CBWIPS

宽带无线IP标准工作组标准

CBWIPS/Z XXX—XXXX

WAPI 证书管理 第 5 部分：证书格式范例

WAPI certificate management—Part 5: Example of certificate format

（征求意见稿）

201x – xx – xx 发布　　201x – xx – xx 实施

工业和信息化部宽带无线 IP 标准工作组　发 布

目　　次

CBWIPS

版权声明

CBWIPS

前　言

本规范的附录A和B为规范性附录，附录C、D和E为资料性附录。

本指导性技术文件由工业和信息化部宽带无线IP标准工作组和WAPI产业联盟（中国计算机行业协会无线网络和网络安全接入技术专业委员会）共同提出，由工业和信息化部宽带无线IP标准工作组归口。

本指导性技术文件主要起草单位：工业和信息化部宽带无线IP标准工作组“WAPI证书管理标准项目组”暨WAPI产业联盟“WAPI证书管理产品方案组”（国家无线电监测中心、中国电信集团股份有限公司上海研究院、西安西电捷通无线网络通信股份有限公司、无锡中太数据通信有限公司、北京网贝合创科技有限公司、广州杰赛科技股份有限公司xx等）。

本指导性技术文件主要起草人：xxx等。

CBWIPS

引　　言

本标准为WAPI证书管理指导性技术文件系列的第5部分。

本标准列举了WAPI协议中所使用的X.509数字证书的格式范例，有利于指导符合WAPI协议的设备生产和方案研发，同时对进一步提高符合WAPI协议的产品的适用性也具有一定的指导意义。

WAPI证书管理指导性技术文件包括如下部分：

——第1部分 证书颁发技术；

——第2部分 证书/私钥存储和使用技术；

——第3部分 证书更新技术；

——第4部分 证书吊销技术；

——第5部分 证书格式范例。

本标准内容同国家已发布的标准保持一致性。本标准中所涉及到的X.509数字证书内容与中华人民共和国国家标准GB/T 20518-2006的关系如下：

a) 本标准中涉及的X.509数字证书的定义、结构和描述同GB/T 20518-2006完全一致；

b) 本标准为基于GB/T 20518-2006中所定义的X.509数字证书而列举的应用在WAPI协议中的具体格式范例。

本标准中未明确指明为可选要素的部分均为必备要素。

本标准实施过程中，涉及到密码技术的具体应用时，按照国家密码管理局的有关规定和相关规范执行。

WAPI 证书管理 第 5 部分：证书格式范例

1 范围

本标准根据GB/T 20518-2006所规定的X.509数字证书的基本结构，进一步描述了符合WAPI协议产品所使用的X.509数字证书中应包含的数据项及其定义，并且列举了具体的数字证书编码范例。

本标准适用于采用WAPI协议的设备生产商、运营商以及检测机构。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 15629.11—2003/XG1—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制(MAC)和物理(PHY)层规范 第1号修改单

GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式

GB/T 16262.1 信息技术 抽象句法表记法一(ASN.1)：基本记法规范（GB/T 16262.1-1996，idt ISO/IEC 8824-1:1995）

GB/T 16262.2 信息技术 抽象句法表记法一(ASN.1)：信息客体规范（GB/T 16262.2-1996，idt ISO/IEC 8824-2:1995）

GB/T 16262.3 信息技术 抽象句法表记法一(ASN.1)：限制规范(GB/T 16262.3-1996，idt ISO/IEC 8824-3:1995）

GB/T 16262.4 信息技术 抽象句法表记法一(ASN.1)：参数化ASN.1规范（GB/T 16262.4-1996，idt ISO/IEC 8824-4:1995）

GB/T 16263.1 信息技术 ASN.1编码规则：基本编码规则(BER)、正则编码规则(CER)和特异编码规则(DER)的规范（GB/T 16263.1-1996，idt ISO/IEC 8825-1:1995）

GB/T 16263.2 信息技术 ASN.1编码规则：包编码规则(PER)规范（GB/T 16263.2-1996，idt ISO/IEC 8825-2:1996）

《无线局域网产品密码算法应用指南》 国家密码管理局商用密码研究中心 2005年12月

《数字证书认证系统密码协议规范》 2007年8月13日国家密码管理局公告第11号

CBWIPS/Z 021-2010 无线局域网网络设备标识规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

公钥证书 public key certificate

用户的公钥连同其他信息，并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

3.2

证书序列号 certificate serial number

为每个证书分配的唯一整数值，在CA颁发的证书范围内，此整数值与该CA所颁发的证书相关联一一对应。

3.3

证书认证机构（CA） Certification Authority（CA）

负责创建和分配证书，受用户信任的权威机构。用户可以选择该机构为其创建密钥。

3.4

数字证书 digital certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行数字签名的一个可信的数字化文件。

3.5

鉴别服务器实体 authentication service entity

为鉴别控制器实体和接入请求者实体提供鉴别的实体。

4 缩略语

下列缩略语适用于本文件。

WAPI	无线局域网鉴别与保密基础结构
TLV	类型/长度/取值
OID	对象标识符
CA	证书认证机构
ECDSA	椭圆曲线签名
DER	特定编码规则
PEM	增强的保密邮件

5 概述

符合WAPI协议的设备应能正确解析X.509数字证书。

WAPI协议中规定采用的X.509数字证书为v3版本，其中签名算法为ECDSA-192，杂凑算法为SHA-256。公钥算法标识、签名算法标识以及椭圆曲线参数均采用OID方式表示。公钥算法字段利用OID值1.2.840.10045.2.1 标识椭圆曲线算法，并在密钥用途字段中标明为签名用途；签名算法字段利用OID值1.2.156.11235.1.1.1标识基于SHA-256的ECDSA-192算法；椭圆曲线参数字段利用OID值1.2.156.11235.1.1.2.1 标识国家密码管理局批准的专用于无线局域网的曲线参数。

X.509 v3数字证书中的所有字段均采用ASN.1/DER进行编码，组成特定的证书数据结构。ASN.1/DER编码是关于每个字段的类型、长度和取值（TLV）的编码系统，如图1所示。

类型	长度	取值

图1　TLV 格式

在对数字证书解析的过程中，应严格按照先判断类型，再确定长度，根据长度读取数值的方式进行，保证数字证书能够正确的扩展应用。

X.509 v3数字证书存储和传输等操作可以以下方式处理：

a) base64binary为编码类型、以PEM格式进行存储（文件名的后缀在Windows系统下可为.cer或者.pl，Linux和Unix等操作系统不限）；

b) 以PKCS #12格式存储的证书和相应私钥（文件名的后缀在Windows系统下为.p12或者.pfx，Linux和Unix等操作系统不限）。

6　数字证书数据结构

WAPI协议中所使用的X.509数字证书数据结构由三个域组成：

——基本证书域

包含了颁发者和使用者名称、使用者公钥信息、有效日期等其他相关基本信息。

——签名算法域

包含证书签发机构签发该证书所使用的密码算法标识符和可选参数。该域的算法标识符必须与基本证书域中的“签名算法”字段的内容相同。

——签名值域

三个基本域包括的字段如下图2所示。其中，基本证书域中的颁发者唯一标识符和使用者唯一标识符为WAPI协议中所使用的X.509数字证书可选项。

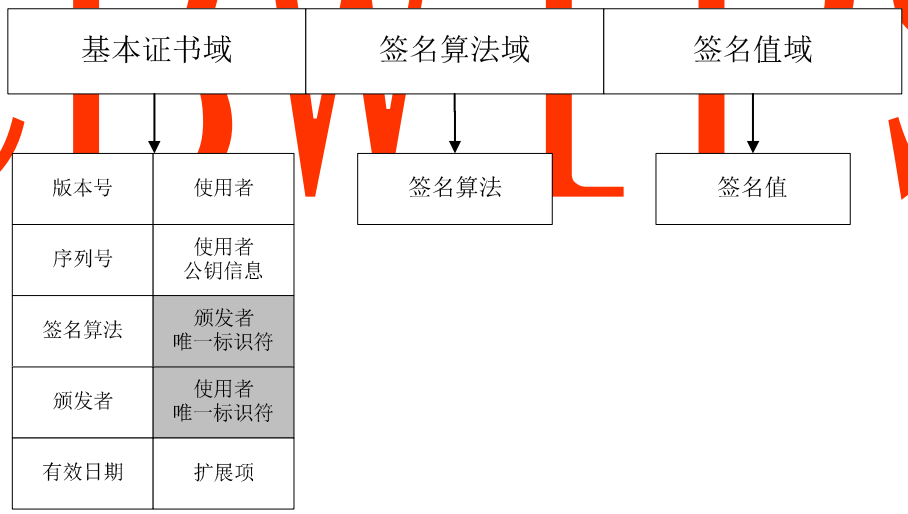

图2　WAPI 协议中所使用的 X.509 数字证书的格式

符合WAPI协议的X.509数字证书编码举例参见附录A，X.509数字证书的ASN.1结构参见附录C。

7　基本证书域数据字段内容

7.1　版本号

本字段定义参见GB/T 20518-2006 5.2.2.1。

WAPI协议中所使用的X.509数字证书的版本号。

7.2　序列号

本字段定义参见GB/T 20518-2006 5.2.2.2。

WAPI协议中规定的鉴别控制器实体、鉴别控制器实体和接入请求者实体所使用的X.509数字证书的唯一标识，为正整数。通过颁发者标识和序列号可以唯一地确定一张证书。

7.3 签名算法

本字段定义参见GB/T 20518-2006 5.2.2.3。

WAPI协议中，签发X.509数字证书所使用的密码算法的标识符。该值同签名算法域中包含的值相同。利用OID 值1.2.156.11235.1.1.1标识基于SHA-256的ECDSA-192算法。

7.4 颁发者

本字段定义参见GB/T 20518-2006 5.2.2.4。

WAPI协议中，颁发者标识了对数字证书签名和颁发的鉴别服务器实体。根据CBWIPS/Z 021-2010《无线局域网网络设备标识规范》，命名中应包含以下五个域：

强制域：DC=WAPI；

国家域：表示管理域所属的国家；

管理域：定义该无线局域网所属的运营者，可以是运营商、政府、企事业等；

网络域：定义在某个运营者域的无线局域网设备层次；

设备域：定义无线局域网设备的名称，要求不超过127个数字或字母的组合。

7.5 有效日期

本字段定义参见GB/T 20518-2006 5.2.2.5。

WAPI协议中所使用的X.509数字证书的有效期，包含有起始时间和终止时间。

7.6 使用者

本字段定义参见GB/T 20518-2006 5.2.2.6。

在某些标准中也被称为“主体”，WAPI协议中，使用者标识了对数字证书中公钥对应的实体，可以为鉴别控制器实体、接入请求者实体和鉴别服务器实体。根据CBWIPS/Z 021-2010《无线局域网网络设备标识规范》，命名中应包含五个域，描述如下：

强制域：DC=WAPI；

国家域：表示管理域所属的国家，中国 C=CN；

管理域：定义该无线局域网所属的运营者,O= XXXX.subManagementDomain，XXXX 根据以下规则分配：

0000：保留

0001：中国电信

0002：中国移动

0003：中国联通

0004-0099：保留

0100-0999：私有

1000-9999：各省根据中国行政区划表取得一个代码，其余保留。

网络域：定义在某个运营者域的无线局域网设备层次，由电信运营商自己定义，OU=XXX；

设备域：定义无线局域网设备的名称，CN=XXX@Type，Type 表示设备的类型，分为三种：

ASU：表示AS 等相关类型后台认证、授权管理设备；

AE：表示AP、AC 等接入设备；

CBWIPS/Z xxx—xxxx

ASUE：表示用户设备。

设备域要求不超过127个数字或字母的组合,即XXX@Type的内容长度。

例如：

中国电信一个AS：CN=SN1@ASU,OU=CS.HN,O=0001,C=CN,DC=WAPI。

中国电信一个用户终端：CN=userid@ASUE,OU=CS.HN,O=0001,C=CN,DC=WAPI。

7.7 使用者公钥信息

本字段定义参见GB/T 20518-2006 5.2.2.7。

WAPI协议中本字段用来标识公钥和对应的公钥算法。公钥算法字段利用OID 值1.2.840.10045.2.1标识椭圆曲线算法；椭圆曲线参数字段利用OID值1.2.156.11235.1.1.2.1 标识国家密码管理局批准的专用于无线局域网的曲线参数。

7.8 颁发者唯一标识符

本字段定义参见GB/T 20518-2006 5.2.2.8。

WAPI协议中，此字段为可选项。

7.9 使用者唯一标识符

本字段定义参见GB/T 20518-2006 5.2.2.9。

WAPI协议中，此字段为可选项。

7.10 扩展项目

扩展项目格式参见附录E，支持WAPI功能的设备和X.509证书必须具备此字段的扩展能力,本字段为可包含以下内容:

——实体唯一标识（编码）：代表一个证书持有者身份的唯一编码，用于关联具体业务，实体唯一标识的OID由各运营商或电子认证服务机构自行申请和定义。

——颁发机构密钥标识符(颁发者密钥标识):以识别与证书签名私钥相应的公钥。当颁发者由于有多个密钥共存或由于发生变化而具有多个签名密钥时使用该扩展。可识别基于颁发者证书中的主体密钥标识符或基于颁发者的名称和序列号。

——主题密钥标识符(主题密钥标识):提供一种识别证书的方法，该证书包含一个特定的公钥。此扩展标识了被认证的公开密钥，它能够区分同一主体使用的不同密钥。

——密钥用法:说明已认证的公开密钥用于何种用途。用户证书（分WLAN终端证书、WLAN设备证书、AS证书等）则根据证书用途，分为“签名”证书和“加密”证书，选择对应的密钥用途进行签发。

8 签名算法域数据字段内容

WAPI协议中，签发X.509数字证书所使用的密码算法的标识符。该值同基本证书域中签名算法字段包含的值相同。利用OID值1.2.156.11235.1.1.1标识基于SHA-256的ECDSA-192算法。

9 签名值域数据字段内容

包含了对基本证书域（第7章内容）进行数字签名的结果。

WAPI协议中，使用ECDSA进行签名，签名值（x,y）包括x和y两部分组成，类型为整形。

附 录 A
（规范性附录）
符合 WAPI 协议的 X.509 数字证书编码举例

A.1 符合WAPI协议的X.509 数字证书编码

以下内容为一个符合WAPI协议的X.509数字证书编码：

```
          30 82 02 45 30 82 01 FA A0 03 02 01 02  0..E0........
02 04 10 00 00 03 30 0C 06 08 2A 81 1C D7 63 01 ......0...*...c.
01 01 05 00 30 51 31 14 30 12 06 0A 09 92 26 89 ....0Q1.0.....&.
93 F2 2C 64 01 19 16 04 57 41 50 49 31 0B 30 09 ..,d....WAPI1.0.
06 03 55 04 06 13 02 43 4E 31 0D 30 0B 06 03 55 ..U....CN1.0...U
04 0A 13 04 30 30 30 33 31 0B 30 09 06 03 55 04 ....00031.0...U.
0B 13 02 53 4E 31 10 30 0E 06 03 55 04 03 14 07 ...SN1.0...U....
61 73 31 40 41 53 55 30 1E 17 0D 30 31 30 31 30 as1@ASU0...01010
31 30 31 30 31 30 31 5A 17 0D 31 30 30 34 32 31 10101015Z..100421
30 32 30 32 30 32 5A 30 52 31 14 30 12 06 0A 09 020202Z0R1.0....
92 26 89 93 F2 2C 64 01 19 16 04 57 41 50 49 31 .&...,d....WAPI1
0B 30 09 06 03 55 04 06 13 02 43 4E 31 0D 30 0B .0...U....CN1.0.
06 03 55 04 0A 13 04 30 30 30 33 31 0B 30 09 06 ..U....00031.0..
03 55 04 0B 13 02 53 4E 31 11 30 0F 06 03 55 04 .U....SN1.0...U.
03 14 08 61 73 31 2D 32 40 41 45 30 4A 30 14 06 ...as1-2@AE0J0..
07 2A 86 48 CE 3D 02 01 06 09 2A 81 1C D7 63 01 .*.H.=....*...c.
01 02 01 03 32 00 04 15 61 78 B6 EF BC 41 5A 7B ....2...ax...AZ{
A8 89 95 28 23 89 7B CF 28 F3 40 7F 3C E1 D0 73 ...(#.{.(.@ <..s
C8 CB C9 17 6C 75 3E 57 34 78 81 B5 1F B9 AF CE ....lu>W4x......
C0 BE A6 FC EE BB C4 A3 81 CB 30 81 C8 30 1D 06 ..........0..0..
03 55 1D 0E 04 16 04 14 F1 DC F6 90 B6 C4 28 9B .U..........(.
3D 2B 5C AB 6B B6 F3 F6 ED BD 33 FD 30 7C 06 03 =+\.k.....3.0|..
55 1D 23 04 75 30 73 80 14 0E A5 88 20 FB 4D C5 U.#.u0s..... .M.
33 56 8F EE CA FC C1 A4 8D 27 E0 0A 34 A1 55 A4 3V.......'..4.U.
53 30 51 31 14 30 12 06 0A 09 92 26 89 93 F2 2C S0Q1.0.....&...,
64 01 19 16 04 57 41 50 49 31 0B 30 09 06 03 55 d....WAPI1.0...U
04 06 13 02 43 4E 31 0D 30 0B 06 03 55 04 0A 13 ....CN1.0...U...
04 30 30 30 33 31 0B 30 09 06 03 55 04 0B 13 02 .00031.0...U....
53 4E 31 10 30 0E 06 03 55 04 03 14 07 61 73 31 SN1.0...U....as1
40 41 53 55 82 04 7F FF 00 08 30 1C 06 03 55 1D @ASU.. ...0...U.
1F 04 15 30 13 30 11 A0 0F A0 0D 86 0B 68 74 74 ...0.0.......htt
70 3A 2F 2F 31 2E 63 6E 30 0B 06 03 55 1D 0F 04 p://1.cn0...U...
04 03 02 07 80 30 0C 06 08 2A 81 1C D7 63 01 01 .....0...*...c..
```

```
01 05 00 03 37 00 30 34 02 18 2A FC EA 9B DB 3E ....7.04..*....>
C4 4F 21 C7 2C 23 BE 29 9B 5B 1D 6A 29 08 31 F4 .O!.,#.).[.j).1.
44 C7 02 18 5E A3 40 E5 4F 7C 86 81 D2 65 DB 53 D...^.@.O|...e.S
30 E4 AD D2 EA 05 73 85 84 FC C3 A2             0.....s.....
```

A.2 符合WAPI协议的X.509 数字证书编码字段定义

各字段具体的内容和意义如下：

30 82 02 45

30 是证书的总结构体的类型 SEQUENCE
82 标识后面有 2 个字节表示长度
02 45 标识证书总的结构体的长度为 581，为后续内容的长度

30 82 01 FA

30 标识证书基本域的结构体类型 SEQUENCE
82 标识后面有 2 个字节表示长度
01 FA 标识证书基本结构域的长度为 506，为后续内容长度，不包括该 4 个字节

A0 03 02 01 02

A0 标识版本号域的类型
03 标识后续版本号的长度为 3 个字节
02 标识版本号类型为整形
01 表示版本类型的长度为 1 个字节
02 标识为 X509V3 版本的证书

02 04 10 00 00 03

02 标识序列号的类型为整形
04 标识长度为后面有 4 个字节的序列号
10 00 00 03 为序列号内容

30 0C 06 08 2A 81 1C D7 63 01 01 01 05 00

30 标识签名算法标识域的结构体类型 SEQUENCE
0C 标识后续两部分内容的长度为 12 个字节
06 标识签名算法 OID 的标识
08 标识后续有 8 个字节的签名算法 OID
2A 81 1C D7 63 01 01 01 标识 OID 内容为
(1.2.156.11235.1.1.1)
05 标识签名算法参数类型
00 标识签名算法参数的长度

30 51 31 14 30 12 06 0A 09 92 26 89 93 F2 2C 64
01 19 16 04 57 41 50 49 31 0B 30 09 06 03 55 04

06 13 02 43 4E 31 0D 30 0B 06 03 55 04 0A 13 04
30 30 30 33 31 0B 30 09 06 03 55 04 0B 13 02 53
4E 31 10 30 0E 06 03 55 04 03 14 07 61 73 31 40
41 53 55

30 标识颁发者名称列表域的类型 SEQUENCE
51 为后续的颁发者名称列表的总长度为 81
31 为颁发者名称[0]的类型 SET
14 颁发者名称域的长度 20
30 为颁发者名称域的类型为 SEQUENCE
12 为颁发者名称域的长度为 18
06 为名称 OID 的类型
0A 为名称 OID 的长度 10
09 92 26 89 93 F2 2C 64 01 19 为 OID
(0.9.2342.19200300.100.1.25)
标识无线局域网设备名称强制域 DC
16 为名称的类型为可打印字符
04 为名称的长度
57 41 50 49 为名称内容“WAPI”
31 为颁发者名称[1]的类型 SET
0B 为颁发者名称域的长度 11
30 为颁发者名称域的类型为 SEQUENCE
09 为颁发者名称域的长度为 9
06 为名称 OID 的类型
03 为名称 OID 的长度
55 04 06 为 OID
(2.5.4.6)
标识无线局域网设备名称国家域 C
13 为名称的类型为可打印字符
02 为名称的长度
43 4E 为名称内容“CN”
31 为颁发者名称[2]的类型 SET
0D 为颁发者名称域的长度 13
30 为颁发者名称域的类型为 SEQUENCE
0B 为颁发者名称域的长度为 11
06 为名称 OID 的类型
03 为名称 OID 的长度
55 04 0A 为 OID
（2.5.4.11）
标识无线局域网设备名称管理域 O
13 为名称的类型为可打印字符
04 为名称的长度 4
30 30 30 33 为名称内容“0003” 0003 表示中国联通
31 为颁发者名称[3]的类型 SET

0B 为颁发者名称域的长度 11
30 为颁发者名称域的类型为 SEQUENCE
09 为颁发者名称域的长度为 9
06 为名称 OID 的类型
03 为名称 OID 的长度
55 04 0B 为 OID
(2.5.3.12)
标识无线局域网设备命名网络域 OU
13 为名称的类型为可打印字符
02 为名称的长度
53 4E 为名称内容“SN”
31 为颁发者名称[4]的类型 SET
10 为颁发者名称域的长度 16
30 为颁发者名称域的类型为 SEQUENCE
0E 为颁发者名称域的长度为 14
06 为名称 OID 的类型
03 为名称 OID 的长度
55 04 03 为 OID
(2.5.4.3)
标识无线局域网设备名称设备域 CN
14 为名称的类型为可打印字符
07 为名称的长度
61 73 31 40 41 53 55 为名称内容“as1@ASU”

30 1E 17 0D 30 31 30 31 30 31 30 31 30 31 30 31
5A 17 0D 31 30 30 34 32 31 30 32 30 32 30 32 5A
30 为有效期域的类型为 SEQUENCE
1E 为有效期域的长度为 30
17 为起始时间的类型 17 为可打印字符
0D 为起始时间的长度为 13
30 31 30 31 30 31 30 31 30 31 30 31 5A 为起始时间
“0101010101012”
17 为起始时间的类型 17 为可打印字符
0D 为起始时间的长度为 13
31 30 30 34 32 31 30 32 30 32 30 32 5A 为结束时间
“1004210202022”

30 52 31 14 30 12 06 0A 09 92 26 89 93 F2 2C 64
01 19 16 04 57 41 50 49 31 0B 30 09 06 03 55 04
06 13 02 43 4E 31 0D 30 0B 06 03 55 04 0A 13 04
30 30 30 33 31 0B 30 09 06 03 55 04 0B 13 02 53
4E 31 11 30 0F 06 03 55 04 03 14 08 61 73 31 2D
32 40 41 45

30 标识持有者名称域的类型为 SEQUENCE
52 标识持有者名称列表的长度 82
31 标识持有者名称列表[0]的类型为 SET
14 持有者名称域的长度 20
30 为持有者名称域的类型为 SEQUENCE
12 为持有者名称域的长度为 18
06 为名称 OID 的类型
0A 为名称 OID 的长度 10
09 92 26 89 93 F2 2C 64 01 19 为 OID
(0.9.2342.19200300.100.1.25)
标识无线局域网设备名称强制域 DC
16 为名称的类型为可打印字符
04 为名称的长度
57 41 50 49 为名称内容“WAPI”
31 为持有者名称[1]的类型 SET
0B 为持有者名称域的长度 11
30 为持有者名称域的类型为 SEQUENCE
09 为持有者名称域的长度为 9
06 为名称 OID 的类型
03 为名称 OID 的长度
55 04 06 为 OID
(2.5.4.6)
标识无线局域网设备名称国家域 C
13 为名称的类型为可打印字符
02 为名称的长度
43 4E 为名称内容“CN”
31 为持有者名称[2]的类型 SET
0D 为持有者名称域的长度 13
30 为持有者名称域的类型为 SEQUENCE
0B 为持有者名称域的长度为 11
06 为名称 OID 的类型
03 为名称 OID 的长度
55 04 0A 为 OID
(2.5.4.11)
标识无线局域网设备名称管理域 O
13 为名称的类型为可打印字符
04 为名称的长度
30 30 30 33 为名称内容“0003” 0003 表示中国联通
31 为持有者名称[3]的类型 SET
0B 为持有者名称域的长度 11
30 为持有者名称域的类型为 SEQUENCE
09 为持有者名称域的长度为 9
06 为名称 OID 的类型

03 为名称 OID 的长度
55 04 0B 为 OID
(2.5.4.12)
标识无线局域网设备名称网络域 OU
13 为名称的类型为可打印字符
02 为名称的长度
53 4E 为名称内容“SN”
31 为持有者名称[4]的类型 SET
11 为持有者名称域的长度 17
30 为持有者名称域的类型为 SEQUENCE
0F 为持有者名称域的长度为 15
06 为名称 OID 的类型
03 为名称 OID 的长度
55 04 03 为 OID
（2.5.4.3）
标识无线局域网设备名称设备域 CN
14 为名称的类型为可打印字符
08 为名称的长度
61 73 31 2D 32 40 41 45 为名称内容“as1-2@AE”

30 4A 30 14 06 07 2A 86 48 CE 3D 02 01 06 09 2A
81 1C D7 63 01 01 02 01 03 32 00 04 15 61 78 B6
EF BC 41 5A 7B A8 89 95 28 23 89 7B CF 28 F3 40
7F 3C E1 D0 73 C8 CB C9 17 6C 75 3E 57 34 78 81
B5 1F B9 AF CE C0 BE A6 FC EE BB C4

30 为持有者证书公钥域类型 SEQUENCE
4A 为后续部分的总长度 74
30 持有者公钥算法签名域类型 SEQUENCE
14 为持有者签名算法标识和签名算法参数的总长度 20
06 为签名算法 OID 的类型
07 为签名算法 OID 的长度
2A 86 48 CE 3D 02 01 为签名算法 OID
(1.2.840.10045.2.1)
06 为签名算法参数类型为 OID 标识
09 为签名算法参数长度
2A 81 1C D7 63 01 01 02 01 为签名算法参数
(1.2.156.11235.1.1.2.1)
03 标识持有者公钥的类型为 BIT STRING
32 为持有者公钥的长度为 50
00 04 15 61 78 B6 EF BC 41 5A 7B A8 89 95 28 23
89 7B CF 28 F3 40 7F 3C E1 D0 73 C8 CB C9 17 6C
75 3E 57 34 78 81 B5 1F B9 AF CE C0 BE A6 FC EE
BB C4 为持有者公钥值，其中开头 00 为 bitstring 位

04 为压缩标志位

A3 81 CB 30 81 C8 30 1D 06 03 55 1D 0E 04 16 04
14 F1 DC F6 90 B6 C4 28 9B 3D 2B 5C AB 6B B6 F3
F6 ED BD 33 FD 30 7C 06 03 55 1D 23 04 75 30 73
80 14 0E A5 88 20 FB 4D C5 33 56 8F EE CA FC C1
A4 8D 27 E0 0A 34 A1 55 A4 53 30 51 31 14 30 12
06 0A 09 92 26 89 93 F2 2C 64 01 19 16 04 57 41
50 49 31 0B 30 09 06 03 55 04 06 13 02 43 4E 31
0D 30 0B 06 03 55 04 0A 13 04 30 30 30 33 31 0B
30 09 06 03 55 04 0B 13 02 53 4E 31 10 30 0E 06
03 55 04 03 14 07 61 73 31 40 41 53 55 82 04 7F
FF 00 08 30 1C 06 03 55 1D 1F 04 15 30 13 30 11
A0 0F A0 0D 86 0B 68 74 74 70 3A 2F 2F 31 2E 63
6E 30 0B 06 03 55 1D 0F 04 04 03 02 07 80

A3 为证书扩展域类型
81 标识后面有 1 个字节的长度位
CB 为整个扩展域的总长度 203
30 为证书扩展域内的扩展列表类型为 SEQUENCE
81 标识后面有 1 个字节的长度位
C8 为整个扩展列表的总长度 200
30 为扩展列表[0]的类型 SEQUENCE
1D 为以下扩展 OID 标识和扩展属性值的总长度 29
06 标识扩展 OID 标识类型
03 标识扩展 OID 标识的长度
55 1D 0E 为扩展 OID 标识值
04 标识扩展属性值类型
16 为扩展属性值长度 22
04 14 F1 DC F6 90 B6 C4 28 9B 3D 2B 5C AB 6B B6
F3 F6 ED BD 33 FD 为扩展属性值
30 为扩展列表[1]的类型 SEQUENCE
7C 为以下扩展 OID 标识和扩展属性值的总长度 124
06 标识扩展 OID 标识类型
03 标识扩展 OID 标识的长度
55 1D 23 为扩展 OID 标识值
04 标识扩展属性值类型
75 为扩展属性值长度 117
30 73 80 14 0E A5 88 20 FB 4D C5 33 56 8F EE CA
FC C1 A4 8D 27 E0 0A 34 A1 55 A4 53 30 51 31 14
30 12 06 0A 09 92 26 89 93 F2 2C 64 01 19 16 04
57 41 50 49 31 0B 30 09 06 03 55 04 06 13 02 43
4E 31 0D 30 0B 06 03 55 04 0A 13 04 30 30 30 33
31 0B 30 09 06 03 55 04 0B 13 02 53 4E 31 10 30

0E 06 03 55 04 03 14 07 61 73 31 40 41 53 55 82
04 7F FF 00 08 为扩展属性值
30 为扩展列表[2]的类型 SEQUENCE
1C 为以下扩展 OID 标识和扩展属性值的总长度 28
06 标识扩展 OID 标识类型
03 标识扩展 OID 标识的长度
55 1D 1F 为扩展 OID 标识值
04 标识扩展属性值类型
15 为扩展属性值长度 21
30 13 30 11 A0 0F A0 0D 86 0B 68 74 74 70 3A 2F
2F 31 2E 63 6E 为扩展属性值
30 为扩展列表[3]的类型 SEQUENCE
0B 为以下扩展 OID 标识和扩展属性值的总长度 11
06 标识扩展 OID 标识类型
03 标识扩展 OID 标识的长度
55 1D 0F 为扩展 OID 标识值
04 标识扩展属性值类型
04 为扩展属性值长度 4
03 02 07 80 为扩展属性值

30 0C 06 08 2A 81 1C D7 63 01 01 01 05 00
30 标识签名算法标识域的结构体类型 SEQUENCE
0C 标识后续两部分内容的长度为 12 个字节
06 标识签名算法 OID 的标识
08 标识后续有 8 个字节的签名算法 OID
2A 81 1C D7 63 01 01 01 标识 OID 内容为
(1.2.156.11235.1.1.1)
05 标识签名算法参数类型
00 标识签名算法参数的长度

03 37 00 30 34 02 18 2A FC EA 9B DB 3E C4 4F 21
C7 2C 23 BE 29 9B 5B 1D 6A 29 08 31 F4 44 C7 02
18 5E A3 40 E5 4F 7C 86 81 D2 65 DB 53 30 E4 AD
D2 EA 05 73 85 84 FC C3 A2
03 标识签名值域类型为 BIT STRING
37 为签名值域的总长度 55
00 30 34 02 18 2A FC EA 9B DB 3E C4 4F 21 C7 2C
23 BE 29 9B 5B 1D 6A 29 08 31 F4 44 C7 02 18 5E
A3 40 E5 4F 7C 86 81 D2 65 DB 53 30 E4 AD D2 EA
05 73 85 84 FC C3 A2
标识签名值
其中 00 标识 bitstring 位
30 标识 ECC 签名算法 X,Y 值域的类型 SEQUENCE

34 为两部分的总长度 52
02 标识签名值 X 的类型为整形
18 为签名值 X 的长度为 24
2A FC EA 9B DB 3E C4 4F 21 C7 2C 23 BE 29 9B 5B
1D 6A 29 08 31 F4 44 C7 为签名值 X 的值
02 标识签名值 Y 的类型为整形
18 为签名值 Y 的长度为 24
5E A3 40 E5 4F 7C 86 81 D2 65 DB 53 30 E4 AD D2
EA 05 73 85 84 FC C3 A2
为签名值 Y 的值

注：对于 00 标识 bitstring 位，头字节 00 表示将 bit 转换为 octet 需要补充 0 的个数。如果长度为 8 的整数倍，则不需要补充 0；如果长度不是 8 的整数倍，则需要补充 0 使长度达到 8 的整数倍，头字节表示补充的 0 的个数。

CBWIPS

附 录 B
（规范性附录）
WAPI 协议的 X.509 数字证书编码中 OID 的点分十进制的转换方法

B.1 转换方法

WAPI协议中规定采用的X.509数字证书签名算法为ECDSA-192，杂凑算法为SHA-256。公钥算法标识、签名算法标识以及椭圆曲线参数均采用OID方式表示。WAPI协议的X.509数字证书编码中OID的点分十进制的转换方法如下：

X.509数字证书编码中数据的第一元素表示为data[1]、第二个元素表示为data[2]依次类推，第i或者k元素表示为data[i]或者data[k]；128_i表示为128的i次幂。

1）将data[1]分解，分解公式为：X*40+Y=data[1]，计算得出X和Y的值；

2）如果data[2]不小于128,则判断data[3]是否小于128，如果data[3]不小于128，则判断data[4]是否小于128，以此类推，得到data[i]的值是小于128为止，然后按照如下公式进行计算：

data[i]+(data[i-1]-128)*128_1+(data[i-2]-128)*128_2+data[i-3]-128*128_3+.....+(data[2]-128)*128_(i-2)；

3）后续根据步骤2）的方法进行转换，起点为k（数据为data[k]），终点为i（数据为data[i]），计算公式为：

data[i]+(data[i-1]-128)*128_1+(data[i-2]-128)*128_2+(data[i-3]-128)*128_3+.....+(data[k]-128)*128_(i-k)；

4）点分十进制标识各个阶段得出的结果。

B.2 转换范例

十六进制数据：2a 81 1c d7 63 01 01 02 01

转换步骤：

1）第一元素0x2a的转换方式由公式X*40+Y=0x2a 计算得出X=1和Y=2；

2）第二元素0x81不小于128，第三元素0x1c小于128，即i=3，则计算公式为：data[3]+(data[2]-128)*128_(3-2)=0x1c+(0x81-128)*128_1=28+1*128=156；

3）后续元素转换方法中起始元素k = 4，截止元素i = 5，则计算公式为：data[5]+(data[4]-128)*128_(5-4) =0x63+(0xd7-128)*128_1=99+87*128=11235；后续元素的转换方式为：

——起始元素k=6，截止元素i=6：data[6]=0x01=1；

——起始元素k=7，截止元素i=7：data[7]=0x01=1；

——起始元素k=8，截止元素i=8：data[8]=0x02=2；

——起始元素k=9，截止元素i=9：data[9]=0x01=1；

4）点分十进制计算结果：1.2.156.11235.1.1.2.1。

附 录 C
（资料性附录）
证书私钥的组成

C.1 X.509 数字证书私钥的组成

X.509数字证书的私钥由以下部分组成：
——私钥的版本号
——私钥的内容
——私钥签名的 OID 标识
——私钥对应的公钥值

C.2 X.509 数字证书私钥的范例

30 60 02 01 01 04 18 31 9d c8 36 c2 09 e5 31 c6
31 16 ca 15 d3 88 c0 97 e8 f4 fe 11 21 64 b2 a0
0b 06 09 2a 81 1c d7 63 01 01 02 01 a1 34 03 32
02 04 15 61 78 b6 ef bc 41 5a 7b a8 89 95 28 23
89 7b cf 28 f3 40 7f 3c e1 d0 73 c8 cb c9 17 6c
75 3e 57 34 78 81 b5 1f b9 af ce c0 be a6 fc ee
bb c4

30 60

30 标识证书私钥结构体的类型 SEQUENCE
60 为证书内容字段的总长度为 96 个字节

02 01 01

02 标识私钥版本号类型
01 标识版本号的长度
01 标识版本号的类型

04 18 31 9d c8 36 c2 09 e5 31 c6 31 16 ca 15 d3
88 c0 97 e8 f4 fe 11 21 64 b2

04 标识私钥的类型
18 为私钥内容的长度为 24
31 9d c8 36 c2 09 e5 31 c6 31 16 ca 15 d3 88 c0
97 e8 f4 fe 11 21 64 b2 为私钥的内容

a0 0b 06 09 2a 81 1c d7 63 01 01 02 01

a0 标识私钥签名 OID 域的类型
0b 为私钥类型签名算法 OID 的 DER 编码长度

06 标识签名算法 OID
09 为算法 OID 的长度
2a 81 1c d7 63 01 01 02 01 为签名算法 OID
(1.2.156.11235.1.1.2.1)

a1 34 03 32 02 04 15 61 78 b6 ef bc 41 5a 7b a8
89 95 28 23 89 7b cf 28 f3 40 7f 3c e1 d0 73 c8
cb c9 17 6c 75 3e 57 34 78 81 b5 1f b9 af ce c0
be a6 fc ee bb c4

a1 标识公钥域的类型
34 为公钥域的长度 52
03 标识公钥的类型
32 为公钥的长度 50
02 标识公钥为整形值
04 为公钥值的压缩标志
15 61 78 b6 ef bc 41 5a 7b a8 89 95 28 23 89 7b
cf 28 f3 40 7f 3c e1 d0 73 c8 cb c9 17 6c 75 3e
57 34 78 81 b5 1f b9 af ce c0 be a6 fc ee bb c4
为与私钥配对的公钥值，即基本证书域中的使用者公钥信息字段中的公钥值。

附 录 D
（资料性附录）
X.509 证书 ASN.1 结构

X.509 证书的结构是用 ASN.1(Abstract Syntax Notation One)进行描述数据结构，并使用 ASN.1 语法进行编码。X.509 证书基本结构如下:

```
Certificate  ::=  SEQUENCE  {
tbsCertificate        TBSCertificate,
signatureAlgorithm    AlgorithmIdentifier,
signatureValue        BIT STRING  }
TBSCertificate  ::=  SEQUENCE  {
version          [0]  EXPLICIT Version  DEFAUT v1,
serialNumber          CertificateSerialNumber,
signature             AlgorithmIdentifier,
issuer                Name,
validity              Validity,
subject               Name,
subjectPublicKeyInfo  SubjectPublicKeyInfo,
issuerUniqueID  [1] IMPLICIT UniqueIdentifier OPTIONAL,
                                        -- 如果出现，version必须是v2或者v3（WAPI证书
                                           中此部分为可选）
subjectUniqueID [2] IMPLICIT Unique Identifier OPTIONAL,
                                        -- 如果出现，version必须是v2或者v3 WAPI证书
                                           中此部分为可选）
extensions       [3] EXPLICIT Extensions OPTIONAL      扩展项
                                        -- 如果出现, version 必须是v3
}
Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }
CertificateSerialNumber  ::=  INTEGER
Validity ::= SEQUENCE {
```

```
    notBefore       Time,
    notAfter        Time }
    Time ::= CHOICE {
    utcTime         UTCTime,
    generalTime     GeneralizedTime }
    UniqueIdentifier  ::=  BIT STRING
    SubjectPublicKeyInfo  ::=  SEQUENCE  {
    algorithm           AlgorithmIdentifier,
    subjectPublicKey    BIT STRING  }
    Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
    Extension  ::=  SEQUENCE  {
    extnID      OBJECT IDENTIFIER,
    critical      BOOLEAN DEFAULT FALSE,
    extnValue   OCTET STRING  }
```


上述的证书数据结构由 **tbsCertificate**， **signatureAlgorithm** 和 **signatureValue** 三个域构成。这些域的含义如下：

— **tbsCertificate** 域包含了颁发者名称和使用者名称、使用者的公钥、证书的有效期以及其他的相关信息。

— **signatureAlgorithm** 域包含证书颁发机构颁发该证书所使用的密码算法的标识符。一个算法标识符的 ASN.1 结构如下：

```
AlgorithmIdentifier  ::=  SEQUENCE  {
                              algorithm    OBJECT IDENTIFIER,
                              parameters  ANY DEFINED BY algorithm OPTIONAL }
```

算法标识符用来标识一个密码算法，其中的 OBJECT IDENTIFIER 部分标识了具体的算法。其中可选参数的内容完全依赖于所标识的算法。该域的算法标识符必须与 tbsCertificate 中的 signature 标识的签名算法项相同。

— **signatureValue** 域包含了对 tbsCertificate 域进行数字签名的结果。采用 ASN.1 DER 编码的 tbsCertificate 作为数字签名的输入，而签名的结果则按照 ASN.1 编码成 BIT STRING 类型并保存在证书签名值域内。

附 录 E
（资料性附录）
X.509 证书扩展项

X.509 证书扩展项结构如下：

```
Extension ::= SEQUENCE {
        extnID      OBJECT IDENTIFIER,
        critical    BOOLEAN DEFAULT FALSE,
        extnValue   OCTET STRING }
```

extnID：表示一个扩展元素的 OID

critical：表示这个扩展元素是否重要

extnValue：表示这个扩展元素的值，字符串类型。

CBWIPS