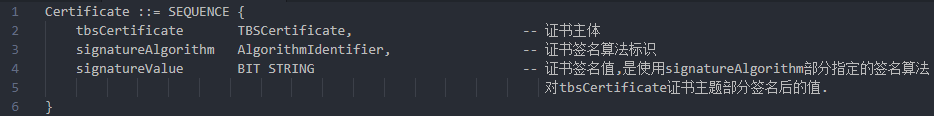
**X.509证书解析程序设计和实现——实验报告**

1. **X.509证书结构描述**

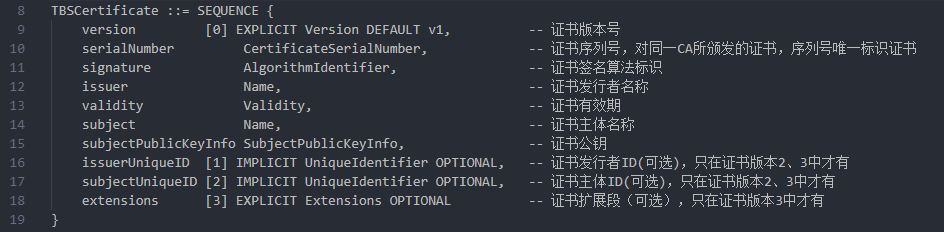
\*这部分的内容保存在 “X509证书结构解析.txt” 文件中

**①X.509证书的总体结构**

****

X.509证书（Certificate）结构主要分成了三大部分：证书主体、证书签名算法标识、证书签名值三个部分。其中证书主体和证书签名算法标识的存储结构为结构体，证书签名值的存储格式为BitString。

**②证书主体（TBSCertificate）结构**



证书主体（TBSCertificate）结构分成了10个部分，包括了证书版本号、证书序列号、证书签名算法标识、证书发行者名称、证书有效期、证书主体名称、证书公钥、证书发行者ID、证书主体ID、证书扩展部分。各部分的存储结构如下图所示。

1. 证书版本号

1544797444(1)

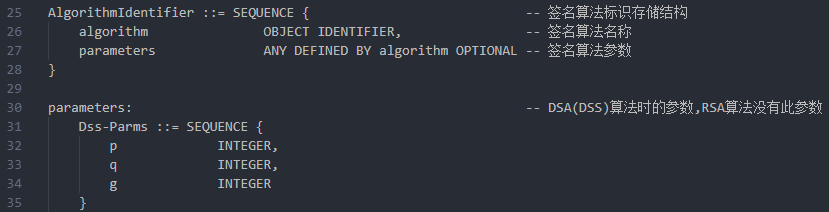
证书版本号的存储结构为整型数。

1. 证书序列号

1544797463(1)

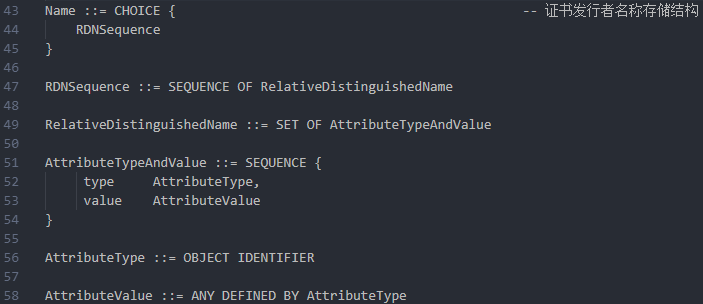
证书序列号的存储结构为整型数。

1. 证书签名算法标识



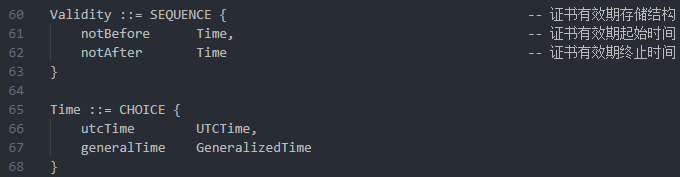
证书签名算法标识的存储结构为AlgorithmIdentifier，里面包含了算法名称和算法参数。算法名称使用OID结构保存，算法参数的存储结构为整型数。

1. 证书发行者名称、证书主体名称



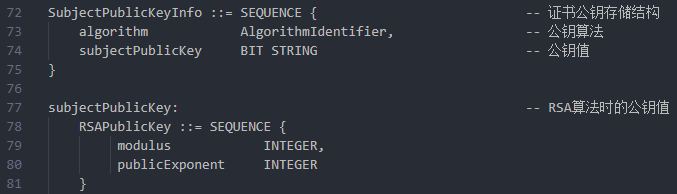
证书发行者名称、证书主体名称均使用Name结构体进行存储，包含了OID结构和其他自定义结构。

1. 证书有效期



证书有效期使用Time结构体进行存储。

1. 证书公钥



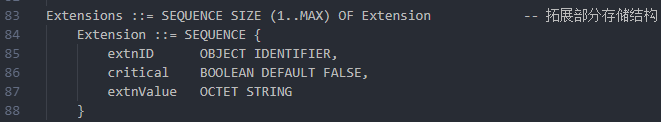
证书公钥使用AlgorithmIdentifier和BitString组成的结构体进行存储。

1. 证书发行者ID、证书主体ID

1544797952(1)

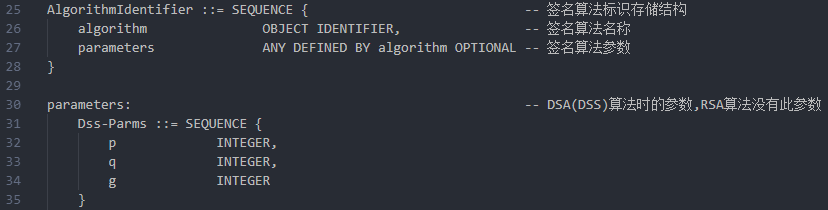
证书发行者ID、证书主体ID使用BitString进行存储。

1. 证书扩展部分



证书扩展部分使用Extension结构体进行存储。

**③证书签名算法标识（signatureAlgorithm）结构**

****

证书签名算法标识的存储结构为AlgorithmIdentifier，里面包含了算法名称和算法参数。算法名称使用OID结构保存，算法参数的存储结构为整型数。

**④证书签名值（signatureValue）结构**

**1544798741(1)**

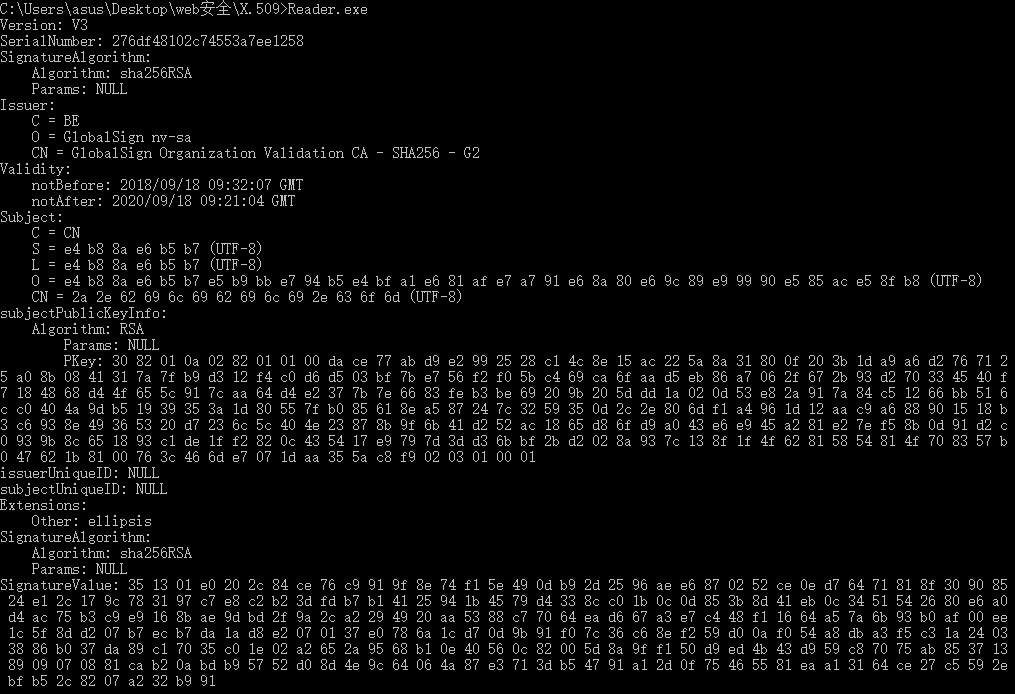
证书签名值的存储格式为BitString。

1. **数据结构**

|  |  |
| --- | --- |
| **说明** | **代码截图** |
| X.509证书的编码格式使用（键[T]，长度[L]，值[V]）的格式，因此使用一个结构体进行证书内容的分割和保存。Seg结构体用于保存字段的值，数据类型为整型数。 | **1544802039(1)** |
| X.509证书的整体结构 | **1544801896(1)** |
| X.509证书的证书主体的保存结构 | **1544802019(1)** |
| X.509证书的公钥算法的保存结构 | **1544801961(1)** |
| X.509证书的发行者和证书拥有主体的保存结构 | **1544801994(1)** |
| X.509证书的签名算法的保存结构 | **1544801947(1)** |
| X.509证书的签名值的保存结构 | **1544801981(1)** |

1. **编译运行结果**

解析DER\_x509.cer得到的结果



**比对结果**

|  |  |
| --- | --- |
| 程序输出 | Windows显示 |
| 1544800436(1) | 1544800460(1) |
| 1544800477(1) | 1544800504(1) |
| 1544800538(1)  注：GMT时间与北京时间有时差（+8） | 1544800564(1) |
| 1544800625(1)  注：C++无法输出UTF8编码，下图为转码后得到的结果 | 1544800649(1) |
| 1544800829(1) | |
| 1544800948(1) | 1544800929(1) |

**得出结论**

程序输出结果与Windows内置解析程序输出的结果一致，证明解析X.509证书成功，实验结果符合预期目标。

\*证书的扩展部分由于不清楚其内容的实际含义，因此在本次实验中只对其进行了TLV（键、长度、值）编码格式的解析，而没有对其内容进行翻译。