的通讯簿中”的选项。因为当发送加密型电子邮件时，或别人发送加密型电子邮件时，接受端的

人都必须获取对方的密钥（存储在数字标识中）才可以读取到原始的信件内容，勾选此选项是确保能够正确获取对方解密所使用的密钥信息。

另外，用户也可以根据需要，调整其它的设置，诸如密钥的长度的限制。到此时用户已经完成了 Outlook Express 的设置。当发送电子邮件信息时，邮件会自动进行加密，并加上数字签名信息。

当设置好 Outlook Express 里的安全设置选项后，用户就可以开始发送具有安全性质的电子邮件。因为，Windows 2000 操作系统上的证书服务采用公钥的基础技术来建立的，因此，所有架构在 Windows 2000 公钥基础的许多应用程序都具有上述的安全性应用功能。在 Windows 2000 操作系统内建提供的 Outlook Express 也提供了数字签名以及电子邮件加密的基本功能。

获取收件人的公钥和证书

若要发送属性加密的电子邮件，用户必须先获取对方的公钥或者证书，再利用对方的公钥对用户信件进行加密处理（也就是使用收件人的公钥来进行加密），这时候，只有此公钥映射的私钥（假设此私钥只有收件人持有）才能够对此加密过的信件进行解密的处理，因此，只有持有该私钥的人，才能够阅读信件属性（加密邮件）、或确认该信件的确实性（数字签名）。

要获取对方的公钥或者证书的话，必须要求电子邮件的收件人发送一封带有数字签名的信件给用户，并将带有数字签名信息的邮件中，将其内的证书（数字 ID）存储下来，这时候用户就可以保有对方的证书以及公钥的信息。

若要存储证书或公钥，请按照下列的步骤进行操作：

1. 先要求发送者发送一份带有数字签名的电子邮件给接收者。
2. 接收者启动 Outlook Express，接收发送者发送的电子邮件（带有数字签名的邮件），并打开该签名邮件。
3. 在送件人的“发件人”字段上，按下鼠标右键，并选择“添加到通讯簿”选项，按下“确定”按钮，将收件人以及其证书存储到 Outlook Express 的通讯簿列表里（参见图 5-58）。这时候就完成了存储对方公钥与证书的操作过程。

使用 Outlook Express 发送属性加密的邮件

要发送加密的邮件，先必须确定接收者已经得到发送者的证书（证书

包含了公钥信息)。

要发送一封加密过的邮件，按照下列的步骤进行操作：

1. 按下 Outlook Express 上方的“新邮件”按钮，开始编辑新的邮件信息。
2. 接着，在“收件者”的字段上，选择该加密邮件的收件者。注意，若 Outlook Express 通讯簿清单里的收件者有附带数字标识(证书)信息时，其通讯簿的清单上图标会有一个标志(红色的证书标志)，您必须选择夹带有证书信息的收件者。如图 5-58 所示。



图 5-58 选择收件人

3. 接着，填写电子邮件的主题等相关字段的信息，并填写好该邮件的内容。
4. 按下“加密”按钮，要求将此邮件信息加密过，加密信息按钮图标如图 5-59 所示。

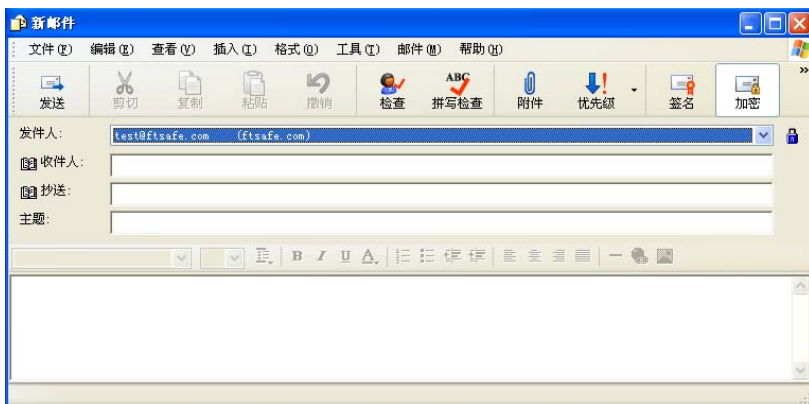


图 5-59 加密邮件

5. 按“发送”按钮，将邮件发送出去。

5.5.7 使用 ePass1000 进行 Win2000 智能卡登录

Windows 2000 及更高版本的 Windows 操作系统都内置了对智能卡用户认证的支持，计算机用户可以选择使用传统的用户名、口令验证方式进行域用户身份验证，也可以使用智能卡来自动完成用户身份验证。智能卡用户身份验证的优势是更加安全和易于使用。用户只需记住智能卡的用户 PIN 码就可利用智能卡自动进行安全身份认证。

要在 Windows2000 的工作站上进行智能卡用户登录，用户必须拥有一份含有智能卡登陆证书的智能卡。

这里不讲述如何设置为用户颁发智能卡证书，请参阅微软的相关文档。

下面说明一下如何用 ePass1000 来申请智能卡登录证书。

假设现在有一个可以申请智能卡数字证书的网站，在填写完基本的用户信息之后，要注意的事项有：

1. 选择证书模板为“智能卡用户”。
2. 在“加密服务提供程序”中选择“FTSafe ePass1000 RSA Cryptographic Service Provider”。
3. 在“管理员签名证书”中选择我们先前申请的注册代理证书。
4. 在“输入用户名”中，选择适当的域用户。然后单击“提交”按钮。

5. 在接下来弹出的验证用户 PIN 码对话框中输入正确的 ePass1000 用户 PIN 码，然后等待证书生成。

不同的智能卡注册站可能有一些不同的注册过程，请您参考具体情况而定，在此仅作为一个例子来说明。申请智能卡登录证书与申请普通的数字证书过程基本相同。

用户智能卡登录证书申请完成之后，就可以进行使用智能卡进行域用户登录了。

5.5.8 使用 ePass1000 进行 VPN 远程登录

VPN 就是虚拟专用网，可以用来在不安全的网络环境上建立一条安全的网络信道，就好像专用信道一样安全。Windows2000 操作系统内置了对 VPN 应用的支持。Windows 用户可以像使用拨号网络登录到 ISP 的服务器上一样，通过 VPN 连接到需要进行安全传输的网络接入服务器。

在建立 VPN 安全信道的时候，服务器和客户机需要相互进行认证操作，以此建立起安全会话密钥，并用会话密钥完成后续的信息加密操作。Windows Server 2003 允许用户在客户端使用智能卡进行登录用户身份验证。下面我们以 Windows Server 2003 的 VPN 路由软件为例讲述 VPN 服务器的配置。

1. 首先打开控制面板里面的“管理工具”工具夹，双击“路由与远程控制”图标，弹出控制台窗口。
2. 用鼠标右键单击左边树型结构的服务器名，从弹出菜单中选择“配置路由服务器”，弹出对话框如图 5-60 所示。

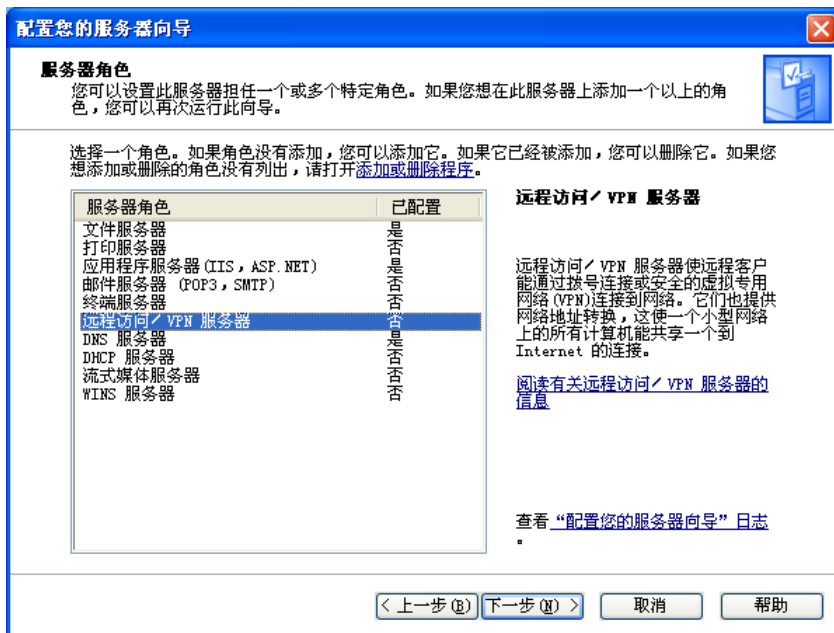


图 5-60 配置服务器

3. 单击下一步，并选择进行 VPN 服务的配置，如图 5-61 所示。

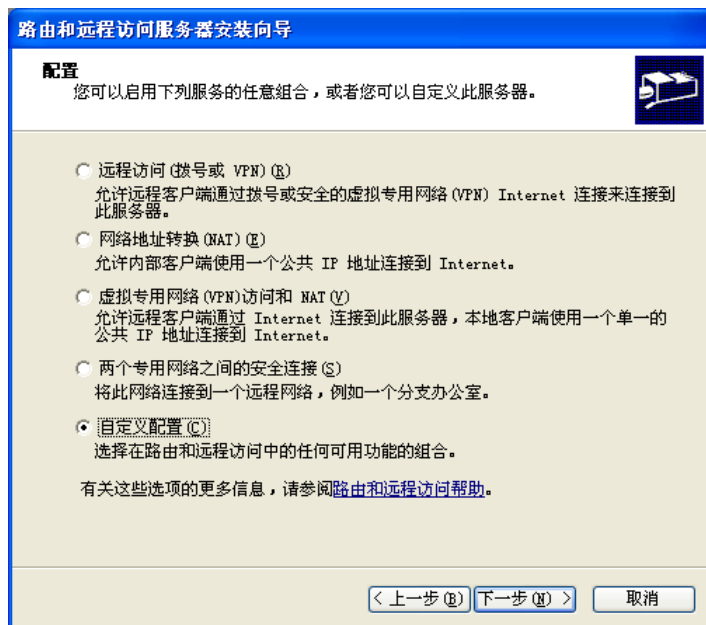


图 5-61 远程访问设置

4. 单击“下一步”，选择支持的协议类型。
5. 单击“下一步”，选择网络连接接口。
6. 单击“下一步”，选择 VPN 登录客户端 IP 地址分配策略。可使用现有的 DHCP 服务器进行自动分配，也可以指定固定的 IP 地址范围作为分配地址池。
7. 单击“下一步”，可以为 VPN 配置验证服务器 RADIUS，可以先不配置。

完成上述步骤之后，VPN 接入服务器就安装完成了。接下来，我们需要为 VPN 服务器配置登录验证的方式，我们需要使用智能卡登录方式。

8. 在“路由和远程访问”控制台左边的树型结构中鼠标右键单击服务器名，并选择“属性”。
9. 在弹出的服务器属性对话框中选择“安全”属性页，并单击“验证”按钮。显示结果如图 5-62 所示：

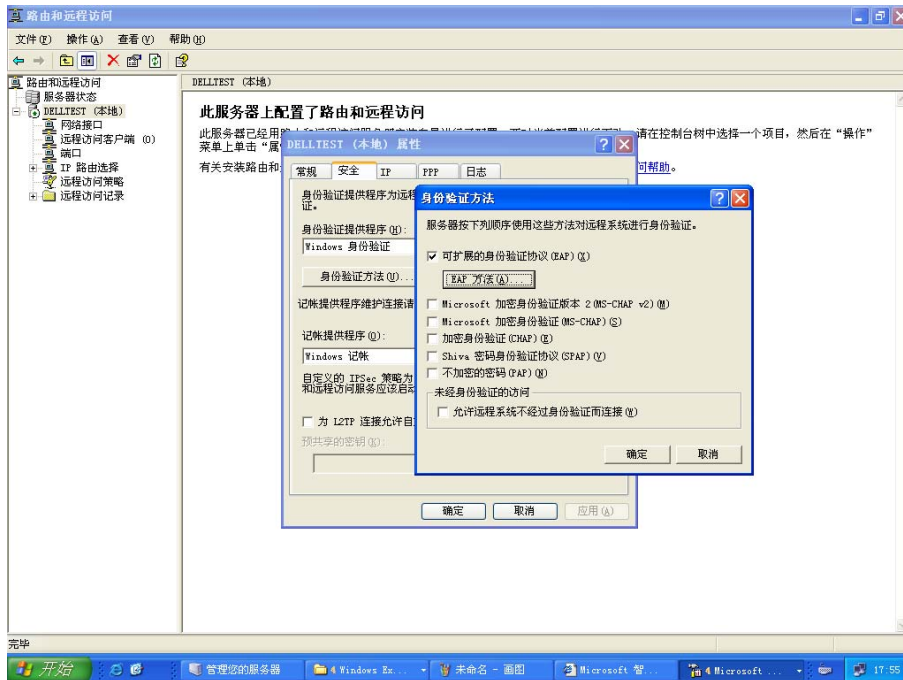


图 5-62 选择身份验证方式

10. 选择扩展验证协议(EAP)。扩展验证协议是对传统用户名、口令验证的改进,智能卡用户验证属于扩展验证协议。
11. 关闭“验证方式”对话框。
12. 关闭“服务器属性”对话框。
13. 在“路由与远程访问”控制台窗口左边的树型结构中选择“远程访问策略”。
14. 双击窗口中列出配置项。
15. 在弹出的对话框中单击“编辑配置文件”按钮。
16. 在“编辑拨入配置文件”对话框中,单击“身份验证”属性页。

如图 5-63:

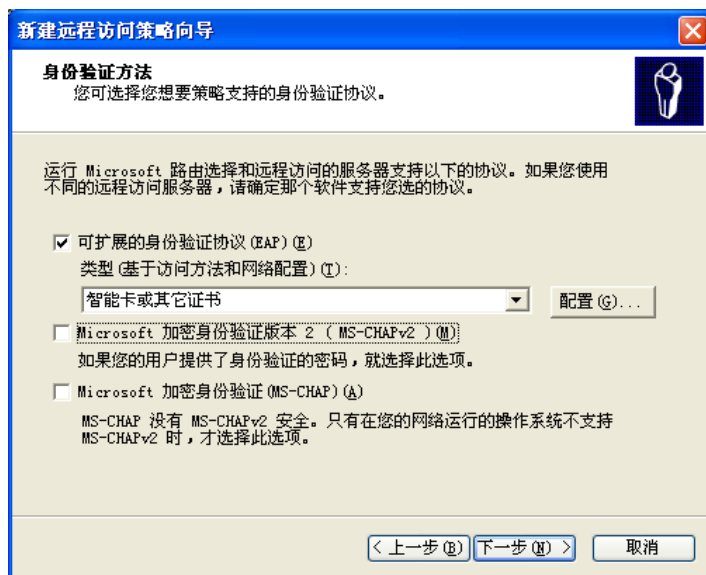


图 5-63 智能卡验证

17. 选择扩展验证协议。然后单击“确定”按钮完成配置。至此,VPN 接入服务器的配置就完成了。
- 接下来,我们进行客户端软件的配置。
- (1) 打开控制面板中的“拨号网络”工具夹。
 - (2) 双击“建立新的链接”图标,弹出“网络连接向导”对话框如图 5-64 所示:

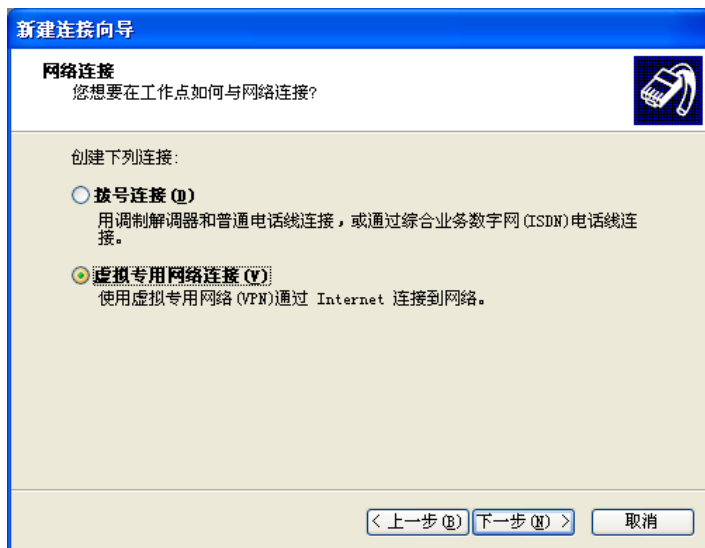


图 5-64 设置网络连接类型

- (3) 选择“通过 Internet 连接到虚拟专用网，并单击“下一步”。
- (4) 接下来填入要连接的 VPN 服务器的 IP 地址或域名。
- (5) 选择“使用我的智能卡”。

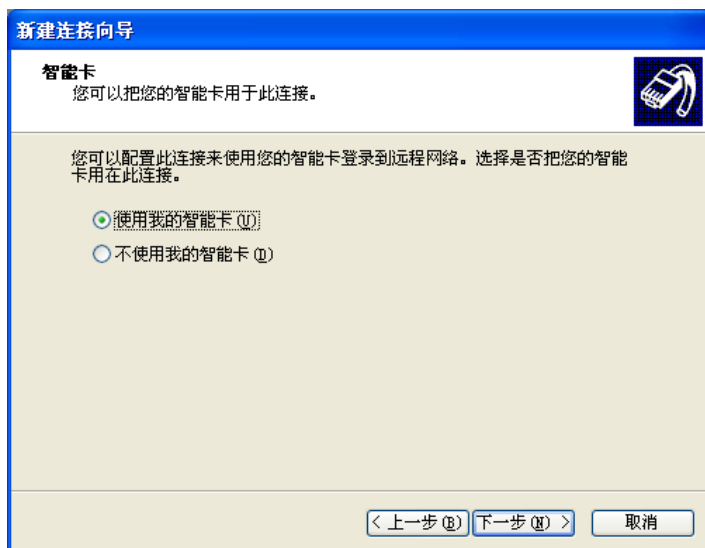


图 5-65 选择智能卡登录

(6) 最后，输入新建的 VPN 连接的名称。

支持 VPN 客户端软件的配置就完成了。

最后一步是利用 ePass1000 申请一个证书，申请过程与前面所述的证书申请过程是类似的。

要进行 VPN 登录，插入 ePass1000，双击新建立的 VPN 拨号图标，按提示输入 ePass1000 的用户 PIN 码就可以进行 VPN 连接访问了。

5.6 其它应用

在此，主要是说明 ePass1000 的其它应用开发，即可以运用 ePass1000 来完成一些非 PKI 应用的开发程序。

ePass1000 提供了 C 语言接口函数。使用此接口可以完成另外的某些应用。同样地，利用此私有接口也完全可以使数据达到较高的安全性。

关于 ePass1000 C 语言接口函数的更多资料，请参考 ePass1000 SDK 的 ePass1000 开发人员参考手册。

第六章 发布 ePass1000 应用程序

在应用程序能够访问 ePass1000 之前，必须正确安装 ePass1000 的驱动程序和其他库文件。有两种安装 ePass1000 运行库的方法：

- ✓ 使用 ePass1000 SDK 中的提供的可分发组件包安装
- ✓ 使用 ePass1000 SDK 中提供的编程接口编写自己的安装程序

要使用 ePass1000 的安装编程接口，需要下列文件：

Files	SDK Paths
epsSetupApi.h	/Include
ePsIns_drv.lib	/Lib
ePsInst_drv.dll	/Lib (运行时必须存在)
ePsInst_Mw.lib	/Lib
ePsInst_Mw.dll	/Lib(运行时必须存在)

调用 `esa_DoInstall` 函数来安装 ePass1000 驱动。用 `esa_DoUnInstall` 函数来卸载。ePass1000 的安装接口库不会自动重新启动计算机。应用程序可通过 `esa_IsNeedReboot` 来判断是否需要重新启动系统。如果应用程序需要使用进度条来显示当前的安装进度，则可使用 `esa_SetShowMsgNotifyCallBack()`来安装一个回调函数更新用户界面的刷新。

有的时候反安装程序可能需要删除一个正在被程序使用的文件。ePass1000 安装接口提供 `esa_SetDeleteFileCallback` 函数允许应用程序提供一个回调函数来处理这种情况。

要获取有关 ePass1000 安装接口更多的信息，请参阅 ePass1000 API 在线文档和 SDK 中包含的安装示例。

附录一 常见问题

1. 插入 **ePass1000** 时，系统没有提示找到新硬件，并且 **ePass1000** 不可使用。

首先检查操作系统是否支持 **ePass1000**（WIN 98SE/ME/2000/2003/XP；MAC OS 8/9/10x；Linux）。然后检查系统 BIOS，查看与 USB 端口的选项是否被激活，如果 USB 选项被禁止，激活它然后重新插入 **ePass1000**。

如果系统还是没有正常工作，那么问题可能出在 USB 端口或者连接线上。试着连接另外的 USB 设备（例如 USB 鼠标或 USB 键盘）到 USB 端口上。如果其他的 USB 设备能够正常工作，那么可能是 **ePass1000** 发生故障，如果其他 USB 也无法正常工作，那么可能是 USB 端口有问题。

2. **ePass1000** 已经正常安装，但是无法登录到 **ePass1000** 保护的站点？

请检查浏览器的安全设置。确定允许 ActiveX 控件和插件运行。

3. **ePass1000** 可以被一个程序正常打开，但是第二个程序试图打开时却无法找到 **ePass1000**？

因为安全因素，**ePass1000** 在同一时间内只能由一个应用程序打开。只有第一个应用程序正常关闭了 **ePass1000**，第二个应用程序才可以打开它。

4. 为什么将 **ePass1000** 插入到一个 USB 集线器上会导致 **ePass1000** 工作不正常？

我们发现一些内置电源的 USB 集线器会对 **ePass1000** 造成电器干扰。如果一定要使用集线器，请选择外置电源的类型。

5. 我的计算机有 USB 接口吗？

一般来说，所有的 PII 计算机和一些旧的计算机都具备 USB 接口。

如果您的计算机上没有 USB 端口,您可以在主板的 PCI 槽中插入 USB 扩展卡。请注意,如果您的主板支持 USB 功能,您必须在 BIOS 中屏蔽它。

附录 二 ePass1000 技术及规格表

操作系统	Windows 98SE/ME/2000/ XP /2003, Mac OS 8/9/10.X, Linux
证书及标准	PKCS#11, MS CAPI, PC/SC, X.509 v3 证书存储, SSL, IPSec/IKE
内存容量	8K、32K
硬件算法	MD5
芯片安全级别	安全加密数据存储
功率	< 250 mW
工作温度	0℃至 70℃
存放温度	-40℃至 85℃
湿度	0 至 100%，不结露
接口类型	USB A 型 (通用串行主线)
封装	硬塑料防篡改
数据保存年限	至少 10 年
内存写次数	至少 10 万次