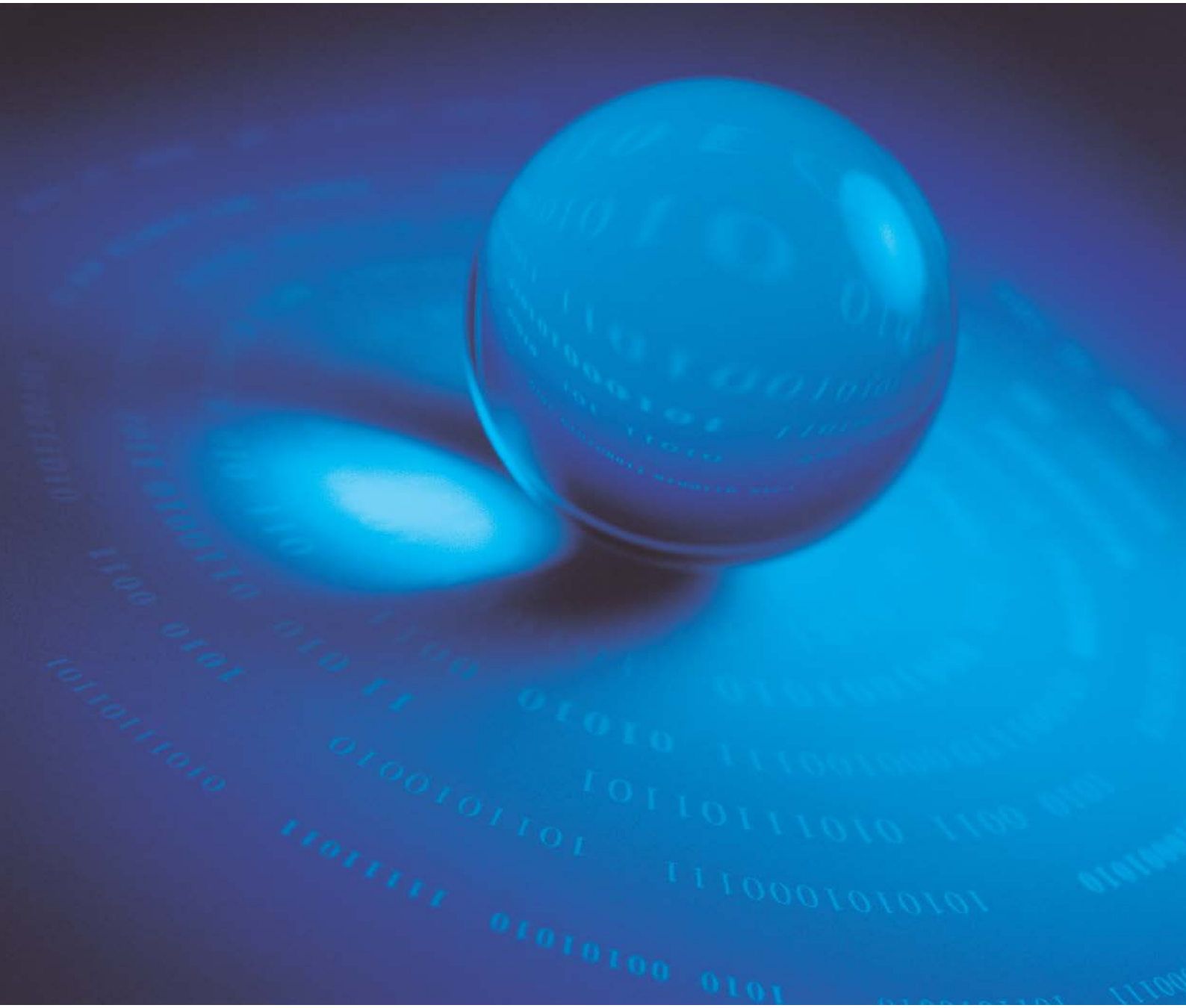
ePass3003 的 Check Point 应用

1.2 版



http://www.EnterSafe.com

EnterSafe 尽最大努力使这篇文档中的内容完善且正确。EnterSafe 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	说明
2008 年 3 月	1.0	第一版
2009 年 5 月	1.1	第一版第一次修订

EnterSafe
软件开发协议

本《软件开发协议》（以下简称《协议》）是用户（个人或者单一机构团体）与 EnterSafe 之间有关随附本《协议》的 EnterSafe 软件产品的法律协议。本软件产品包括计算机软件，并且还可能包括电子文档、相关媒体和印刷材料（以下简称“软件产品”）。您一旦安装、复制或以其他方式使用本“软件产品”，即表示您同意接受本《协议》中的条款的约束。如果您不同意本《协议》中的条款，则您不得安装、复制或以其他方式使用本“软件产品”；您可以将本“软件产品”退还原购买处并取得全额退款。

1.软件产品使用许可

如果您遵守本协议的条款，EnterSafe 将授予您协议中所述的权利。

1.1 EnterSafe 授予您作为个人的、非独家性的许可证，仅供您为用于设计、开发及测试您的设计以及与任何 EnterSafe 产品一起运行的软件产品。您可在无数量限制的计算机上安装本“软件产品”的副本，但您必须是本“软件产品”的唯一使用者。如果您为一个机构团体，EnterSafe 授予您指定您组织内一位人员依以上所规定的方式使用本“软件产品”的权力。

1.2 EnterSafe 允许您将本软件合并或链接到您的计算机程序中，但本软件产品中被合并或链接的部分仍受本协议的约束。

1.3 您可以以存档为目的复制合理数量本软件产品的副本;但如果 Entersafe 通过公开声明或发布新闻的形式终止软件副本的使用，您必须马上遵守这个要求。

2.反向工程、反向编译、反汇编的限制

您不可以对本“软件产品”的部分或全部进行反向工程、反向编译或反汇编；尽管有这项限制，如果适用法律明示允许上述活动，则不在此限制范围。

3.禁止租借、传播或商业主办服务

您不可出租、租赁或出借本“软件产品”；或将本“软件产品”放在服务器上传播；或利用本“软件产品”提供商业主办服务。

4.责任限制和补救措施

无论任何原因（包括但不限于上述所有直接规定或一般性的合同规定或其它情况）发生的损害，EnterSafe 与其供应商在本协议条款下的所承担的全部责任以及全部损害的唯一补偿，不超出您购买本“软件产品”所支付的款额。

5.免责声明

在适用法律所允许的最大范围内，EnterSafe 或其供应商按“现有状况且包含所有错误”提供本“软件产品”或支持服务（如果有），并声明不承担所有其他明示、隐含或法定的担保、责任和条件。其中包括但不限于下列任何担保、责任或条件（如果有）：适销性、对于特定目的的适用性、可靠性或可用

性、回应的准确性或完整性、结果或工艺的精良性、无病毒以及无疏忽；还包括通过本“软件产品”或因使用本“软件产品”而提供或未提供支持服务或其他服务、信息、软件和相关内容。用户对本“软件产品”没有所有权、不受干扰的使用权、不受干扰的占有权、与说明一致或不侵权的任何保证或条件。

6.版权所有

EnterSafe 保留所有本《协议》中未明确授予您的权利，本“软件产品”受版权和其它知识产权法及相关条款的保护。EnterSafe 拥有本“软件产品”的所有权、版权和其他知识产权。

7.协议终止

本《协议》在终止前有效。若您违反本《协议》的任何条款，使用本“软件产品”的权利将自动终止。本“软件产品”必须被销毁或返回 EnterSafe。您可以销毁本“软件产品”及其所有副本以终止协议。但条款 2，3，4，5，6 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 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.

章节目录

图目录

第一章 ePass3003 的 Check Point 应用指南

ePass3003 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 ePass3003 进行任何形式的编程开发就能通过配置相关服务而可以将 ePass3003 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 CryptoAPI（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。

本章主要讲述如何配置 ePass3003 的 Check Point 应用。本手册包括使用 ePass3003 申请 Check Point 证书和使用申请的证书进行 Check Point 连接的操作方法。

- 使用 ePass3003 申请 Check Point 证书
- 使用 ePass3003 进行 Check Point VPN 连接

首先安装并配置好 Check Point 服务端；并在客户端计算机安装 Check Point 客户端，同时安装好 ePass3003 的 Runtime 包。本文档以 Check Point NGX_R60 为例进行说明。

1.1 使用 ePass3003 申请 Check Point 证书

安装过 Check Point 客户端的计算机，在右下角会有一个黄色钥匙图标。

1. 右键点击黄色钥匙图标，在快捷菜单中选择“Settings”，弹出 Check Point VPN-1 SecureClient Settings 对话框，如图 1 所示：

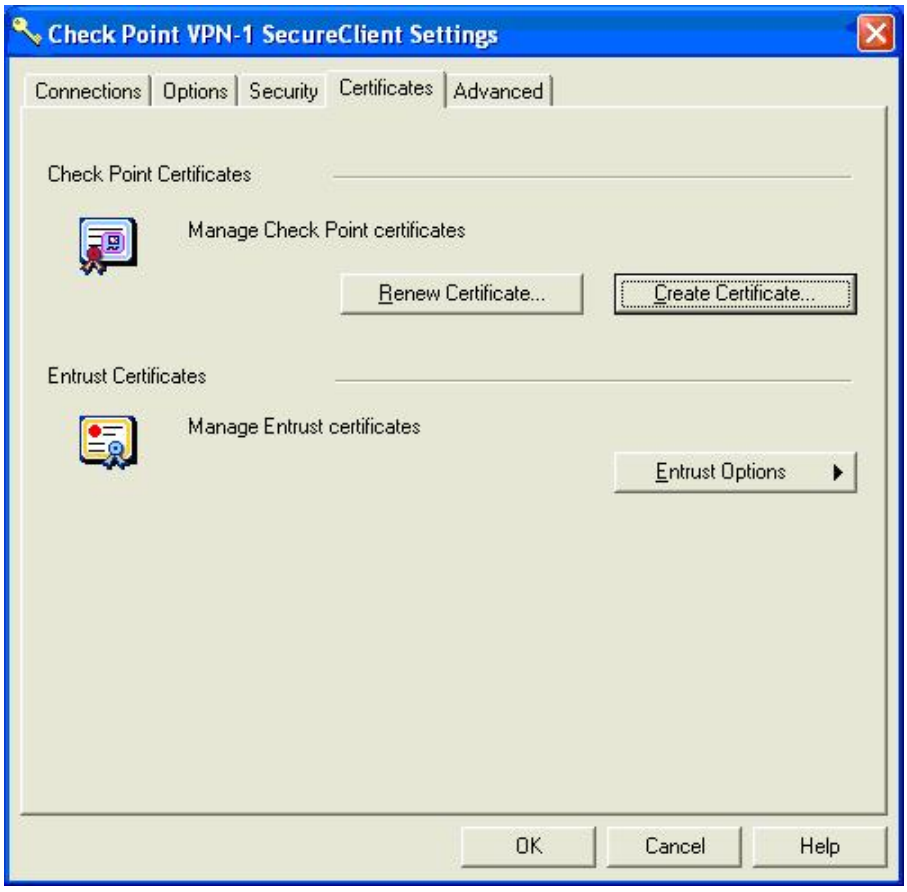


图 1 Check Point VPN-1 SecureClient Settings

2. 选择 Certificates 选项卡，点击 Create Certificate 按钮，弹出 Check Point 创建证书向导，如图 2 所示：

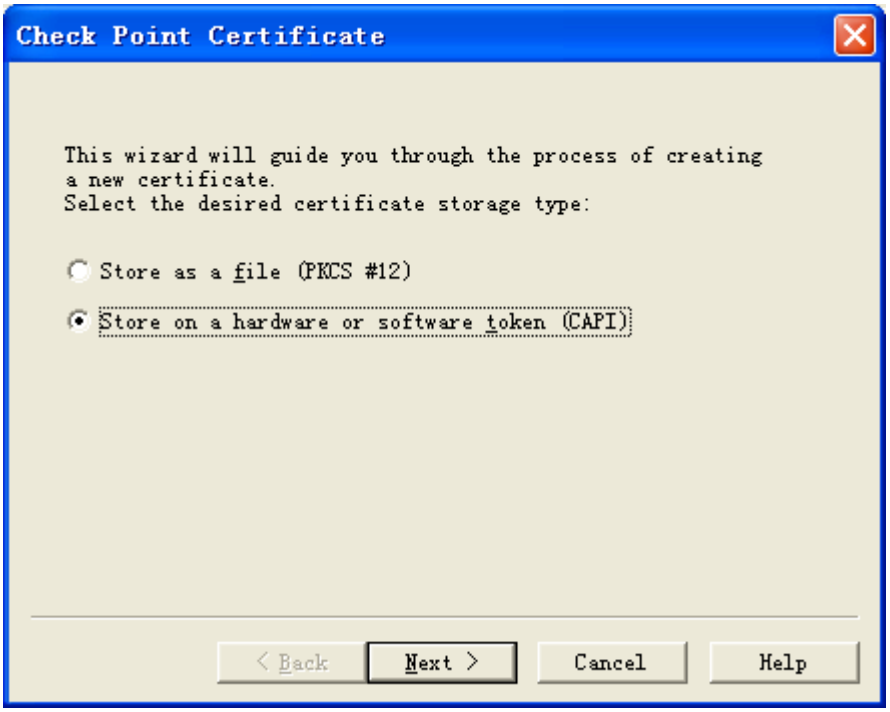


图 2 Check Point 创建证书向导

3. 选择 Store on a hardware or software token（CAPI）以便将证书存储到硬件 Token ePass3003 中，点击 Next，弹出如图 3 所示的 CSP 选择对话框：

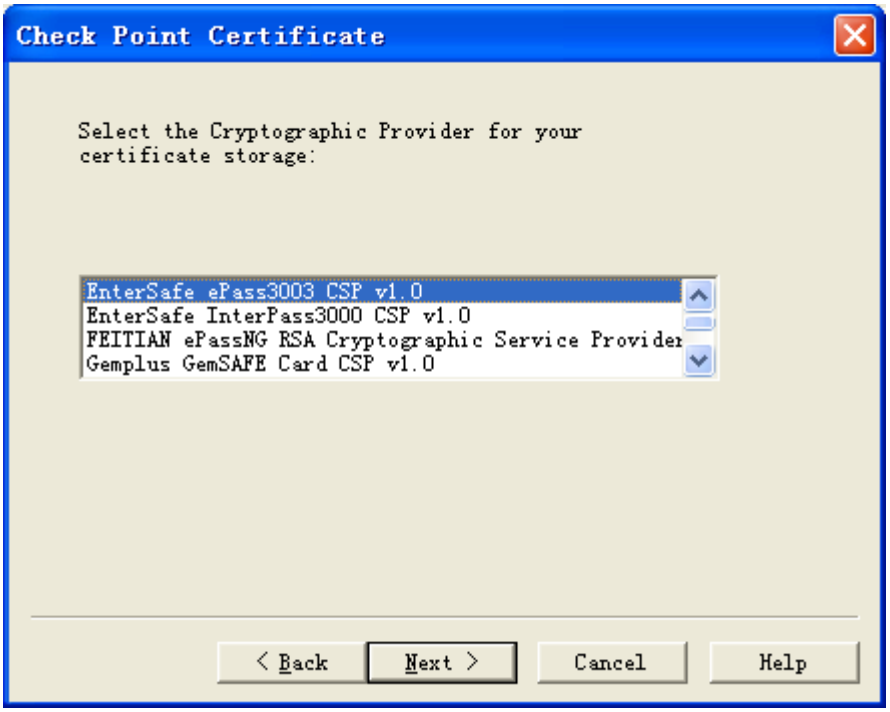


图 3 CSP 选择对话框

4. 选择 EnterSafe ePass3003 CSP v1.0，然后点击 Next，弹出填写 IP 和 Registration Key 对话框，如图 4 所示：

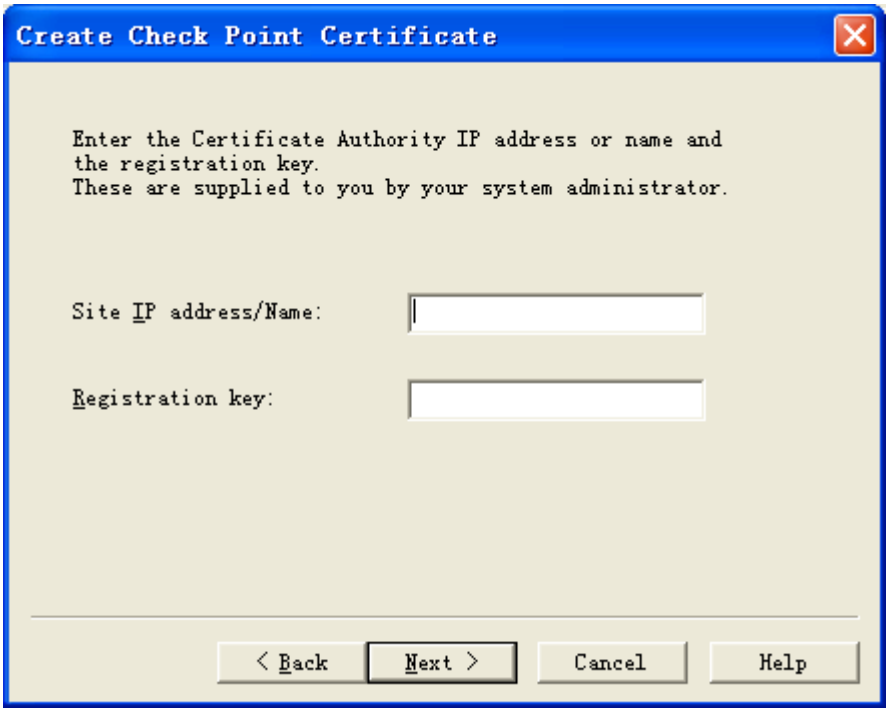


图 4 填写 IP 和 Registration Key 对话框

5. 填入服务端 IP 地址和 Registration Key，点击 Next，此时会弹出如图 5 所示的 PIN 码输入框：

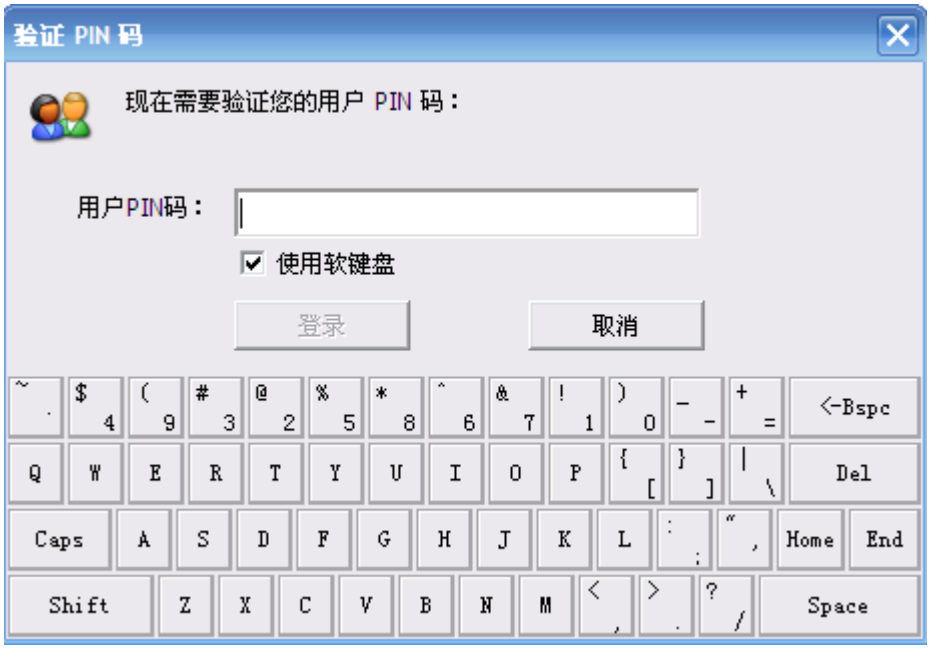


图 5 验证 ePass3003PIN 码

注意：上图显示的是使用软键盘输入用户 PIN 码的情况，用户可以不选择“使用软键盘”，但是建议您选择“使用软键盘”登录到 Token，这样才能保证您的 PIN 码的安全，选择使用“使用软键盘”后，物理键盘的键盘输入将被禁用。

6. 输入正确的 ePass3003PIN 码后点击“登录”按钮，Check Point 认证证书就申请成功了，如图 6 所示：

图 6 证书申请成功界面

7. 点击 Finish 完成 Check Point 证书申请。

1.2 使用 ePass3003 进行 Check Point VPN 连接

证书申请成功后，就可以使用此证书进行 Check Point VPN 连接了。

1. 双击黄色钥匙图标，如果您没有建立过 VPN 连接，将弹出建立新的连接的提示，如图 7 所示：

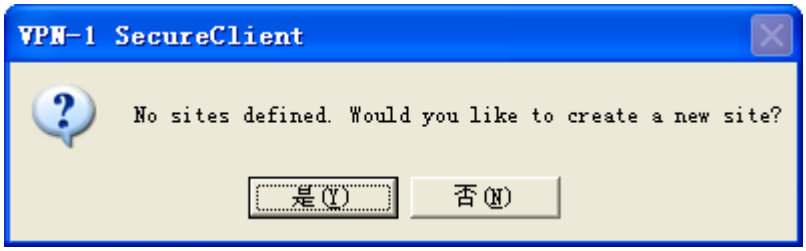


图 7 建立新连接提示

2. 点击“是”，弹出新建连接向导，如图 8 所示：

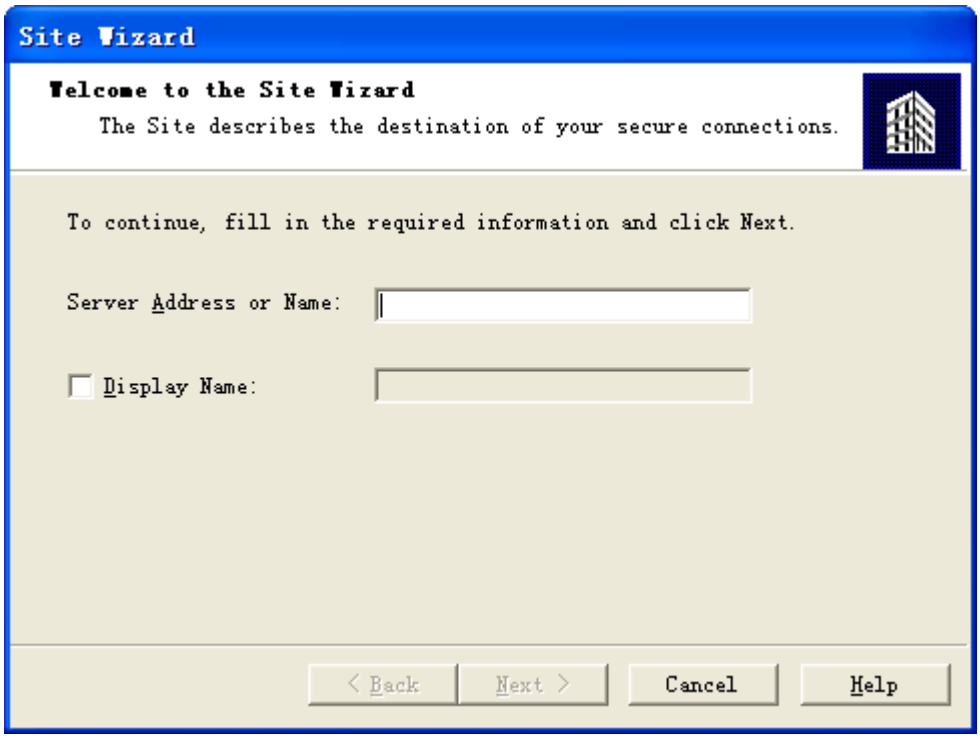


图 8 新建连接向导

3. 填入服务端 IP 地址，点击 Next，弹出选择认证方式对话框，如图 9 所示：

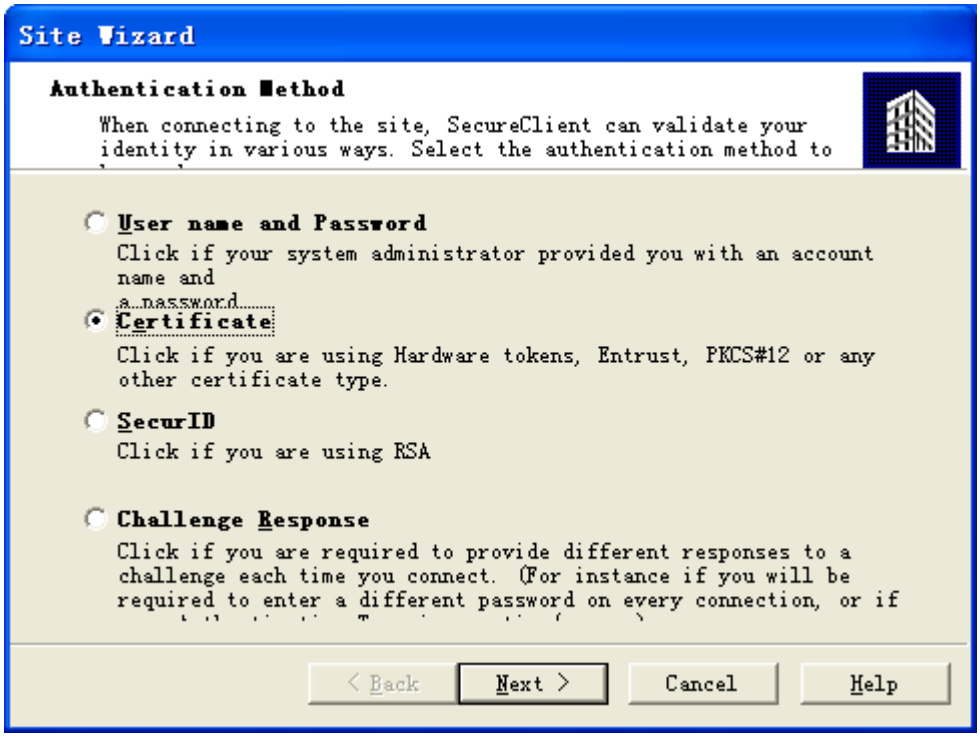


图 9 选择认证方式对话框

4. 在此我们选择 Certificate，以证书方式进行身份认证，点击 Next，弹出证书选择对话框，如图 10 所示：

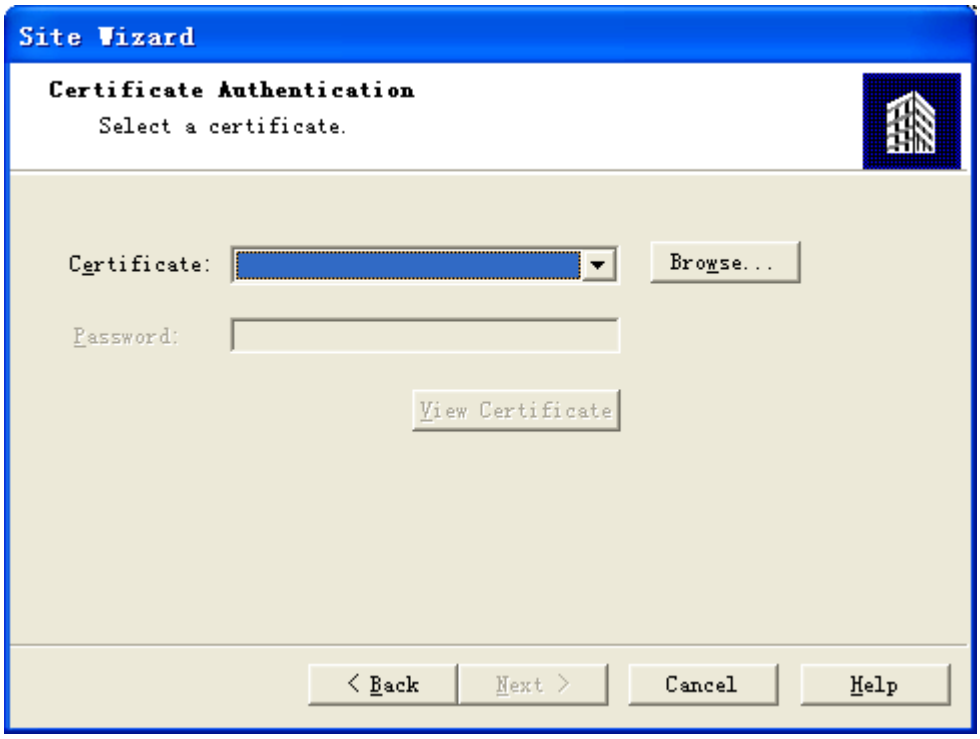


图 10 证书选择对话框

5. 在 Certificate 下拉列表中选择刚刚申请过的证书，点击 Next，弹出选择连接设置对话框，如图 11 所示：

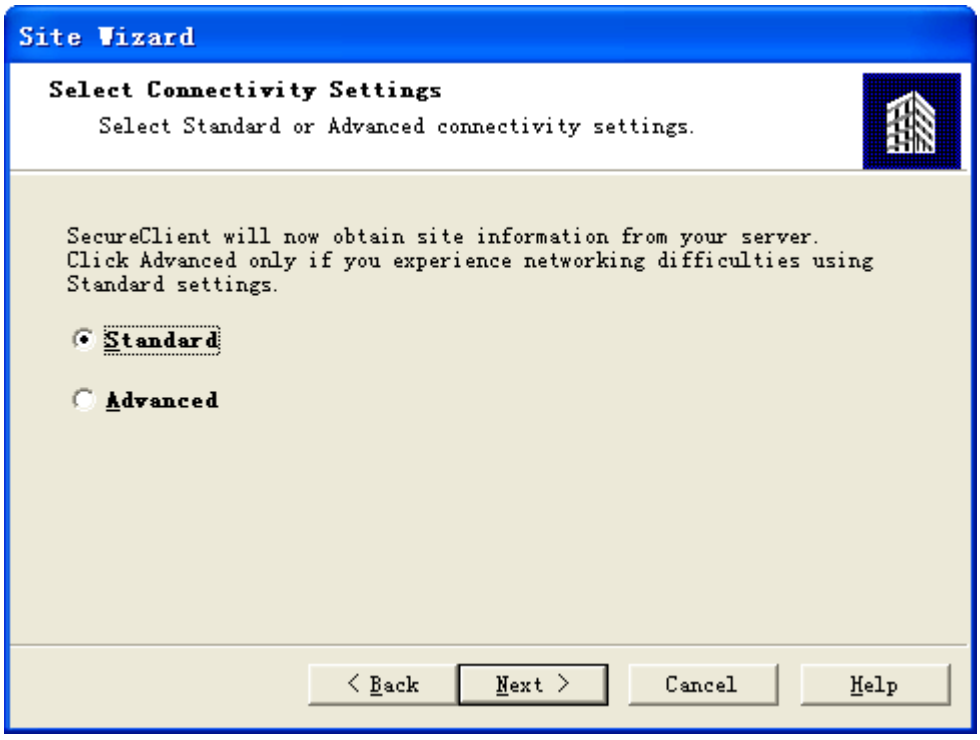


图 11 选择连接设置对话框

6. 默认选择 Standard，点击 Next，显示正在连接，并弹出 ePass3003PIN 码验证对话框，如图 12 所示：

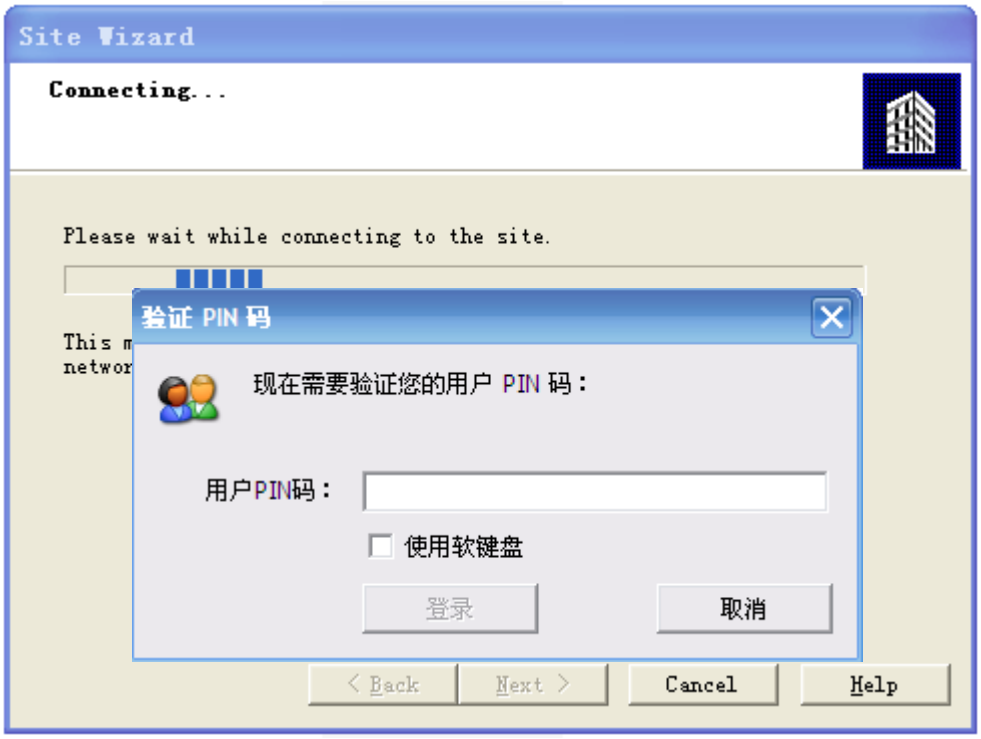


图 12 正在连接界面

7. 输入正确的 ePass3003PIN 码，点击“登录”按钮，显示如图 13 所示的界面：

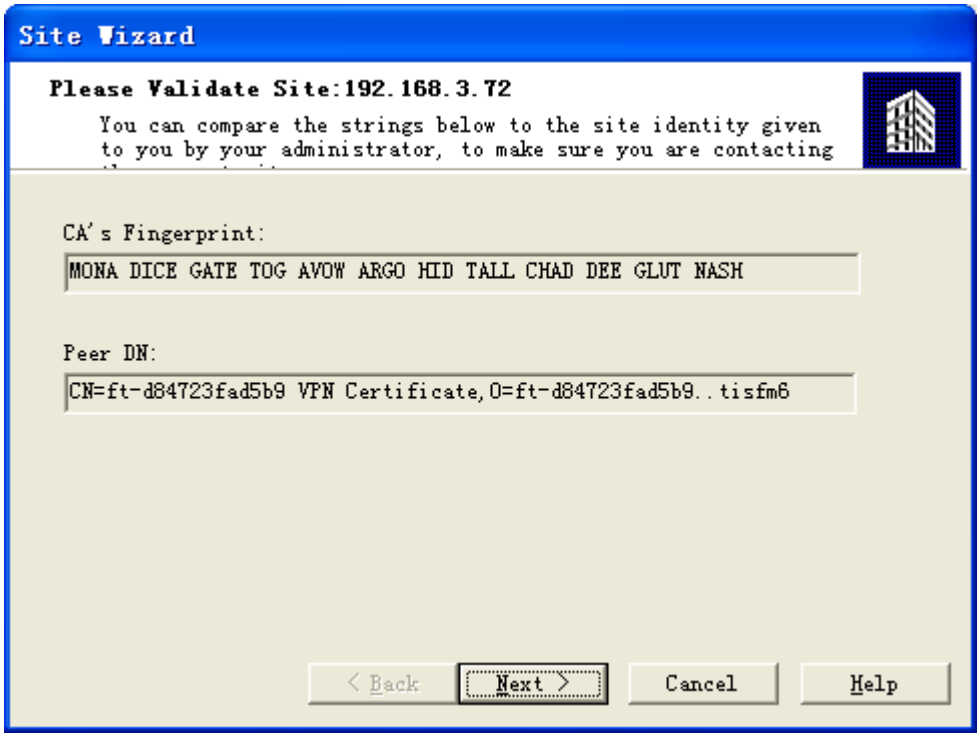


图 13 确认连接对话框

8. 点击 Next，显示如图 14 所示的连接建立成功对话框：

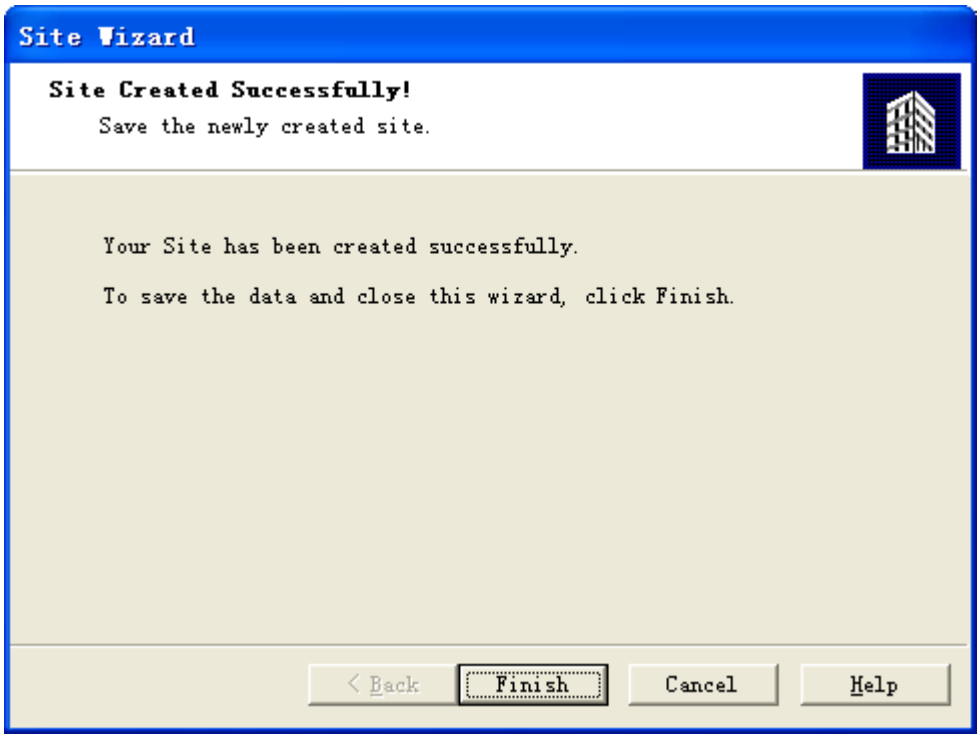


图 14 连接建立成功对话框

9. 点击 Finish 完成建立连接的操作。

10. 根据建立连接后的提示或双击黄色钥匙图标，进行 Check Point VPN 连接，弹出如图 15 所示的连接对话框：

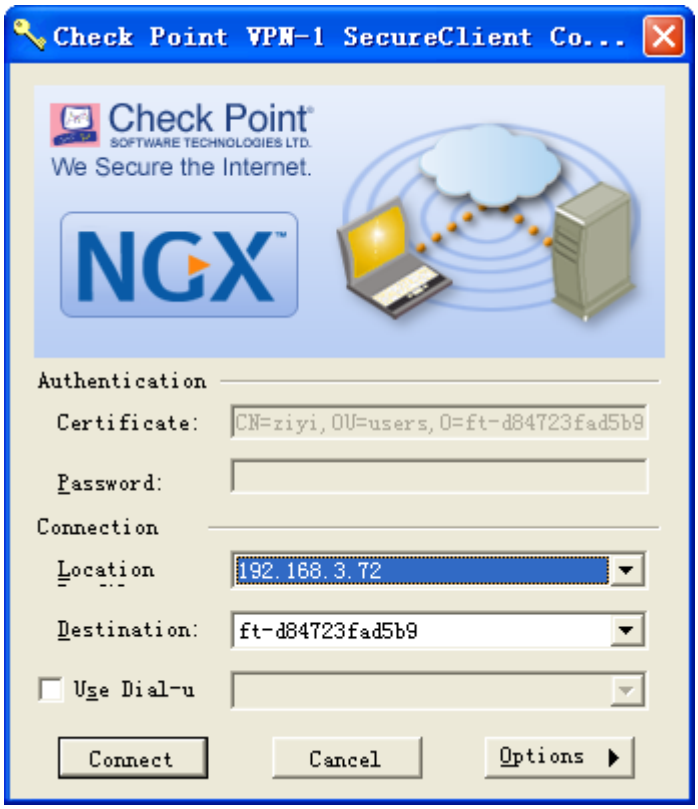


图 15 Check Point 连接对话框

11. 点击 Connect，弹出 PIN 码输入框，输入正确的 ePass3003PIN 码，点击“登录”按钮，认证通

过后显示连接成功对话框，如图 16 所示：

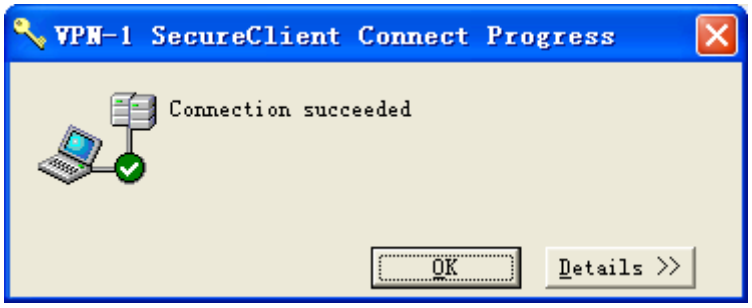


图 16 连接成功对话框

12. 点击 OK 按钮，完成 VPN 连接，以后客户端和服务端之间的数据就会通过 Check Point VPN 建立的安全信道进行交互。

附录 缩略语及术语

缩略语及术语	解　释
ePass3003	飞天推出的 USB 接口的便携式密码设备，具有高性能、高安全性、灵活易用、造价低廉、携带方便等好处。
ePass3003Auto	飞天推出的 USB 接口的便携式密码设备，在 ePass3003 基础上加入自动安装中间件的功能，具有更高的易用性。
Token	密码设备的统称，可以是智能卡，也可以是具有密码和证书存储功能的任何硬件设备。
USB Token	具有 USB 接口的密码设备，其携带方便，操作简单。ePass3003 是其中一种。
CryptoAPI 接口 (简称 CAPI)	由微软公司提供的密码(cryptography)操作接口，提供设备无关的或软件实现的密码算法封装，很容易使开发者能够开发出用于数据加解密、使用数字证书的身份认证、代码签名等的 Windows 平台上的 PKI 应用程序。
PKCS#11 接口	由 RSA 实验室推出的程序设计接口，将密码设备抽象成一种通用的逻辑视图即密码令牌（Cryptographic Token）提供给上层应用，做到设备无关性和资源共享。