ePass3000 的 Microsoft VPN 应用

1.1 版

北京飞天诚信科技有限公司（以下简称“飞天公司”）尽最大努力使这篇文档中的内容完善且正确。飞天公司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。这篇文档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
2007 年 11 月 23 日	1.0	第一版
2009 年 6 月 2 日	1.1	第一版第一次修订

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、ePass 系列硬件和产品的其它部分。禁止对软件和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，ePass 系列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，或发生故障 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。

CE 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.

FCC certificate of approval

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

USB

This equipment is USB based.

WEEE

Dispose in separate collection.

目　录

ePass3000 的Microsoft VPN应用

ePass3000 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 ePass3000 进行任何形式的编程开发就能通过配置相关服务而开始将 ePass3000 集成于 PKI 应用当中。

目前支持 PKI 的应用有些使用 PKCS#11 接口，有些使用 Crypto API（简称 CAPI）接口，后者都是微软的 Windows 平台下的应用，而前者在任何平台下都有。

本文档讲述如何使用 ePass3000 进行 VPN 连接。

1.1 什么是VPN

VPN（Virtual Private Network，虚拟专用网），可以通过特殊的加密通讯协议在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯信道，就好比是架设了一条专线一样，但是它并不需要真正的去铺设光缆等物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。VPN 的核心就是利用公共网络建立虚拟私有网。Windows Server 2003 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 工作站允许用户在客户端在登录时使用智能卡进行用户身份验证。本文当我们以 Windows Server 2003 的 VPN 路由软件为例讲述 VPN 服务器的配置。下图显示了一个典型的 VPN 架构：

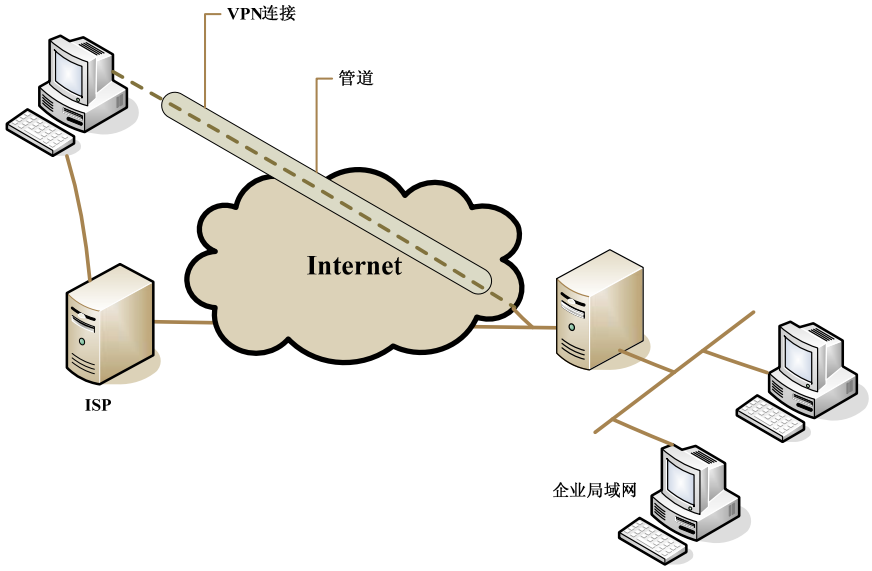

图 1VPN 架构

1.2 在Windows2003 服务器上进行VPN服务端设置

本章讲述如何在 Windows2003 服务器上进行 VPN 服务端的配置，由于我们引入 ePass3000 进行 VPN 连接的认证，所以所使用的 Windows2003 服务器必须是能够颁发证书的 CA 服务器，配置 CA 服务器的方

法请参见 ePass3000_CRYPTO_PKI_C 文档中的 1.8 节配置证书颁发机构。

1.1.1 VPN接入服务器的安装

1. 选择“开始”—〉“管理工具”—〉“路由和远程访问”弹出“路由和访问”对话框，如下图所示：

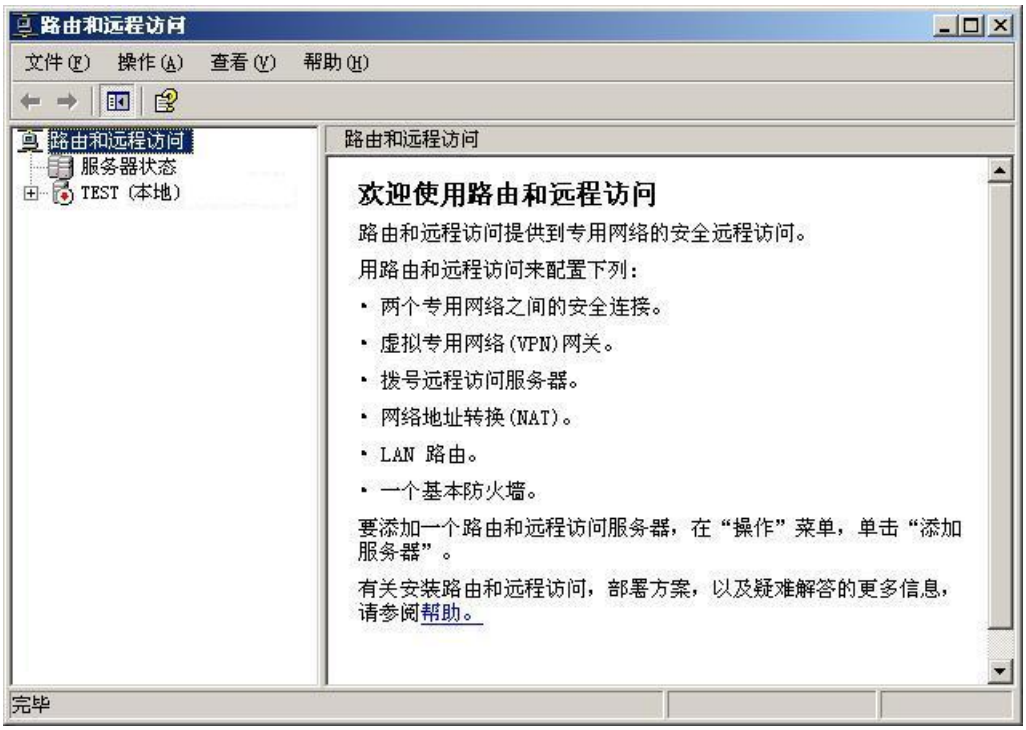

图 2 路由和远程访问

2. 右键单击本地计算机（FT（本地）），在右键菜单中选择“配置并启用路由和远程访问”，弹出路由和远程访问服务器安装向导，如下图所示：

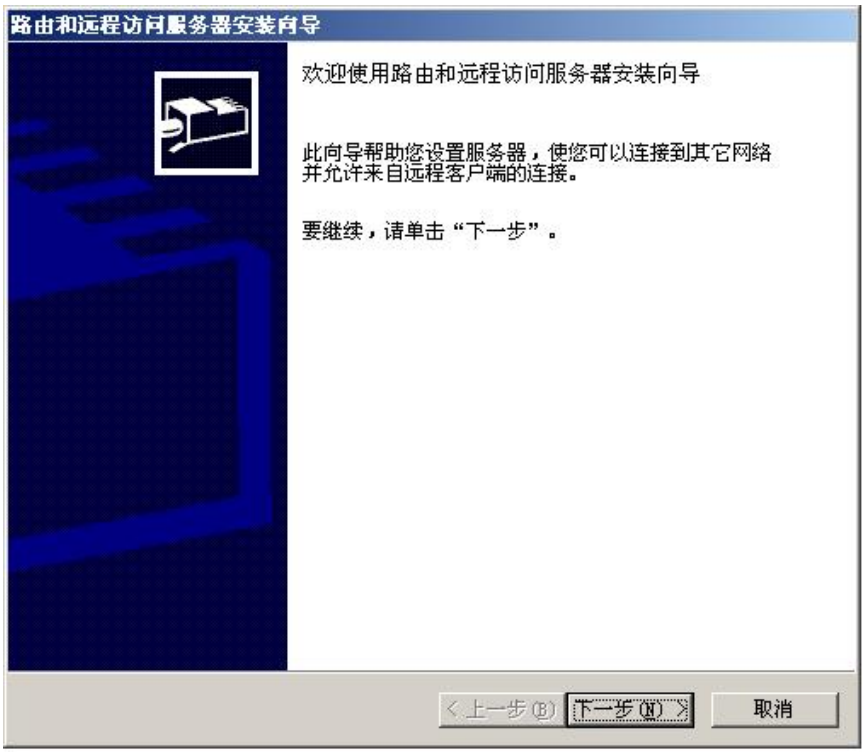

图 3 路由和远程访问服务器安装向导

3. 点击“下一步”进入配置页，选择“自定义配置”，如下图所示：

图 4 VPN 服务的配置

4. 点击“下一步”，进入自定义配置页，选择“VPN 访问”，如下图所示：

图 5 自定义配置

5. 点击“下一步”，进入选择摘要页，确认是否选中了“VPN 访问”，如下图所示：

图 6 选择摘要

6. 点击“完成”，完成服务端配置，此时会弹出对话框询问是否开始服务，点击“是”启动服务。

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。

1.1.2 VPN接入服务器的配置

1. 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”。

2. 在弹出的服务器属性对话框中选择“安全”属性页，并单击“身份验证方法”按钮，弹出“身份验证方法”对话框，如下图所示：

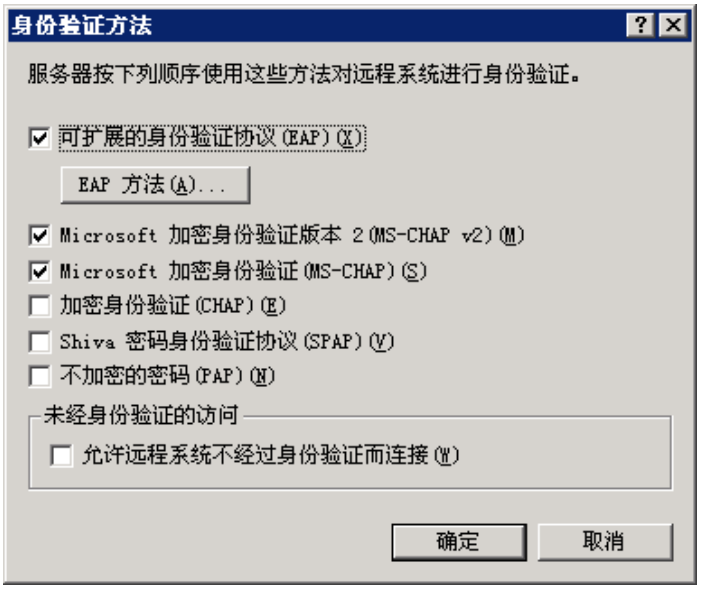

图 7 服务器属性设置

3. 选择“可扩展的身份验证协议(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。

4. 点击“确定”按钮，关闭“身份验证方法”对话框。

5. 点击“确定”按钮，关闭“服务器属性”对话框。

6. 最后在 Active Directory 中新建一个用户，右键单击此用户，选择“属性”，再选择“拨入”页，在“远程访问权限（拨入或 VPN）”栏内选择“允许访问”，之后点击“确定”按钮，保存用户的设置，如下图所示：

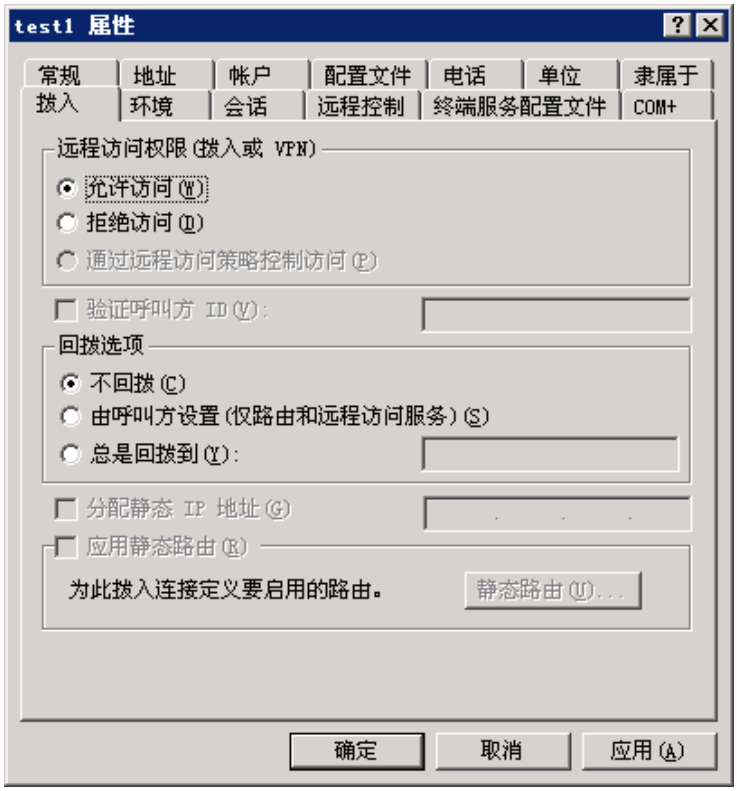

图 8 用户属性设置

注意：经过上述配置后用户即可申请用于 VPN 连接时进行身份验证的证书了，在申请证书时，您必须使用上述设置过的用户申请。

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。

1.3 VPN客户端配置

客户端的配置是在客户端计算机上进行的，本文档以 Windows XP 为例进行说明。

1. 右键单击“网上邻居”，弹出“网络连接”对话框；
2. 选择“创建一个新的连接”，弹出“新建连接向导”，如下图所示：

图 9 新建连接向导

3. 点击“下一步”，在“网络连接类型”页面中选择“连接到我的工作场所的网络”，如下图所示：

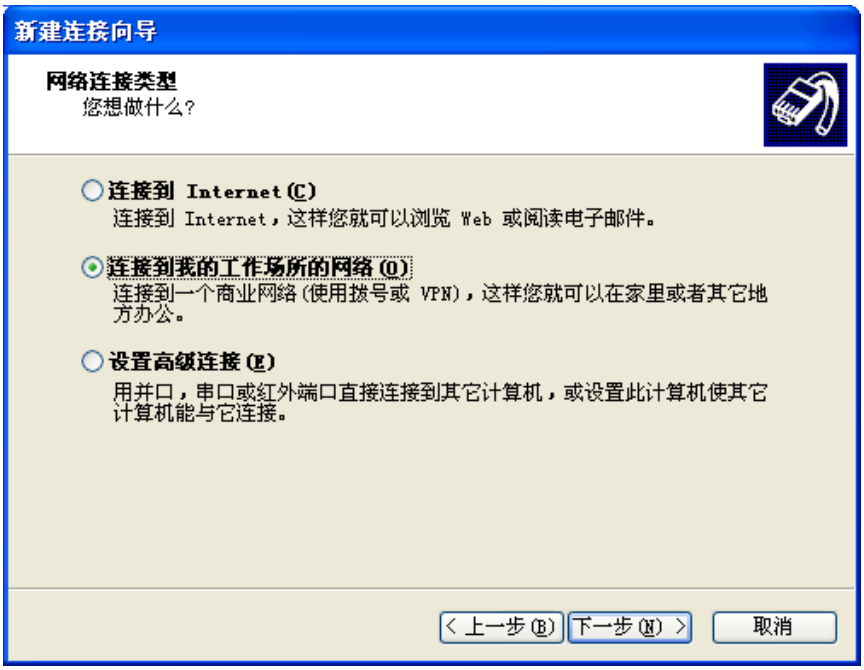

图 10 选择网络连接类型

4. 点击“下一步”，在“网络连接”页选择 “虚拟专用网络连接”，如下图所示：

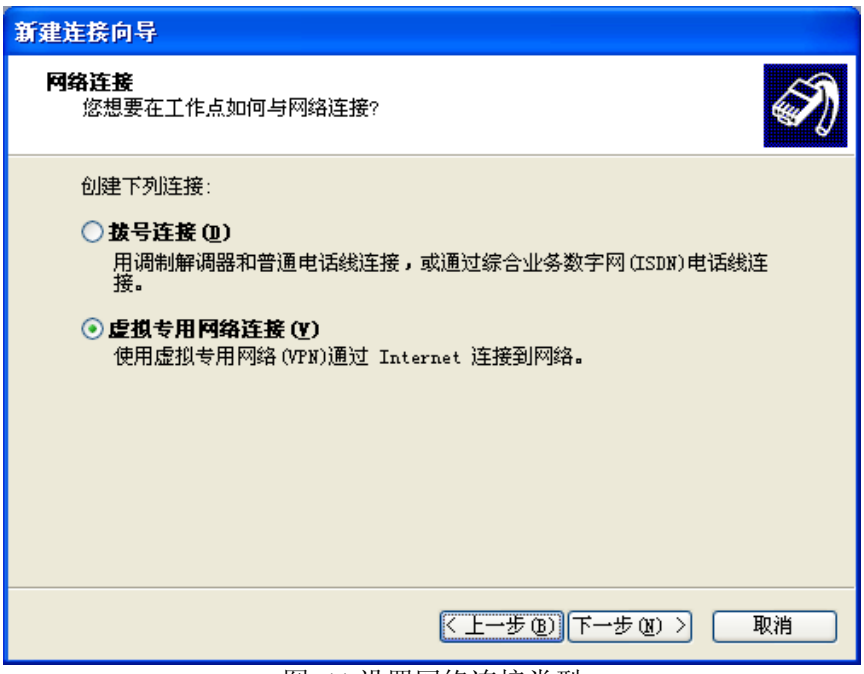

图 11 设置网络连接类型

5. 点击“下一步”，在“连接名”页中输入合适的连接名，如下图所示：

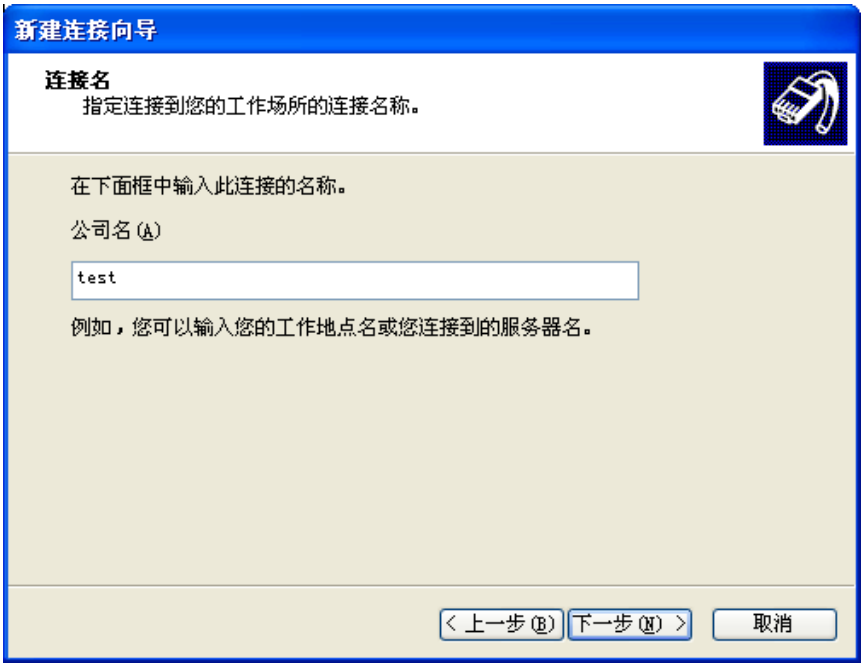

图 12 设置连接名

6. 点击“下一步”，在“公用网络”页根据需要选择连接方式，如下图所示：

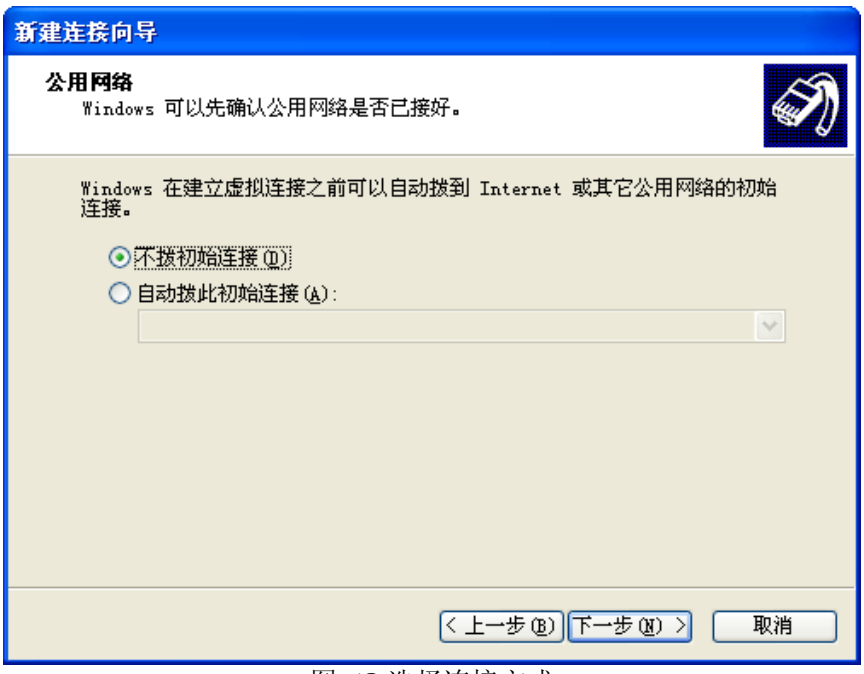

图 13 选择连接方式

7. 点击“下一步”，在“VPN 服务器选择”页，输入服务端的 IP，如下图所示：

图 14 输入服务端 IP 地址

8. 点击“下一步”，在“智能卡”页选择“使用我的智能卡”，如下图所示：

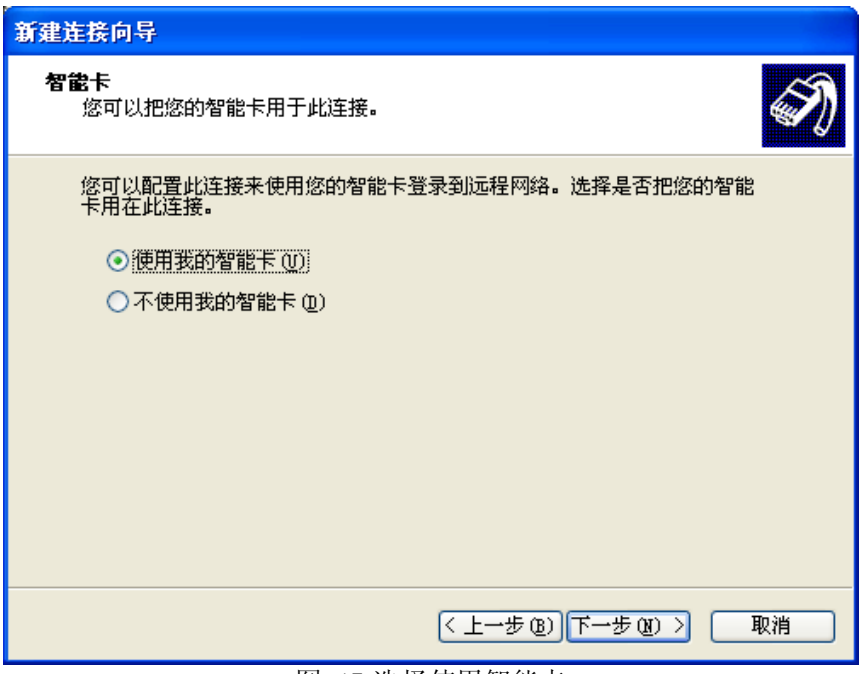

图 15 选择使用智能卡

9. 点击“下一步”，在“可用连接”页选择设置此连接的权限，如下图所示：

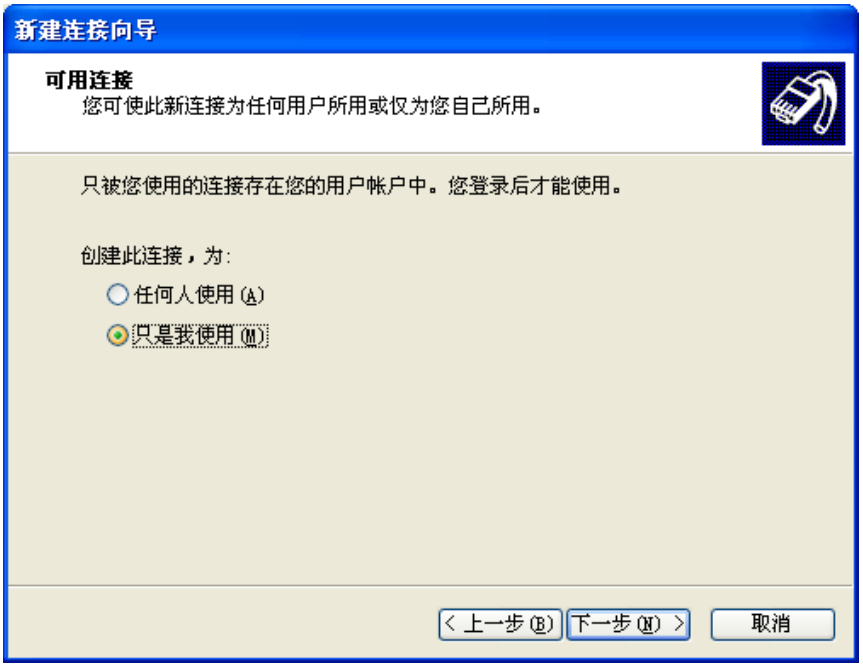

图 16 选择用户权限

10. 点击“下一步”，出现“正在完成新建连接向导”页，确认无误后，点击“完成”，如下图所示：

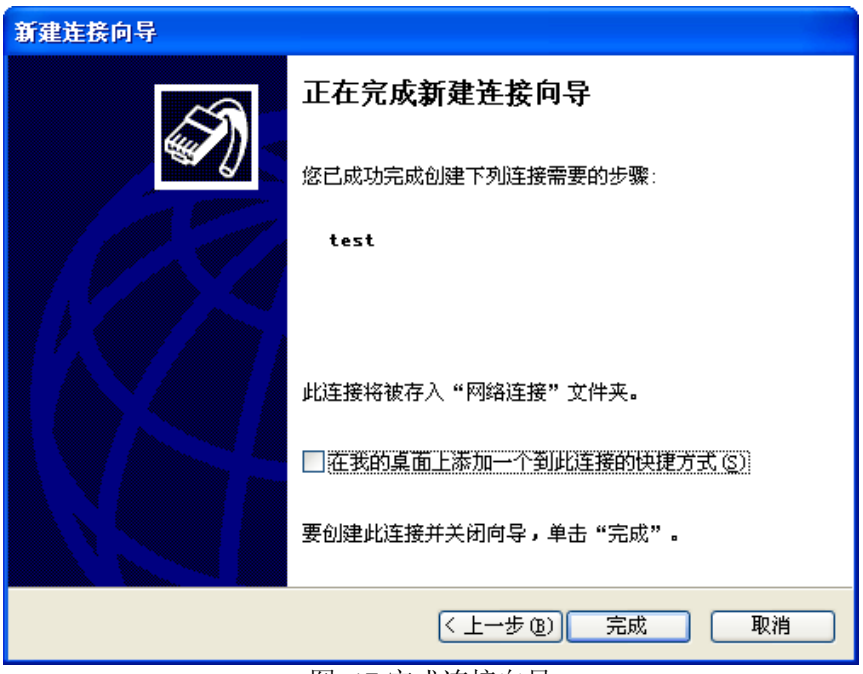

图 17 完成连接向导

至此 VPN 客户端软件的配置就完成了。要进行 VPN 登录，双击新建立的 VPN 拨号图标，插入申请过证书的 ePass3000，按提示输入 ePass3000 的用户 PIN 码就可以进行 VPN 连接访问了。