注释：“说明”里的开头的加粗的值：1为一致，0为不一致

国标总长： 752个字节

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项名 | | 国标 | 得安 | 说明 |
| 1 | 版本号 | | 1字节 | 1字节 | **1** |
| 2 | 序列号 | | 32字节 | 32字节 | **1** |
| 3 | 签名算法 | | 16字节 | 19字节 | **0**，这个值是固定的，采用的是算法SM3，是19个字节 |
| 4 | 签发单位 | 名称（CN） | 8字节 | 8字节 | **1** |
| 区/县（L） | 2字节 | 2字节 | **1**，例如08，参照：GBT 2260-2007 中华人民共和国行政区划代码.pdf |
| 地市（L） | 2字节 | 2字节 | **1**，例如01，参照：GBT 2260-2007 中华人民共和国行政区划代码.pdf |
| 省份（S） | 2字节 | 2字节 | **1**，例如11，参照：GBT 2260-2007 中华人民共和国行政区划代码.pdf |
| 国家（C） | 2字节 | 2字节 | **1**，参照GB/T 2659-2000，例如CN |
| 5 | 有效日期 | 生效日期 | 19字节 | 19字节 | **1**，采用“YYYY-MM-DD HH:MM:SS” |
| 失效日期 | 19字节 | 19字节 | **1**，采用“YYYY-MM-DD HH:MM:SS” |
| 6 | 证书持有者信息 | 设备标识（CN） | 128字节 | 128字节 | **1**,格式为“设备ID\_密码模块ID”，某个ID为空值为“NULL”。 |
| 网络类型（O） | 2字节 | 2字节 | **1**，01：公安信息网 02：视频专网 |
| 预留（O） | 2字节 | 2字节 | **1**，“00”预留代表空值，无意义 |
| 区/县（L） | 2字节 | 2字节 | **1**，例如05，参照：GBT 2260-2007 中华人民共和国行政区划代码.pdf |
| 地市（L） | 2字节 | 2字节 | **1**，例如06，参照：GBT 2260-2007 中华人民共和国行政区划代码.pdf |
| 省份（S） | 2字节 | 2字节 | **1**，例如44，参照：GBT 2260-2007 中华人民共和国行政区划代码.pdf |
| 国家（C） | 2字节 | 2字节 | **1**，参照GB/T 2659-2000，例如CN |
| 7 | 证书持有者公钥信息 | | 256位 | 520位（65字节） | **0**，得安的公钥信息是32字节为R，32字节为s。没有256位的公钥信息。 |
| 8 | 扩展项 | CRL分布点 | 128字节 | 128字节 | **1**，是用户下载CRL的网址，也可以是官网 |
| 证书持有者密钥标识符 | 20字节 | 20字节 | **1**， |
| 签发单位的密钥标识符 | 20字节 | 20字节 | **1**， |
| 密钥用法 | 64字节 | 64字节 | **1**， |
| 指纹 |  | 20字节 | **0**， |
| 预留 | 128字节 | 128字节 | **1**， |
| 9 | 签名项 | | 256位 | 512位（64字节） | **0**， 这个也是签名值，是不显现的，必须是标准的签名值才可以。 |