# 证书格式说明

适用于基于ECC，国标SM2算法的公钥证书信息（16进制格式），信息只有到签名值的位置，后面的还没有归纳

|  |  |  |
| --- | --- | --- |
| 地址 | 内容 | 意义 |
| 0000 | 30 82 02 00 | SEQUENCE  Certificate:: SEQUENCE类型(30)，数据块长度字节为2(82)，长度为512(02 00) |
| 0004 | 30 82 01 a5 | SEQUENCE  tbsCertificate:: SEQUENCE类型,长度421(01 a5) 证书的内容的长度，到达扩展内容结束 |
| 0008 | a0 03 | Version::特殊内容-证书版本(a0),长度3 |
| 0010 | 02 10 02 | INTEGER 2 version::整数类型(02),长度1,版本3(2) |
| 0013 | 02 10 | 证书序列号的长度为16(10) |
|  | 00 07 00 01 20 18 08 23 11 00 00 00 00 00 03 08 | 证书序列号的具体内容 |
| 0031 | 30 0c | 签名算法，长度为12(0c) |
| 0045 | 30 3c | 证书颁发者，长度为60(3c) |
| 0107 | 30 1e | 证书的日期，长度为30(1e) |
| 0139 | 30 50 | 证书持有者，长度为80(50) |
| 0221 | 30 59 | 证书公钥信息，长度为89(59) |
| 0223 | 30 13 | 参数，长度为19(13) |
| 0244 | 03 42 | 公钥信息具体长度为66(42) |
| 0246 | 00 04 | 公钥信息的开头固定为 00 04 |
| 0248 | 0f …… | 公钥的值，长度为66-2=64 |
| 0312 | a3 73 | 扩展部分，长度为115(73) |
| 0314 | 30 71 | 扩展部分，长度为113(71) |
| 0316 | 30 1F | 颁发者密钥标识信息，长度为31(1F) |
| 0318 | 06 03 | OID，长度为3(03) |
| 0323 | 30 18 30 16 30 14 | 颁发者密钥标识符，长度为20(14) |
| 0329 | 8b …… | 颁发者密钥标识符的值 |
| 0349 | 30 1d | 拥有者密钥标识信息，长度为29d) |
| 0351 | 06 03 | OID，长度为3(03) |
| 0356 | 4 16 4 14 | 拥有者密钥标识符，长度为20(14) |
| 0360 | 4c …… | 拥有者密钥标识符的值 |
| 0380 | 30 0b | 长度为11(0b) |
| 0393 | 30 22 | 长度为34(22) |
| 0429 | 30 0c | signatureAlgorithm:: = AlgorithmIdentifier, 长度12(0c) |
| 0443 | 03 47 00 30 44 | 签名值的长度为68(44) |
| 0448 | 02 20 | 具体签名值长度为32(20) R |
| 0450 | 45 0c …… | 签名值 |
| 0482 | 02 20 | 具体签名值长度为32(20) S |
| 0484 | 58 0d | 签名值 |
| 0516 | ff …… | 证书内容结束 |
| 0530 | ff | 结束 |