Certificate 为 SEQUENCE 结构类型，编码规则采用结构类型定长模式。

Certificate 具体编码过程如表 13-10 所示。

表 13-10　Certificate 编码过程

Certificate	标识串	长度串	内　容　串
Certificate	30	82 02 EC	30 82…B0 F9：tbsCertificate 30 0D…05 00：signatureAlgorithm 03 82…CC 81：signatureValue

该数字证书 DER 编码后的文件大小为 752 字节，具体二进制值如表 13-11 所示。其中，每行显示 16 个字节，每行最前面 4 个数字表示该行第 1 个字节的地址序号（从 0 开始）。

表 13-11　数字证书 DER 文件内容

```
0000: 30 82 02 EC 30 82 01 D4 -- A0 03 02 01 02 02 02 04
0010: 96 30 0D 06 09 2A 86 48 -- 86 F7 0D 01 01 05 05 00
0020: 30 22 31 0B 30 09 06 03 -- 55 04 06 13 02 43 4E 31
0030: 13 30 11 06 03 55 04 03 -- 13 0A 56 69 72 74 75 61
0040: 6C 20 43 41 30 1E 17 0D -- 31 34 30 32 32 31 31 36
0050: 30 30 30 30 5A 17 0D 31 -- 36 30 32 32 31 31 36 30
0060: 30 30 30 5A 30 32 31 0B -- 30 09 06 03 55 04 06 13
0070: 02 43 4E 31 0F 30 0D 06 -- 03 55 04 0B 13 06 50 65
0080: 72 73 6F 6E 31 12 30 10 -- 06 03 55 04 03 13 09 5A
0090: 48 41 4E 47 20 53 61 6E -- 30 81 9F 30 0D 06 09 2A
00A0: 86 48 86 F7 0D 01 01 01 -- 05 00 03 81 8D 00 30 81
00B0: 89 02 81 81 00 B4 F6 CF -- 18 3D 5E 8E 1D 46 7A 90
00C0: 7D 8E 41 D2 E3 C8 F1 A3 -- AE F3 6D 8A 24 FF 55 23
00D0: 25 BD EB 0C D0 7B 87 36 -- 5D 1F 73 98 65 3E 57 97
00E0: F6 65 7D 13 E0 E1 B5 FC -- BC 38 6F 56 3E 57 4E D6
00F0: 51 1D 13 12 7C 33 B3 60 -- 31 79 32 07 97 F3 3C 8B
0100: 29 0D B5 78 38 93 CE 84 -- E4 A3 DD FB F9 25 47 1C
0110: 72 A6 5E 78 02 CF F3 48 -- 9D CA D9 00 73 DE 4B 16
0120: 07 52 48 20 06 F3 4F CA -- A5 2D 66 88 95 C6 6C D6
0130: 3F 61 34 F7 E3 02 03 01 -- 00 01 A3 81 9F 30 81 9C
0140: 30 0C 06 03 55 1D 13 01 -- 01 FF 04 02 30 00 30 1D
0150: 06 03 55 1D 0E 04 16 04 -- 14 2C 04 87 10 60 FC 61
0160: F6 2B 64 81 3D FB 66 30 -- DA F0 73 BC 08 30 0E 06
0170: 03 55 1D 0F 01 01 FF 04 -- 04 03 02 03 F8 30 29 06
0180: 03 55 1D 25 04 22 30 20 -- 06 08 2B 06 01 05 05 07
0190: 03 02 06 0A 2B 06 01 04 -- 01 82 37 14 02 02 06 08
01A0: 2B 06 01 05 05 07 03 04 -- 30 11 06 09 60 86 48 01
01B0: 86 F8 42 01 01 04 04 03 -- 02 05 A0 30 1F 06 03 55
01C0: 1D 23 04 18 30 16 80 14 -- 96 F0 94 F8 49 8D 23 05
01D0: 86 B0 CA B5 2D 7A 9A 60 -- 32 FB B0 F9 30 0D 06 09
01E0: 2A 86 48 86 F7 0D 01 01 -- 05 05 00 03 82 01 01 00
01F0: 8D 42 AD 5C DF C7 C7 90 -- FA 58 C0 74 15 C6 4F 20
0200: 9B F1 49 9C B8 3C 22 98 -- 45 75 A6 0D 7C 02 9D 83
0210: 1D C4 5D CF 4F 8E 57 E7 -- 0A 9B 67 02 33 23 59 76
```

（续表）

```
0220: B4 B5 B7 F3 27 36 6F F4 -- 32 6C 1C E9 B3 4B 81 DC
0230: D0 CF 2E CF 07 4C 65 75 -- 74 DF 23 9D 7D 2B E4 F1
0240: 15 0C 84 61 41 5F DC 67 -- 92 A9 7C 39 A0 CA A9 58
0250: 6B ED 7D 94 08 F7 83 42 -- 61 F8 62 D8 DC 3B 5D B7
0260: 69 5C D0 36 F2 99 A8 0C -- 99 6E B0 0C 21 E3 98 9F
0270: 12 6D D1 76 4E 0C 31 CB -- 7F 54 73 FE 96 83 76 35
0280: 22 2F BF F6 2B 11 04 3A -- A7 BE 33 3C D5 DA EE 56
0290: 7A C4 1A 67 3B 77 DE 52 -- C0 DA 09 CA 45 71 11 B2
02A0: D5 35 BF 44 54 08 C2 FA -- 0C 5C EF C0 EF 82 63 37
02B0: 3C 4C AB 59 4C FD 6C 2A -- 9D 64 27 35 4E 4F D8 2E
02C0: 2C 5C EB A1 99 DB FA 3A -- 53 54 13 92 91 5D 8F 38
02D0: DD 1C D8 AB 34 22 9A EF -- 8A E4 62 C2 23 9D 06 A5
02E0: D7 D8 58 B7 F4 98 CA 61 -- 29 9D DE A8 F6 DA CC 81
```

13.3　Windows 证书库操作示例

13.3.1　查看证书库内容

1．进入证书库

打开 IE 浏览器，单击菜单“Internet 选项”后进入“内容”页，单击“证书”按钮即可进入证书库界面，如图 13-1 所示。

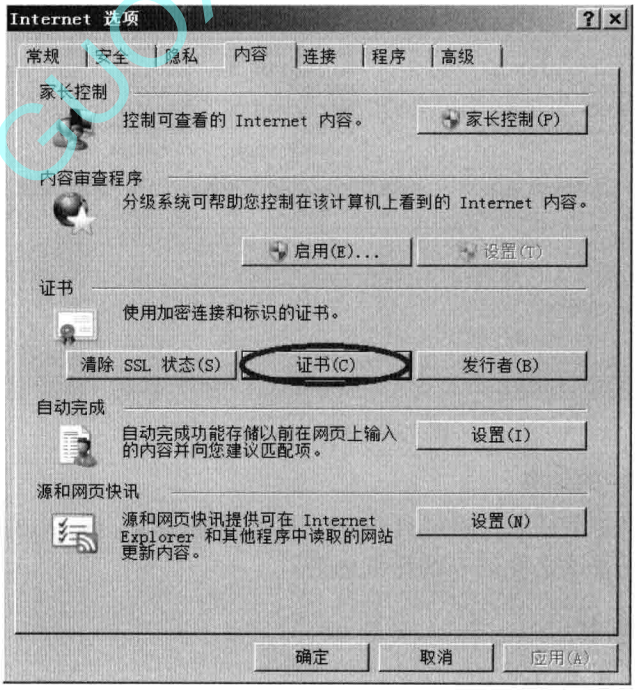

图 13-1　IE 浏览器 Internet 选项

2. 查看证书库

Windows 证书库分为以下几类：

（1）受信任的根证书颁发机构

保存多个可信任的根 CA 证书。通过该类证书可以验证用户证书或子 CA 证书的合法性。

（2）中级证书颁发机构

保存多个子 CA 证书。

（3）受信任的发布者

保存多个可信任的可执行代码发布者证书。如果某可执行程序具有代码签名，且使用该类证书能验证代码签名的合法性，则说明该程序值得信赖。

（4）未受信任的发布者

保存多个不受信任的可执行代码发布者证书。如果某可执行程序具有代码签名，且使用该类证书能验证代码签名的合法性，则说明该程序不受信任，可能存在安全风险，不建议安装或使用。

（5）其他人证书

保存多个他人的证书。

（6）个人证书

包含自己的数字证书，如果有对应的私钥，则与其关联。

单击不同的标签页即可进入不同的证书库，如图 13-2 所示。

图 13-2　Windows 证书库

3. 查看证书库中的证书

双击证书库中的某个证书，即可查看该证书的详细内容，如图 13-3 所示。双击某个证书文件名称，也可查看该文件证书的详细内容。

13.3.2　导入证书

进入证书导入向导有两种方法。

方法一：在证书库查看界面中（见图 13-2），单击“导入”按钮后进入证书导入向导。

方法二：双击某个证书文件名称，将进入该证书详细内容查看界面，单击“安装证书”按钮后进入证书导入向导，如图 13-4 所示。

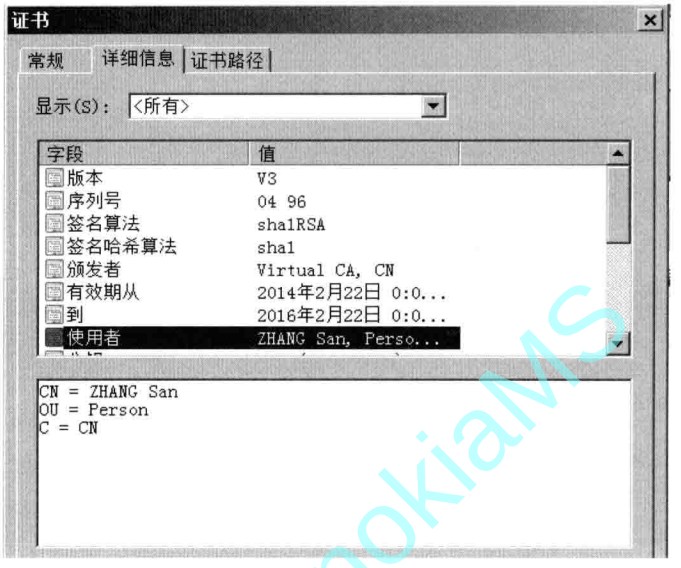

图 13-3　数字证书详细内容查看

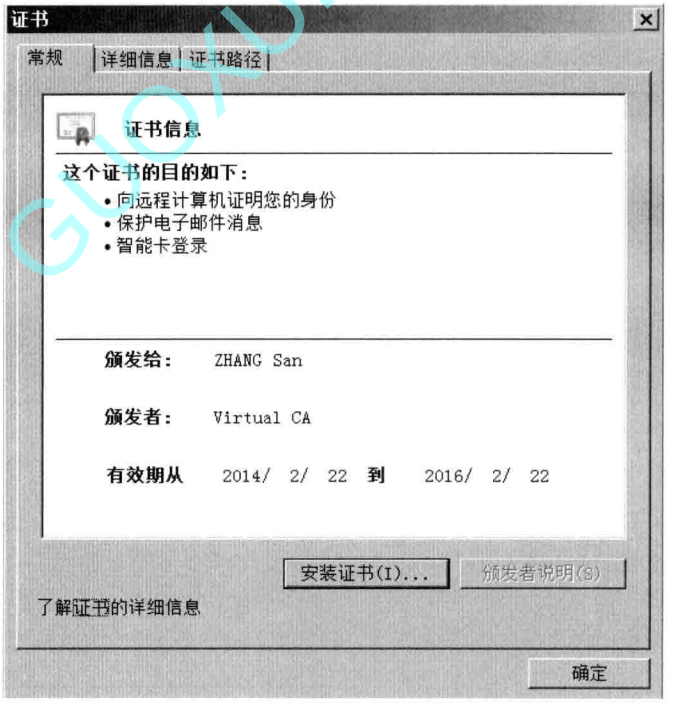

图 13-4　通过查看文件证书进入证书导入向导

首先，选择需要导入的证书文件名称，如图 13-5 所示。支持的证书文件类型包括 PKCS#12（P12 或 PFX）、PKCS#7（P7B）、CER 或 DER 等。

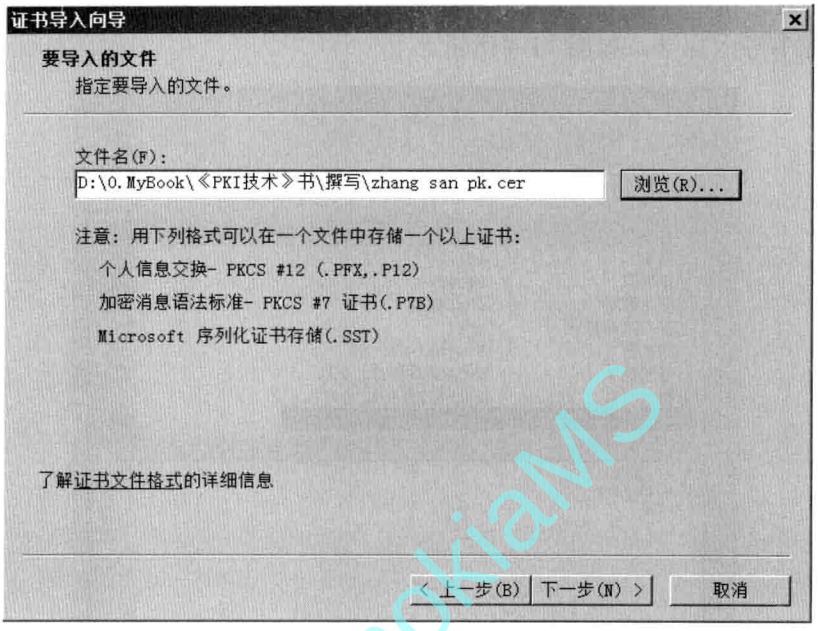

图 13-5　导入证书时证书文件名称选择

然后，设置证书存储位置选择方式，如图 13-6 所示。支持两种选择方式：根据证书类型自动选择和手工选择。

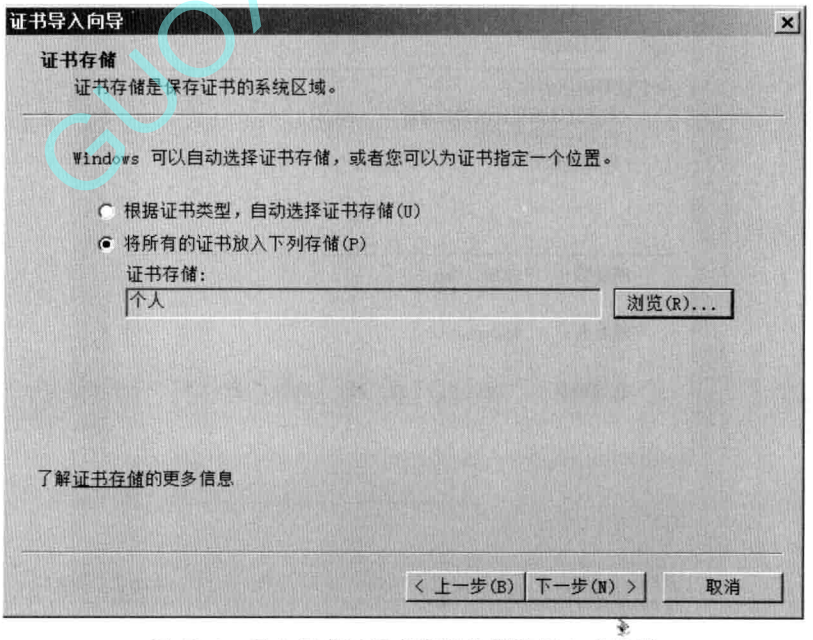

图 13-6　导入证书时证书存储位置选择方式设置

单击“浏览”按钮后，可手工选择证书存储位置，如图 13-7 所示。