



TheGreenBow IPsec VPN 客户端

证书使用指南

网站：<http://www.thegreenbow.com>

联系我们：support@thegreenbow.com

目录

1	简介.....	3
1.1	文档目标.....	3
1.2	特性.....	3
2	管理证书.....	4
2.1	使用证书.....	4
2.2	导入 PKCS#12 证书.....	6
2.3	导入 PEM 文件.....	8
2.4	读智能卡.....	Erreur ! Signet non défini.
2.5	配置选项.....	12
3	使用微软证书服务器.....	13
3.1	安装微软证书服务器.....	13
3.2	生成证书.....	15
3.2.1	生成一个用户证书.....	15
3.2.2	签署证书申请.....	18
3.3	证书导出.....	19
4	使用 OpenSSL.....	21
4.1	生成证书.....	21
4.1.1	生成一个自签名的证书.....	21
4.1.2	生成一个用户证书.....	22
4.2	其它 TgbSmallPKI 工具.....	24
4.2.1	显示证书信息.....	24
5	故障排除.....	26
6	联系我们.....	27

	文件参考	tgvpn_certificates_zh
	文件版本	2.0 – 2006 年 6 月
	VPN 版本	4.00

1 简介

1.1 文档目标

此文档解释如何与 TheGreenBow IPSec VPN 客户端使用证书。这些证书可以存贮在智能卡中或从 PKCS#12 文件导入。

同时，此文档解释如何使用第三方认证机构以生成 X509 证书并且安全打开一个 VPN 隧道。有许多选项可以生成证书，如使用 Windows 2000/2003 服务器系统中的 Microsoft 证书服务器（如：微软证书服务），OpenSSL 或者某些 VPN 路由器本身。

1.2 特性

可以导入两种证书到 TheGreenBow VPN 客户端：

- PKCS#12
- PEM 证书

证书可以存贮在一个受 PIN 码保护的智能卡中。当建立一个隧道时可以动态使用 TheGreenBow VPN 客户端。

一个证书具有三个部分：

- 证书机构公钥
- 用户证书公钥
- 用户证书私钥

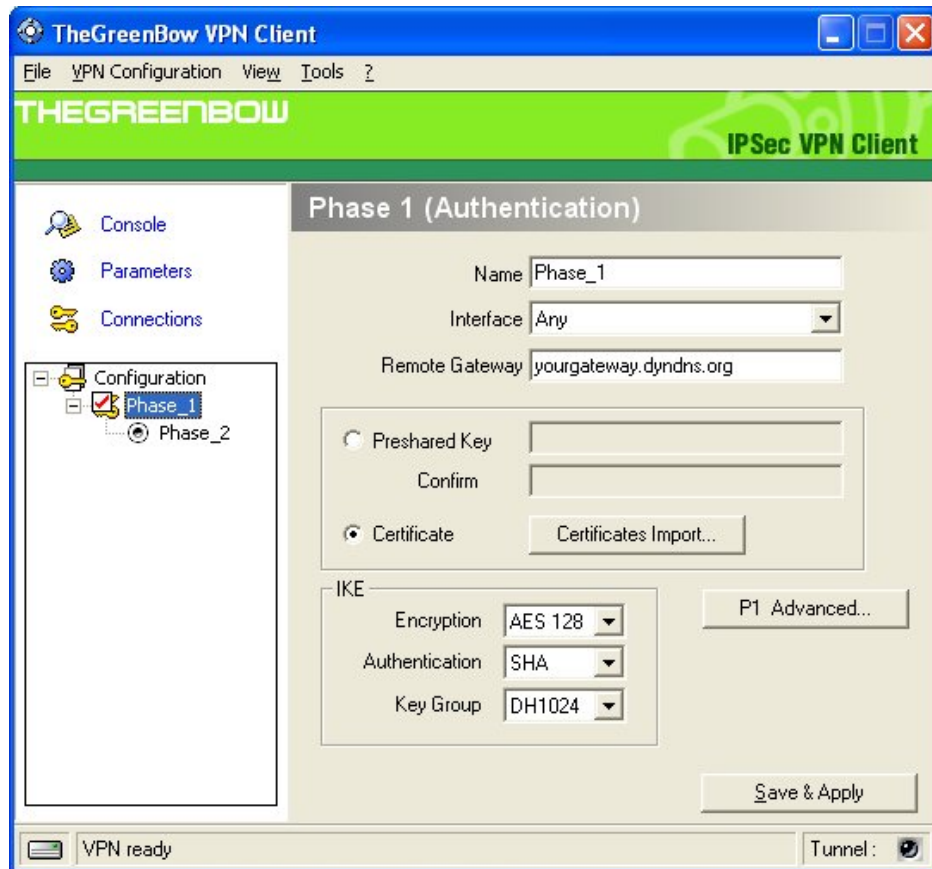
一旦导入，则这些密钥就存贮在配置文件中。一个证书只限于一个隧道。所有配置要素可以轻松导出到另外一台计算机上。

对于智能卡，配置文件不包括密钥。

2 管理证书

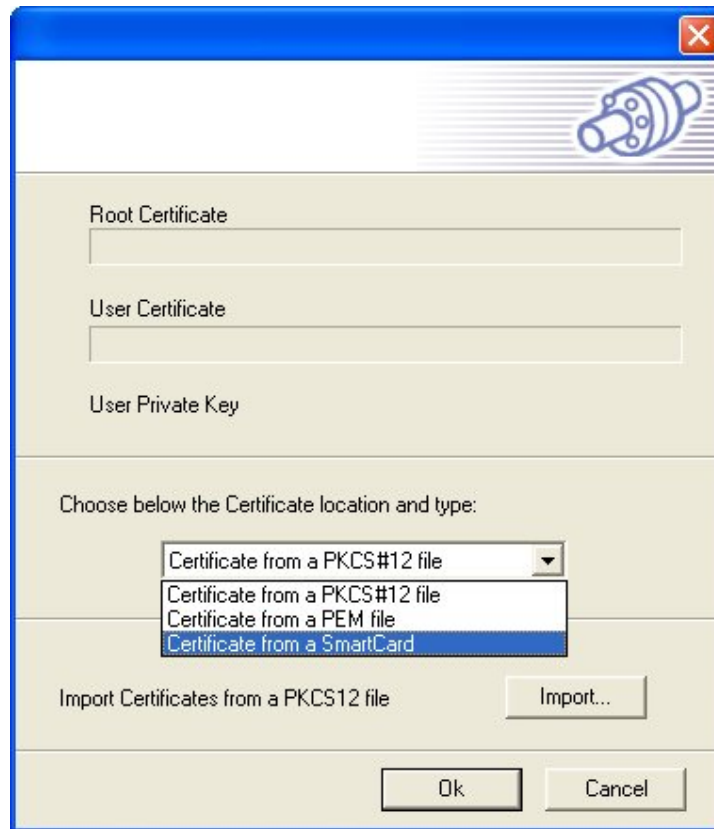
2.1 使用证书

X509 证书及智能卡在阶段 1 设置中管理，阶段 1 必须创建。



点击“证书”，然后点击“证书导入...”。

在证书导入窗口，用户可以在 VPN 配置中导入证书文件或从智能卡中读取证书。

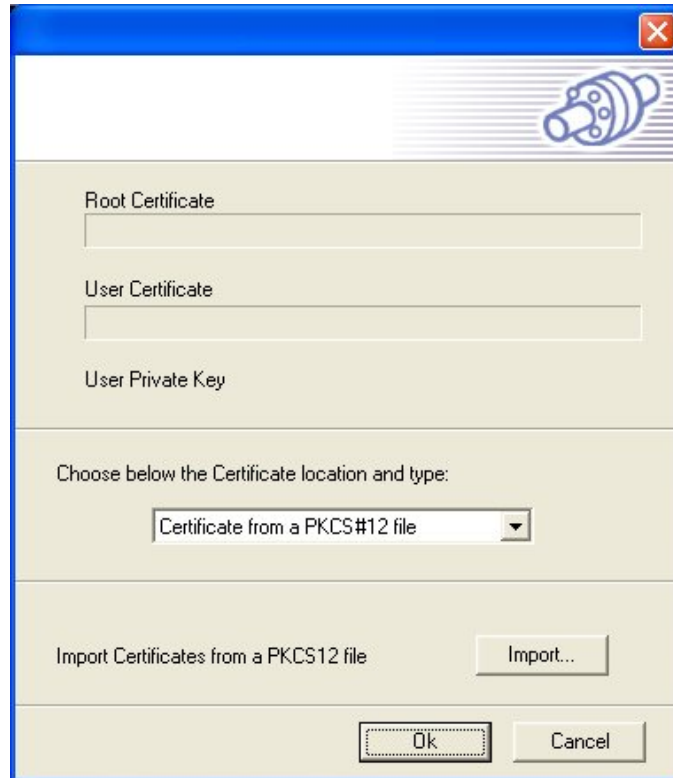


TheGreenBow VPN 客户端支持以下证书格式文件：

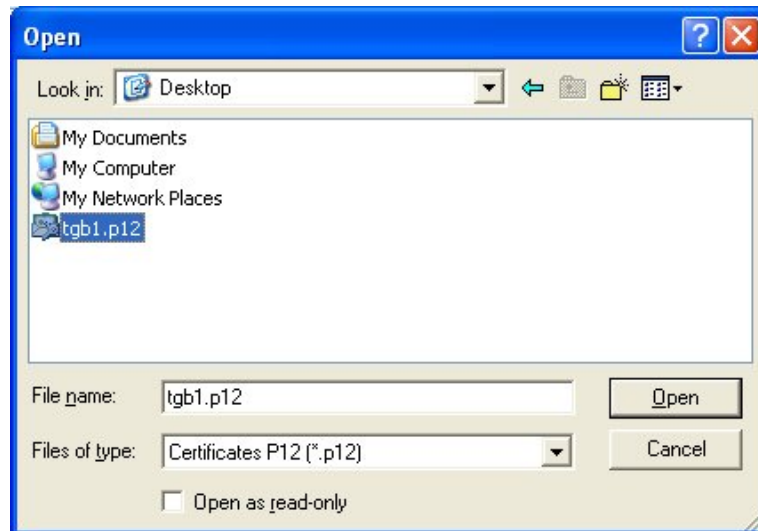
- PKCS#12 文件
- PEM 文件
- CRT 文件

2.2 导入 PKCS#12 证书

从下拉列表中，选择“来自 PKCS#12 文件的证书”。



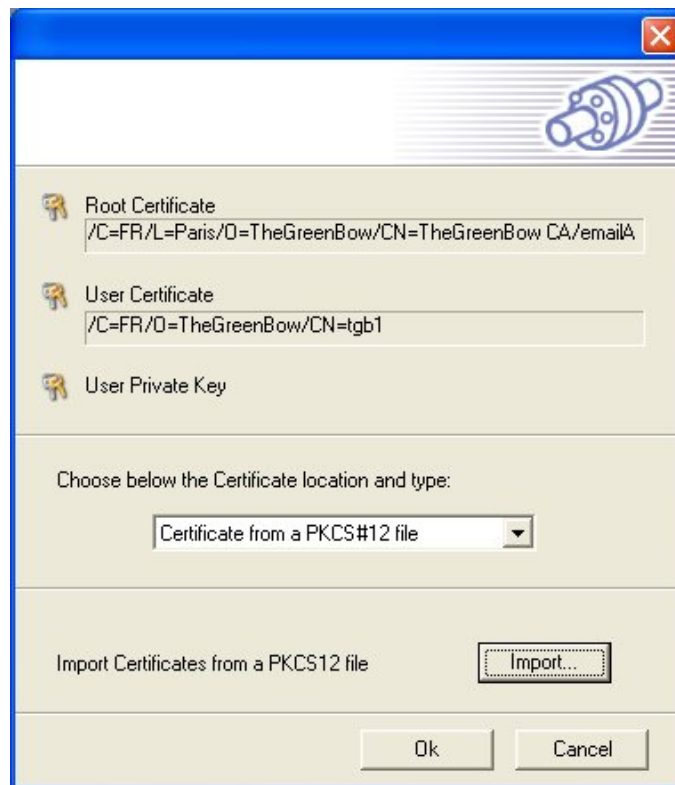
点击“导入...”



选择 PKCS#12 文件并点击“打开”。



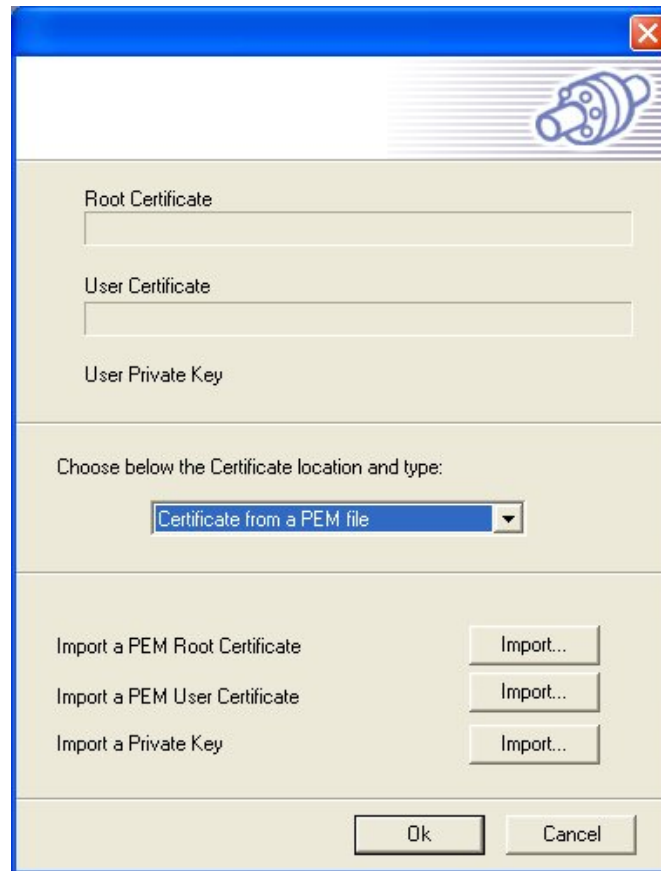
文件可以使用密码进行保护。如果没有密码保护，则编辑框可以为空。
点击“OK”导入文件。



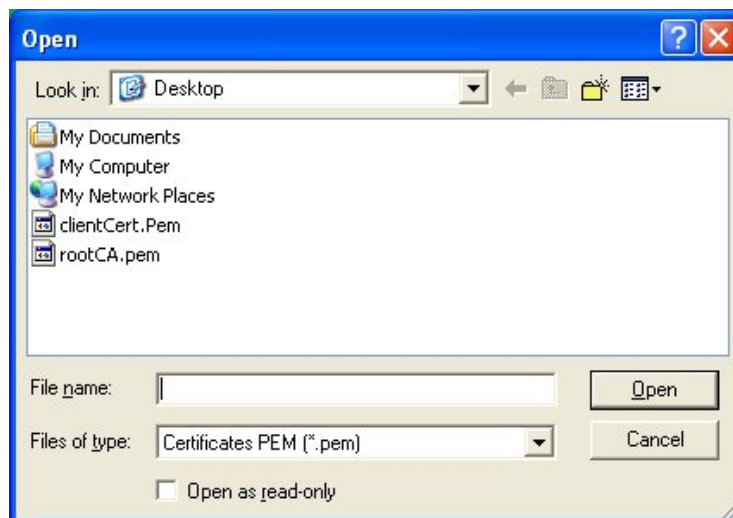
如果密码正确并且文件没有破坏，则显示证书和证书发布人的主题。
关键图标指示现在数据存贮在 TheGreenBow VPN 客户端配置文件中。

2.3 导入 PEM 文件

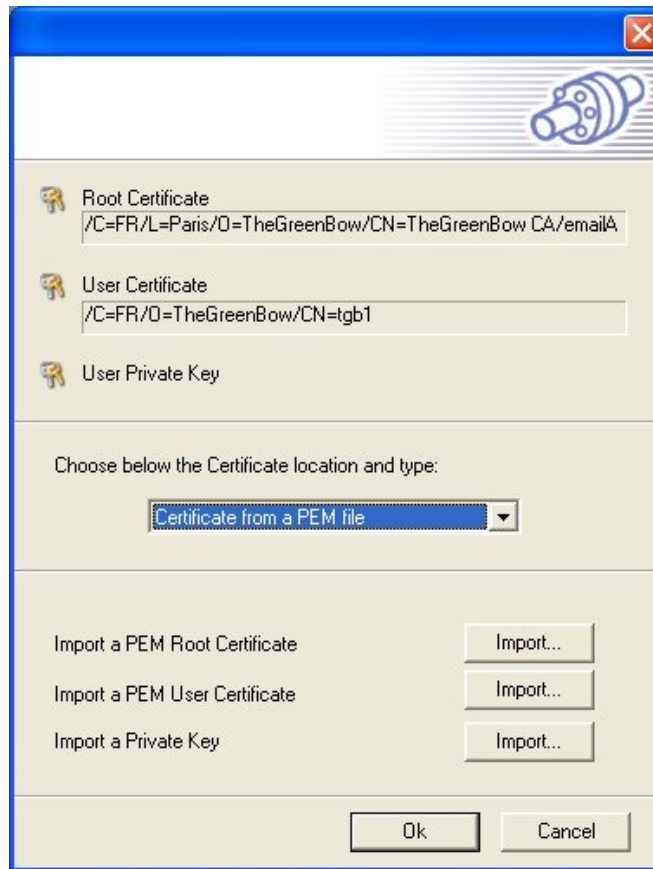
在证书管理窗口，从下拉列表中选择“PEM 文件证书”。



点击按钮“导入...”，可以导入证书机构（CA）公钥、用户公钥及用户私钥。



选择文件并点击“打开”。



一旦导入了文件，则显示用户证书及其发布方的主题。

2.4 读取智能卡

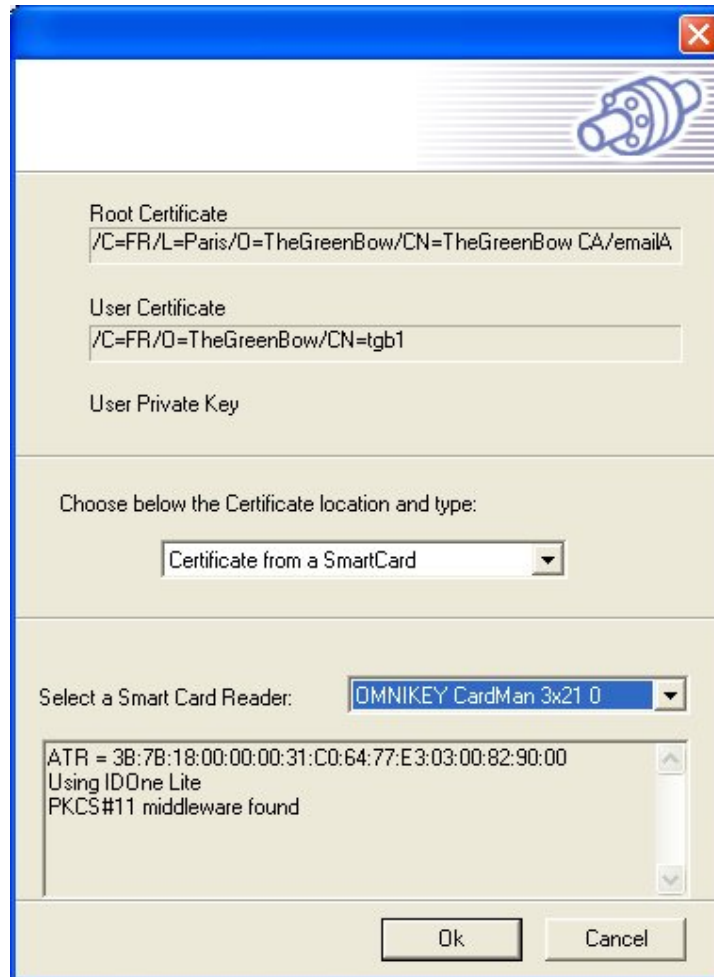
在证书管理窗口，选择“来自智能卡的证书”。



从智能卡列表中选择智能卡读卡器。

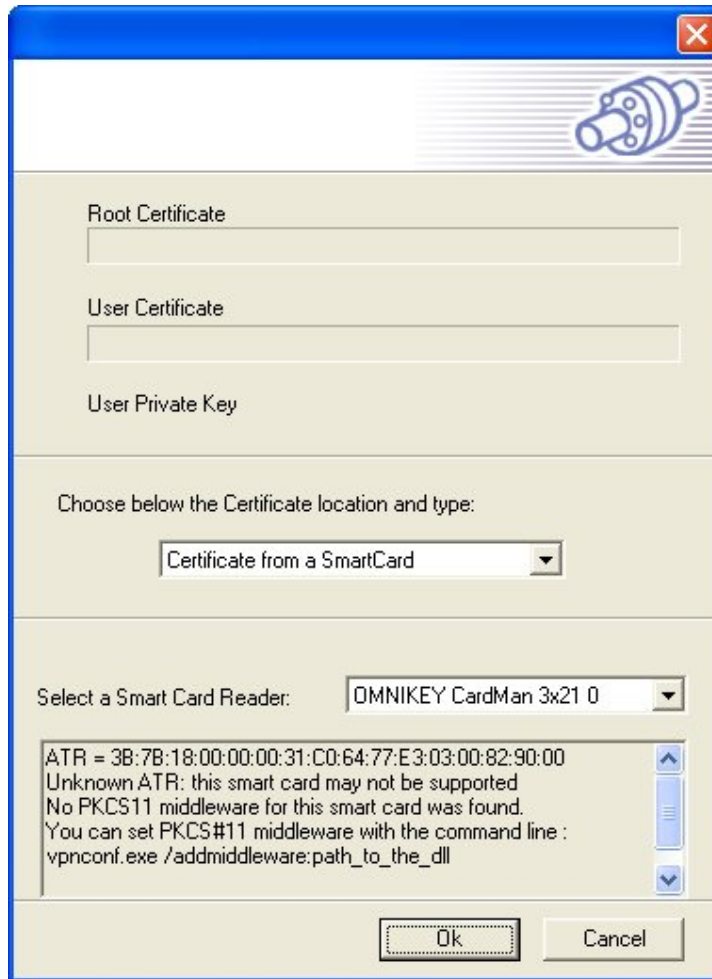


输入智能卡 PIN 码。



如果 PIN 正确，则在窗口中显示证书主题。

如果不支持智能卡，则显示错误消息。



阅读下一节了解关于智能卡支持相关细节。

2.5 配置选项

IT 经理可以选择几种智能卡，例如：可能强迫使用一种特定 PKCS#11 中间件。使用这些选项需要管理权限。

- /addmiddleware:[path_to_middleware.dll]

手动设置客户端必须使用的 PKCS#11 DLL 路径。

- /checkkeyusage:[yes|no]

缺省情况下，TheGreenBow VPN 客户端不检查 X509 密钥使用扩展。

如果使用“yes”，则 VPN 客户端将只寻找那些具有数字签名(DIGITAL_SIGNATURE)密钥使用的证书。

此参数只用于从智能卡读取的证书。

3 使用微软证书服务器

在此节，我们给出生成一个用户证书、对签署证书申请以及使用**微软证书服务器**导出证书的完整步骤。

3.1 安装微软证书服务器

微软证书服务器作为 Windows NT/2000/2003 服务器可选包的一部分。在使用前，证书服务器需要 Microsoft Internet Information 微软互联网信息服务器 (IIS) 及 Microsoft Internet explorer 微软互联网浏览器(IE)。

证书服务提供的注册 Web 网页允许你使用一个网页浏览器连接到服务并且执行通常的任务，如请求证书机构、处理一个证书请求文件或处理一个智能卡注册文件。网页位于 <http://ServerName/CertSrv>，其中 ServerName 为 CA 发布机器的名字。

关于在 Windows 2000 服务器上配置微软证书服务的相关信息，参见以下 URL：

- 关于建立一个证书机构，参见：
<http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp>
- 关于微软证书服务网页，参见：
<http://www.microsoft.com/windows2000/techinfo/planning/security/cawebsteps.asp>
- 关于管理微软证书服务，参见：
<http://www.microsoft.com/windows2000/techinfo/planning/security/adminca.asp>

以下我们提供了使用 Windows 2003 Server 系统的用独立根 CA 安装 Internet Information Server 互联网信息服务器 (IIS 6.0) 和 Microsoft Certificate Server 微软证书服务器(MCS)所需的步骤。

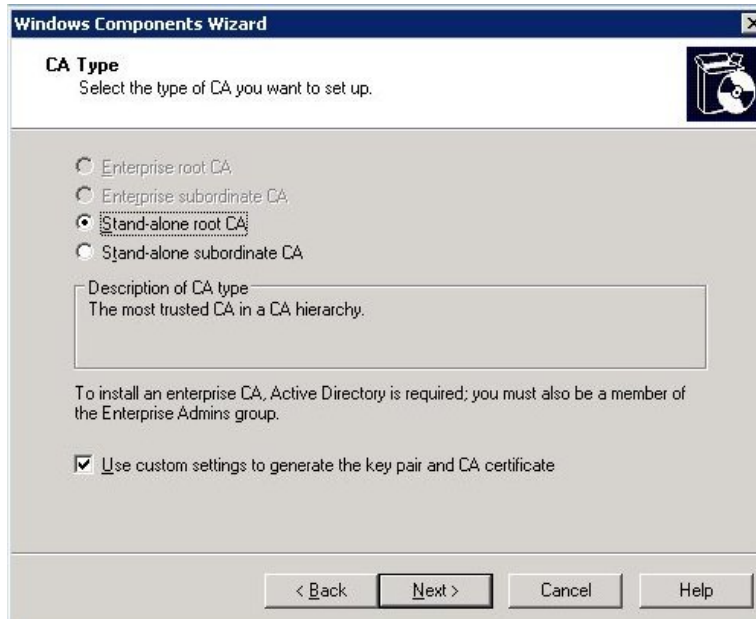
Microsoft Internet Information Server 微软互联网信息服务器安装步骤如下：

- 点击**启动**，指向**控制面板**并点击**添加或移除程序**。
- 在**添加/移除程序**窗口中点击**添加/移除 Windows 组件**按钮。
- 在**Windows 组件**窗口，点击**应用服务器**输入并点击**细节**按钮。
- 在**应用服务器**页面，点击 Internet Information Services (IIS)输入并点击**细节**按钮。
- 在 Internet Information Services (IIS)对话框中，选中 World Wide Web Service 复选框并点击 OK。
- 点击**应用服务器**对话框上的 OK。
- 点击 Windows **组件**对话框上的**下一步**按钮。
- 点击完成 Windows **组件向导**网页上的**完成**按钮。

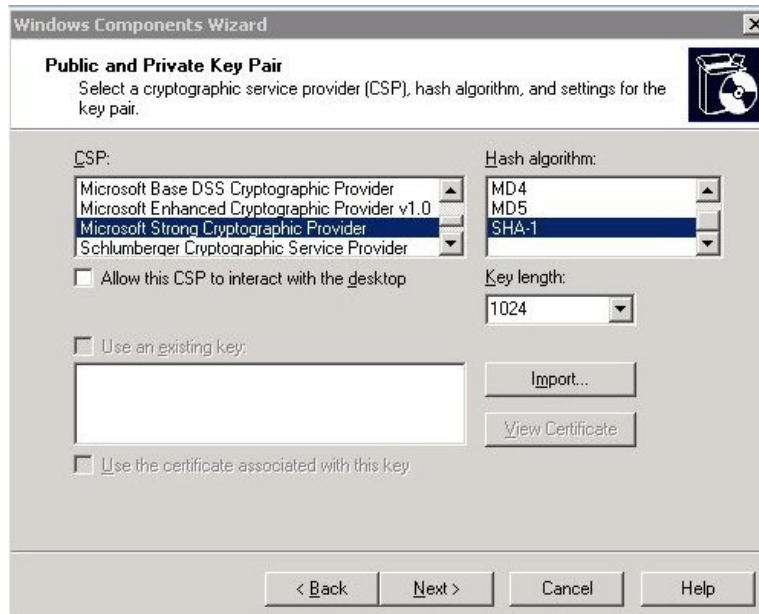
使用独立的根 CA 安装微软证书服务器的步骤：

- 点击**启动**，指向**控制面板**并点击**添加/移除程序**。
- 在**添加或移除程序**窗口中点击**添加/移除窗口组件**按钮。
- 在**Windows 组件**窗口，点击**证书服务**输入并点击**细节**按钮。
- 在**证书服务**对话框中，选中**证书服务 CA**复选框。

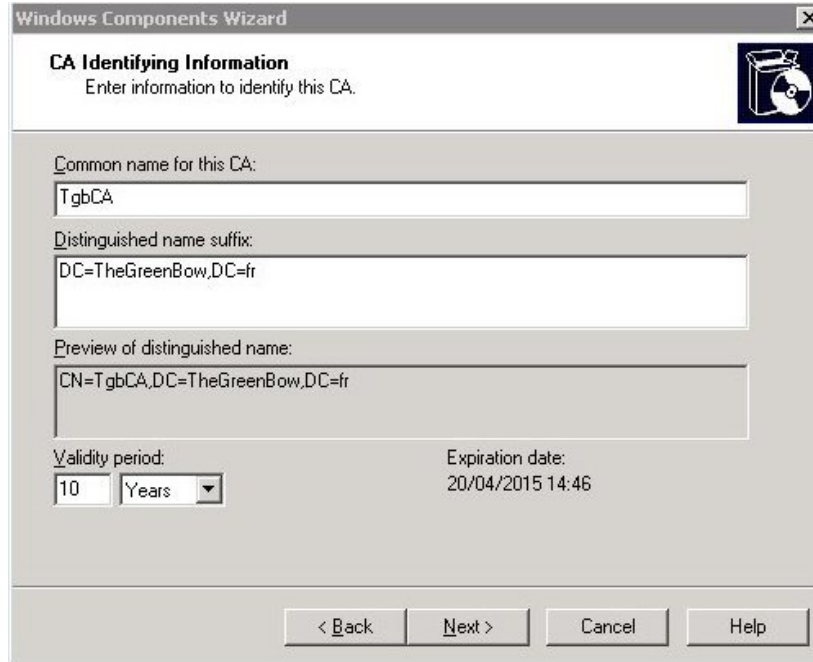
- 证书服务 CA 及证书服务 Web 注册支持复选框选中，点击证书服务对话框中的 OK。
- 点击 Windows 组件对话框上的下一步按钮。
- 如下所示，更新 CA 类型网页并点击下一步按钮。



- 如下所示，更新/定制公钥及私钥页面并点击下一步按钮。



- ▣ 如下所示，更新/定制 CA 确定信息网页并点击下一步按钮。



- ▣ 在证书数据库设置页面，使用证书数据库及证书数据库日志缺省位置。你不需要指定一个共享文件夹以存贮配置信息，因为此信息将被存贮在活动目录中，然后点击下一步按钮。
- ▣ 点击微软证书服务对话框上的 YES 按钮，可以通知你 IIS 互联网信息服务必须临时停止。
- ▣ 点击微软证书服务对话框上的 YES 按钮，可以通知当你希望使用证书服务 Web 注册站点时，激活服务器网页必须在 IIS 上启用。
- ▣ 点击完成 Windows 组件向导网页上的完成按钮。
- ▣ 关闭添加或移除程序窗口。

3.2 生成证书

在此节中，我们提供生成一个用户证书并签名证书请求的完整步骤。

3.2.1 生成一个用户证书

此节描述了 TheGreenBow VPN IPSec 客户端的用户证书生成。此节适用于任何其它 VPN IPSec 端点，像一个 VPN 路由器。

为了生成一个用户证书，步骤如下：

- ▣ 连接到证书服务器 (<http://ServerName/CertSrv>，其中 ServerName 是 CA 发布机器的名字)。

- 点击欢迎页面上的**请求一个证书**按钮。
- 点击**请求一个证书**页面上的**高级证书请求**按钮。
- 点击**高级证书请求**页面上的**创建并向此 CA 提交一个请求**按钮。
- 填写高级证书请求页面（样本显示如下）。你必须选中 **Mark keys as exportable 标记密钥可导出**，因为 TheGreenBow VPN IPsec 客户端需要一个证书私钥以建立一个隧道，然后点击**提交**按钮。

Microsoft Certificate Services -- TgbCA [Home](#)

Advanced Certificate Request

Identifying Information:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Type of Certificate Needed:

Key Options:

Create new key set Use existing key set

CSP:

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 16384 (common key sizes: 512 1024 2048 4096 8192 16384)

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

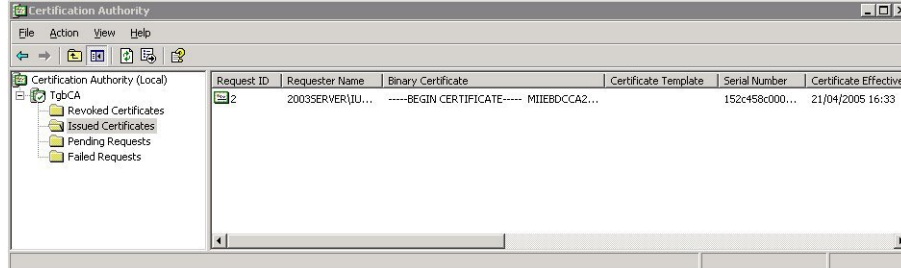
Hash Algorithm:
Only used to sign request.

Save request to a file

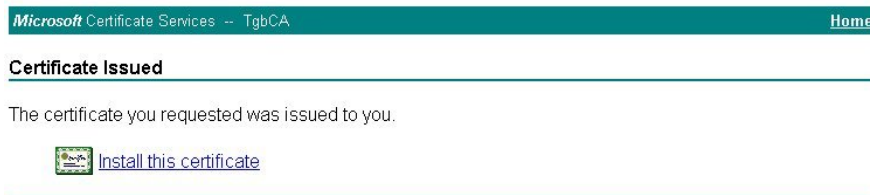
Attributes:

Friendly Name:

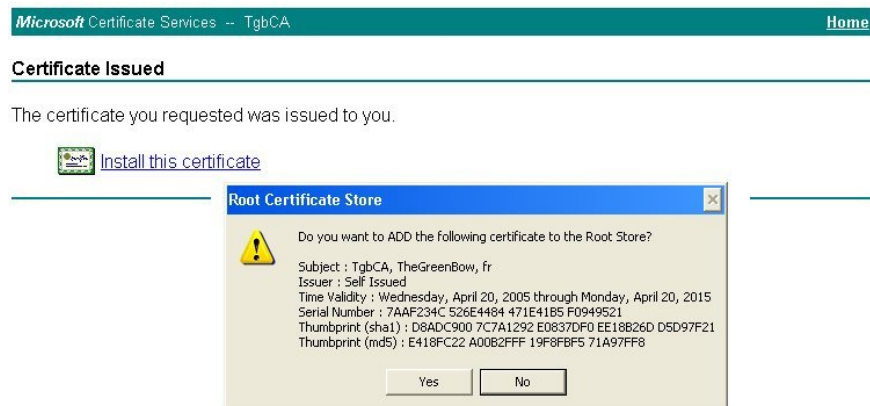
在处理完之后，**证书待定**页面出现。你必须等待直到你的请求被接受并且被微软证书服务器管理员验证。



- ❑ 为了查找证书，返回微软证书服务器主页并点击浏览待定证书请求的状态。
- ❑ 在浏览待定证书请求的状态页面上，选择你想浏览的请求。
- ❑ 证书发布页面显示如下：



为了将当前证书添加到你的本地证书存储库中，点击**安装此证书**。



在处理完后，已安装页面出现以确认 Internet Explorer 证书存储库中证书成功安装。

Certificate Installed

Your new certificate has been successfully installed.

如果需要从 Internet Explorer 证书存储库中导出一个证书，参见 3.3 节。

3.2.2 签署证书申请

如果需要使用微软证书服务器对签署证书申请，步骤如下：

- ❑ 连接到证书服务器(<http://ServerName/CertSrv>，其中 ServerName 是 CA 发布机器的名字)。
- ❑ 点击欢迎页面上的**请求一份证书**按钮。
- ❑ 点击**请求一份证书**页面上的**高级证书请求**按钮。
- ❑ 使用一个 base-64 编码的 CMC 或 PKCS #10 文件，点击**提交一个证书请求**，或使用一个 base-64 编码 PKCS #7 文件**提交一个更新请求**。
- ❑ 点击**浏览一个要插入的文件**并且浏览证书请求文件，然后点击 **Read 读取!**按钮。**提交一个证书请求或更新请求**页面如下所示：

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBpDCCAQCAQAwIjEgMB4GA1UEAwXen14ZUwx
gZ8wDQYJKoZIhvcNAQEBBQADgYOAAMIGJAoGBAM7c
44igK119Zw3Y+CVm9uiyD1IXS3v8yyWq9yvCqDpT
y8mfEwORvPNWkBktSKHpbuiyD/1igWHs1JTh13Lr
XXCYAR0WtdecFmWDAgMBAAGGQjBABGkqhkiG9w0B

```

[Browse for a file to insert.](#)

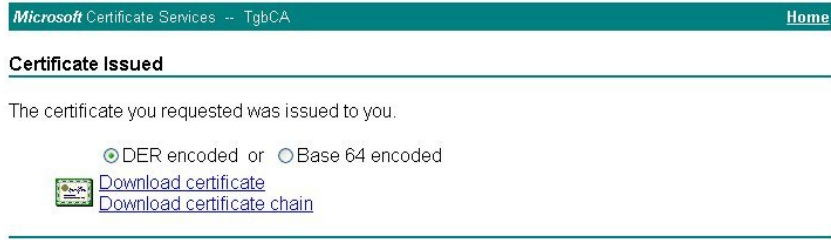
Additional Attributes:

Attributes:

点击**提交**。

在处理完之后，**证书待定**页面出现。你必须等待直到你的请求被接受并且被微软证书服务器管理员验证。

- ❑ 为了查找证书，返回微软证书服务器主页并点击**浏览待定证书请求的状态**。
- ❑ 在**浏览待定证书请求的状态**页面上，选择你想浏览的请求。
- ❑ 如下所示，**证书发布**页面出现。



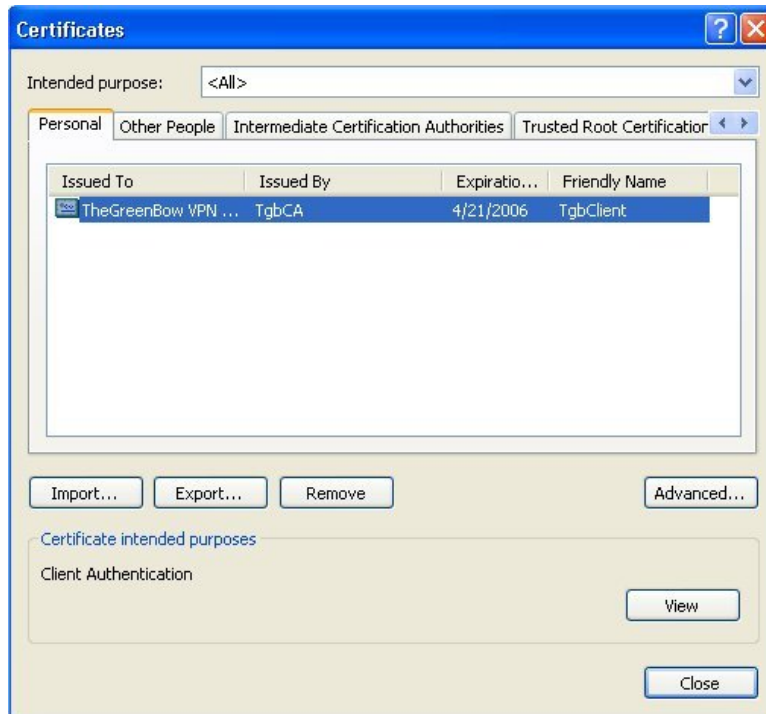
- 点击下载证书，弹出文件下载，按下保存按钮（缺省名字为 certnew.cer）。

3.3 证书导出

在 Internet Explorer 证书存储中已安装的证书可以使用 PKCS12 文件格式导出。

如果要从 Internet Explorer 证书存储中导出证书，步骤如下：

- 运行 Internet Explorer。
- 在工具菜单中打开 Internet 选项…。
- 选择目录标签，然后点击证书按钮。
- 在证书对话框中，打开个人标签，选择导出的证书，如下所示。



- 点击导出…。
- 在证书导出向导上，点击下一步。
- 在导出私钥窗口上，选择 YES，根据 TheGreenBow VPN IPSec 客户端的需要导出私钥。



- 在导出文件格式页面，选择“如果可能，包括认证路径中的所有证书”。也可以根据 TheGreenBow VPN IPSec 客户端需要导出根 CA。



- 点击下一步。
- 在密码页面上，输入并确认密码，然后点击下一步。
- 在导出文件页面，指定目标文件路径，然后点击下一步。
- 在完成证书导出向导窗口上，点击完成。

	文件参考	tgbvpn_certificates_zh
	文件版本	2.0 – 2006 年 6 月
	VPN 版本	4.00

4 使用 OpenSSL

OpenSSL 是一种免费的非商业工具包，可以提供各种密码操作。同时也包括证书管理工具。关于构建和使用 OpenSSL 的细节，访问<http://www.openssl.org>。

由于 openssl 程序是一个命令行工具，我们为证书生成及管理写了几个批处理脚本。例如：将 TgbSmallPKI.zip 文件解压缩到 C:\TgbSmallPKI（在以下章节中，我们将假设此路径为我们的工作文件夹）。工作文件夹包括：

- RootCA.bat:产生一个自签名的根证书。
- UserCA.bat:生成一个由根证书签名的用户证书。
- Pkcs12.bat:将 P12 文件转换到 PEM 文件。
- CAinfo.bat:显示一个 PEM 证书信息。
- CAsign.bat:签名一个证书请求。
- \Bin 文件夹包括：
 - openssl.cnf:证书内容主要取决于此配置文件的内容。此文件夹可以分成几个部分，这样有助于使配置文件模块化。你可以根据需要定制此文件（参见 OpenSSL 文档以了解细节）。
 - openssl.exe, libeay32.dll 及 ssleay32.dll 为 Windows 平台的主要工具包。
- ReadME.txt:文档文件。

4.1 生成证书

在下面部分，我们将显示如何生成一个自签名的根证书和一个用户证书并且使用 OpenSSL for Windows 对证书请求进行签名。

4.1.1 生成一个自签名的证书

自签名证书为非认可的证书机构签名的证书。自签名证书可以用于证书机构进行证书发布、更新及撤消。

如果需要创建一个自签名证书，运行 RootCA，以下为输出样本：

```

*
! Creating Root CA folders
*
Root CA folder set to .\RootCA
Root CA key length is 1024 bits
Root CA validity is 3650 days
The system cannot find the file specified.

*
! Creating CA private key (1024 bits, 3650 days)
*
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++

```

	文件参考	tgbvpn_certificates_zh
	文件版本	2.0 – 2006 年 6 月
	VPN 版本	4.00

```

.+++++
e is 65537 (0x10001)

*
! CA autosigning (1024 bits, 3650 days)
*

Using configuration from .\Bin\openssl.cnf
You are about to be asked to enter information that will be incorporated
into your Certificate Request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:FR
State or Province Name (full name) [France]:France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [TheGreenBow]:TheGreenBow
Organizational Unit Name (eg, section) []:Authority Certificate
Common Name (eg, YOUR name) []:TheGreenBow CA
Email Address []:TgbCA@thegreenbow.fr

Please enter the following 'extra' attributes
to be sent with your Certificate Request
A challenge password []:capassword
An optional company name []:TheGreenBow
Loading 'screen' into random state - done
Signature ok
subject=/C=FR/ST=France/L=Paris/O=TheGreenBow/OU=Authority Certificate/CN=TheGreenBow CA/Email=TgbCA
@thegreenbow.fr
Getting Private key

"-----"
"-----"

Root Certificate at .\RootCA\RootCA.pem
Root Private Key at .\RootCA\CAKey.key

```

根证书 RootCA.pem 及其私钥 CAKey.key 位于 RootCA 文件夹中。

4.1.2 生成一个用户证书

当在 IKE 中选择 X.509 证书认证时，则使用用户证书以确定 VPN IPsec 终端点并且进行签名/验证操作。

UserCA 脚本生成一个用户证书、私钥及 PKCS12 文件，其要求中间文件夹作为一个参数，其可以用于为所有 VPN IPsec 端点生成证书。

如果需要为 TheGreenBow VPN IPsec 客户端生成所有所需的文件，运行 UserCA TgbClient。

```

*
! Creating User CA folder
*

```



文件参考	tgbvpn_certificates_zh
文件版本	2.0 – 2006 年 6 月
VPN 版本	4.00

Creating User Certificate folder at .\TgbClient
User CA key length is 1024 bits
User CA validity is 3650 days

*

! Creating User CA private key (1024 bits)

*

Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

*

! Signing User CA

*

Using configuration from .\Bin\openssl.cnf
You are about to be asked to enter information that will be incorporated
into your Certificate Request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [FR]:FR
State or Province Name (full name) [France]:France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [TheGreenBow]:TheGreenBow
Organizational Unit Name (eg, section) []:VPN
Common Name (eg, YOUR name) []:TheGreenBow VPN Client
Email Address []:TgbClient@thegreenbow.fr

Please enter the following 'extra' attributes
to be sent with your Certificate Request
A challenge password []:tgbcapwd
An optional company name []:TheGreenBow
Loading 'screen' into random state - done
Signature ok
subject=/C=FR/ST=France/L=Paris/O=TheGreenBow/OU=VPN/CN=TheGreenBow VPN
Client/Email=TgbClient@thegreenbow.fr
Getting CA Private Key

*

! User CA in P12 Format

*

Loading 'screen' into random state - done
Enter Export Password:
Verifying password - Enter Export Password:
TgbClient.p12 created in .\TgbClient.p12

"-----"
"-----"

User Certificate at .\TgbClient\TgbClient.pem
User Private Key at .\TgbClient\local.key
User Certificate Subject is:
subject= /C=FR/ST=France/L=Paris/O=TheGreenBow/OU=VPN/CN=TheGreenBow VPN
Client/Email=TgbClient@thegreenbow.fr

	文件参考	tgbvpn_certificates_zh
	文件版本	2.0 – 2006 年 6 月
	VPN 版本	4.00

TgbClient 文件夹中最相关的文件包括：

- TgbClient.pem:用户证书
- Local.key:用户证书私钥
- Subject.txt:用户证书主题
- TgbClient.p12: PKCS12 文件格式，包括用户及根证书以及用户证书私钥。

4.2 其它 TgbSmallPKI 工具

在下列部分我们将显示如何显示证书信息以及如何从 PKCS12 格式文件提取证书及私钥。

- Pkcs12.bat:转换 P12 文件到 PEM 文件
- CAinfo.bat:显示 PEM 证书信息。

4.2.1 显示证书信息

显示证书信息可以用助于查找几个域，如发布人、有效期及主题。

CAinfo 脚本显示用户证书信息，其要求证书文件作为一个参数。

如果需要显示关于 TgbClient.pem 的更多信息（4.1.2 中生成的 TheGreenBow 用户证书），运行 CAinfo TgbClient\TgbClient.pem：

```

*
! Certificate TgbClient\TgbClient.pem information
*

Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=FR, ST=France, L=Paris, O=TheGreenBow, OU=Authority Certificate, CN=TheGreenBow CA
    /Email=TgbCA@thegreenbow.fr
    Validity
      Not Before: Apr 19 12:44:03 2005 GMT
      Not After: Apr 17 12:44:03 2015 GMT
    Subject: C=FR, ST=France, L=Paris, O=TheGreenBow, OU=VPN, CN=TheGreenBow VPN Client/Email=Tg
    bClient@thegreenbow.fr
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:ac:00:2c:1b:82:6d:32:2e:17:09:9f:13:8d:b9:
        9f:9b:db:d7:3f:f7:45:9b:f2:73:6d:8b:3d:9b:b1:
        14:99:25:22:fb:a8:56:30:9d:68:43:e9:14:84:6f:
        4c:24:fa:e2:36:84:56:2d:b2:5c:11:fd:be:b9:9e:
        ed:49:c8:c1:08:29:d0:17:ca:b8:12:41:41:55:4d:
        48:01:57:bc:22:9a:c9:48:ca:e2:c2:59:2c:78:8d:
        6d:cc:89:09:3a:97:f5:f4:b7:96:ea:da:82:0e:8c:

```

87:49:a7:45:a4:74:45:31:8e:ac:be:9a:a2:8c:a1:
16:be:f7:46:4a:94:78:31:73


Exponent: 65537 (0x10001)

Signature Algorithm: md5WithRSAEncryption

b2:ba:7c:92:9c:eb:59:c2:7e:d9:95:af:71:8b:06:2f:b8:44:
b3:b5:2a:b7:98:0b:1e:08:97:85:c7:bc:21:1c:cf:df:15:97:
d9:4f:e5:ec:31:14:6f:9e:b1:8a:47:37:ad:6b:4b:c8:15:bf:
cd:8a:1b:ed:a5:f7:3e:ac:72:73:b9:bc:f6:22:b3:05:f5:26:
40:dd:f8:4c:83:3f:25:da:68:32:8b:bd:1b:68:24:e8:df:31:
83:5b:74:91:10:1f:6a:d0:b9:3c:f3:04:50:4c:6e:ce:c9:de:
3a:38:fe:2d:ad:6c:6b:e6:74:38:51:0c:5b:c5:bb:6b:05:25:
44:d9

5 故障排除

在我们网站上的故障排除文档（pdf）中，你能找到所有故障排除相关问题。通过访问 www.thegreenbow.com/vpn_doc.html 可以获取此文档。

	文件参考	tgbvpn_certificates_zh
	文件版本	2.0 – 2006 年 6 月
	VPN 版本	4.00

6 联系我们

信息及更新网址：<http://www.thegreenbow.com>

技术支持联系电子邮箱：support@thegreenbow.com

销售电话：+33 1 43 12 39 37，电子邮箱：sales@thegreenbow.com