表 11-1　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
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
```

GUOXUnotes

将该表内容恢复成二进制文件，取文件后缀为 cer 或 crt，在 Windows 环境下鼠标双击即可查看该数字证书的内容。

11.1.2 Base64 文件形式

由于数字证书 DER 编码后的内容为二进制形式，不方便显示，因此需要将其转换成文本形式，通常采用 Base64 编码方式。

例如，表 11-1 中所示 ZHANG San 的数字证书 Base64 编码后，长度由 752 字节变成 1004 字符，如表 11-2 所示。

表 11-2 数字证书 Base64 文件内容

```
MIIC7DCCAdSgAwIBAgICBJYwDQYJKoZIhvcNAQEFBQAwIjELMAkGA1UEBhMCQ04x
EzARBgNVBAMTClZpcnR1YWwgQ0EwHhcNMTQwMjIxMTYwMDAwWhcNMTYwMjIxMTYw
MDAwWjAyMQswCQYDVQQGEwJDTjEPMA0GA1UECxMGUGVyc29uMRIwEAYDVQQDEwla
SEFORyBTYW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALT2zxg9Xo4dRnqQ
fY5B0uPI8aOu822KJP9VIyW96wzQe4c2XR9zmGU+V5f2ZX0T4OG1/Lw4b1Y+V07W
UR0TEnwzs2AxeTIHl/M8iykNtXg4k86E5KPd+/klRxxypl54As/zSJ3K2QBz3ksW
B1JIIAbzT8qlLWaIlcZs1j9hNPfjAgMBAAGjgZ8wgZwwDAYDVR0TAQH/BAIwADAd
BgNVHQ4EFgQULASHEGD8YfYrZIE9+2Yw2vBzvAgwDgYDVR0PAQH/BAQDAgP4MCkG
A1UdJQQiMCAGCCsGAQUFBwMCBgorBgEEAYI3FAICBggrBgEFBQcDBDARBglghkgB
hvhCAQEEBAMCBaAwHwYDVR0jBBgwFoAUlvCU+EmNIwWGsMq1LXqaYDL7sPkwDQYJ
KoZIhvcNAQEFBQADggEBAI1CrVzfx8eQ+ijAdBXGTyCb8UmcuDwimEV1pg18Ap2D
HcRdz0+OV+cKm2cCMyNZdrS1t/MnNm/0Mmwc6bNLgdzQzy7PB0xldXTfl519K+Tx
FQyEYUFf3GeSqXw5oMqpWGvtfZQI94NCYfhi2Nw7XbdpXNA28pmoDJlusAwh45if
Em3Rdk4MMct/VHP+loN2NSIvv/YrEQQ6p74zPNXa7lZ6xBpnO3feUsDaCcpFcRGy
1TW/RFQIwvoMXO/A74JjNzxMq1lM/WwqnWQnNU5P2C4sXOuhmdv6OlNUE5KRXY84
3RzYqzQimu+K5GLCI50GpdfYWLf0mMphKZ3eqPbazIE=
```

将该表内容恢复成文本文件，取文件后缀为 cer 或 crt，在 Windows 环境下鼠标双击即可查看该数字证书的内容。

11.1.3 PKCS#7 文件形式

为方便交换证书链（证书路径或认证路径）上的所有证书，需要将多个证书保存到单个文件中，通常采用 PKCS#7 编码形式。

当证书链采用 PKCS#7 文件形式保存时，常用的文件后缀为 p7b。

PKCS#7 定义了多种密码消息形式，主要包括：data、signedData、envelopedData、signedAndEnvelopedData、digestData、encryptedData、keyAgreementInfo 等。当用于保存证书链时，具体要求如下：

1. ContentInfo

```
ContentInfo ::= SEQUENCE {
    contentType    ContentType,
```

```
content     [0] EXPLICIT ANY DEFINED BY contentType OPTIONAL }
```

其中，contentType = signedData，content 为 SignedData 类型。

2．SignedData

```
SignedData ::= SEQUENCE {
    version Version,
    digestAlgorithms DigestAlgorithmIdentifiers,
    contentInfo ContentInfo,
    certificates    [0] IMPLICIT ExtendedCertificatesAndCertificates    OPTIONAL,
    crls    [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos }
```

其中，digestAlgorithms 为空；contentInfo→ contentType=data，contentInfo→content 可为空；certificates 包含证书链中的证书；crls 可忽略，signerInfos 可为空。

11.1.4　Windows 证书库形式

为加强对数字证书的分类管理，方便应用系统使用，方便用户操作和查看，Windows 提供了证书库机制。

1．证书库分类

Windows 证书库分为以下几类，如图 11-2 所示。

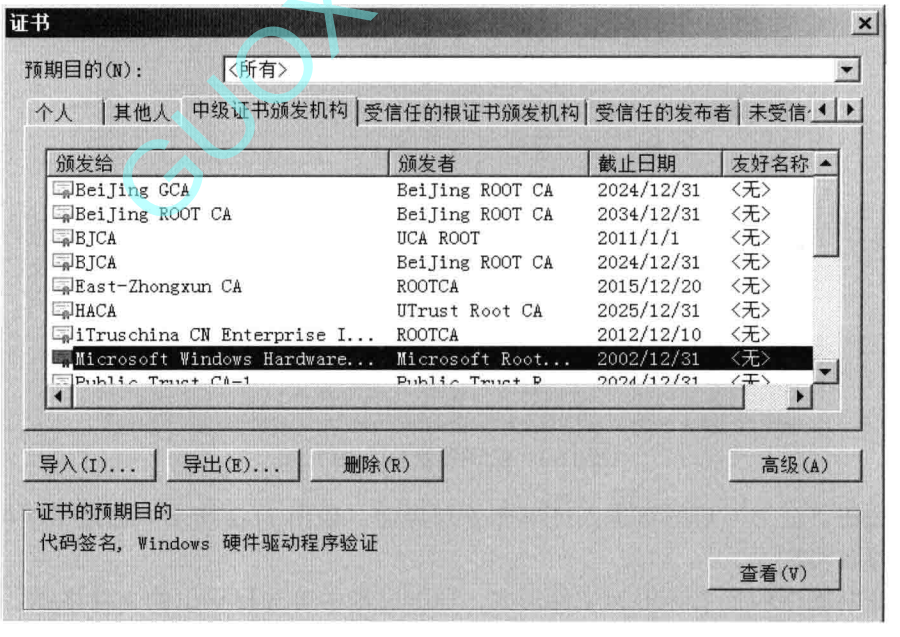

图 11-2　Windows 证书库

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。

SUOXU.nokiaNS

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，并与数字证书进行关联。

2. 证书库管理

打开 IE 浏览器，单击菜单“Internet 选项”后进入“内容”页，如图 11-3 所示。

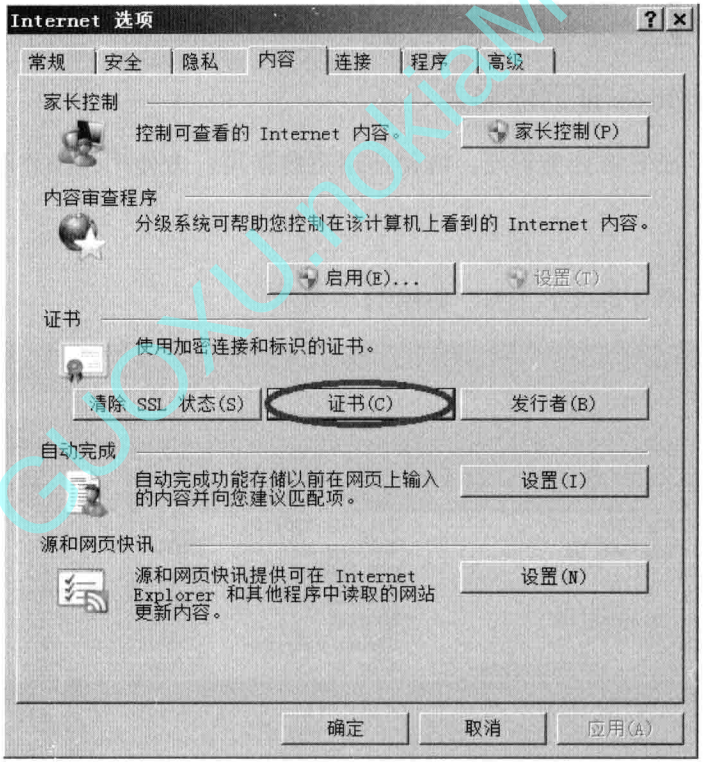

图 11-3　IE 浏览器 Internet 选项

单击按钮“证书”后即可进入证书库管理界面，如图 11-2 所示。通过手工可以导入、导出、删除各类证书。

可将证书库中的证书导出为文件形式，导出过程中可选择导出的文件格式：DER 编码二进制格式、Base64 编码格式、PKCS#7 格式，如图 11-4 所示。

其中，导出个人证书时，可以选择是否将私钥跟证书一起导出。如果选择导出私钥，则只能导出为 PKCS#12 格式文件。

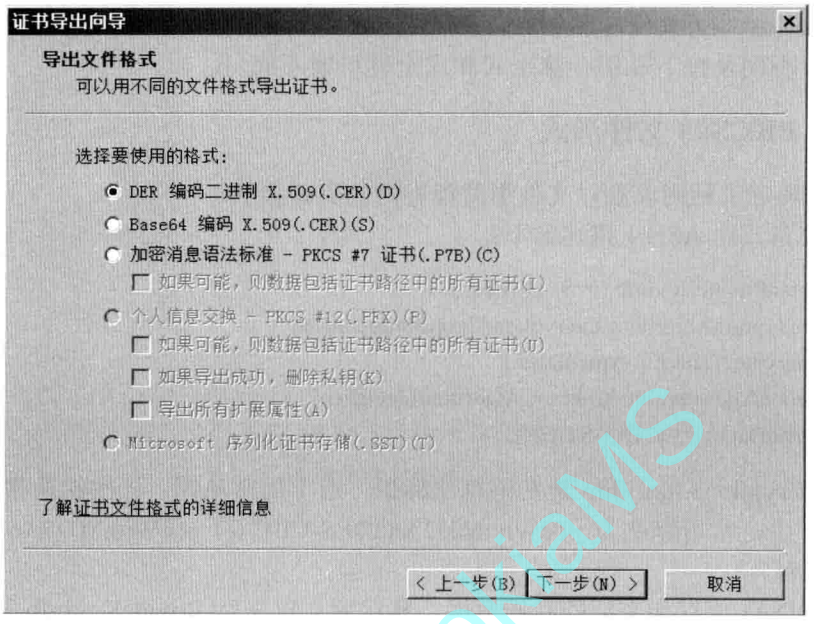

图 11-4　Windows 证书库导出证书格式

3．证书库访问

Windows CryptoAPI 包含证书库管理函数，允许应用系统直接访问证书库，主要包括以下 API 函数。

① CertOpenStore：根据证书库类型打开证书库；
② CertCloseStore：关闭证书库；
③ CertEnumCertificatesInStore：从证书库中枚举证书；
④ CertFindCertificateInStore：从证书库中查找指定的证书；
⑤ CertCreateCertificateContext：根据证书数据创建证书句柄；
⑥ CertFreeCertificateContext：释放证书句柄；
⑦ CertGetCertificateContextProperty：获取证书句柄属性；
⑧ CertSetCertificateContextProperty：设置证书句柄属性；
⑨ CertGetNameString：获得证书中签发者或持有者的 DN 项。

11.2　私钥保存形式

私钥保存形式主要包括：文件形式、密码设备形式和软件系统形式。

当采用文件形式保存私钥时，私钥的安全性通常采用口令进行保护，同时基于口令可对私钥文件进行加密存储。当系统使用私钥进行签名或解密时，需要将该私钥文件读入内存或密码模块中进行密码运算。为保护私钥的安全性，通常使用口令对私钥文件进行加密保护。

当采用密码设备形式保存私钥时，密码设备可提供安全机制保护私钥存储的安全性和私钥访问的安全性。

GUOXU.noxiaMS