

ICS 35.240.99
L 76



中华人民共和国国家标准

GB/T 36904—2018

电子证照 标识规范

Electronic certificate—Identifier specification

2018-11-15 发布

2019-01-01 实施

国家市场监督管理总局 发布
中国国家标准化管理委员会

目 次

前言	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 编码规则	2
5.1 标识结构	2
5.2 电子证照根代码	2
5.3 证照类型代码	2
5.4 证照颁发机构代码	2
5.5 流水号	2
5.6 版本号	2
5.7 校验位	2
6 标识的生成与管理要求	3
附录 A (资料性附录) 校验位的计算示例	4
参考文献	6

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由国家密码管理局提出并归口。

本标准起草单位：中央办公厅信息中心、中国电子技术标准化研究院、福建南威软件有限公司、方正国际软件(北京)有限公司、成都卫士通信息产业股份有限公司、浪潮软件集团有限公司、北京冠群信息技术股份有限公司、福建榕基软件股份有限公司、江苏省建设信息中心、广东省信息中心、北京数科网维技术有限责任公司、航天福昕软件(北京)有限公司、北京海泰方圆科技股份有限公司、北京书生电子技术有限公司、浙江汇信科技有限公司、普华诚信信息技术有限公司、甘肃万维信息技术有限公司、广州市中智软件开发有限公司、山东省标准化研究院、中国软件与技术服务股份有限公司、中安网脉(北京)科技股份有限公司、上海维豪信息安全技术有限公司。

本标准主要起草人：陈亚军、李海波、孙文龙、苗宗利、黄文峰、李平立、代红、钟伟平、王少康、丛培勇、冯辉、方春燕、薛馨枫、王凌、贾宝刚、宁方刚、李波、陈兆亮、许承滨、陈子楚、虞小平、丁曙初、王寒冰、张宇、武文高、王忠义、刘丹、柴德华、董卫兵、刘冰、苗银军、梁国杰、汪翔、张静、逢锦山、程主、冯文化、王天顺、陈晶、郑秉文、李易昂、王雷、龚沫薇。

电子证照 标识规范

1 范围

本标准规定了电子证照标识的编码规则以及标识生成、管理要求。
本标准适用于电子证照标识的生成和校验。

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/T 1988—1998 信息技术 信息交换用七位编码字符集
- GB/T 17710—2008 信息技术 安全技术 校验字符系统
- GB/T 36902—2018 电子证照 目录信息规范
- GB/T 36903—2018 电子证照 元数据规范

3 术语和定义

GB/T 36902—2018、GB/T 36903—2018 界定的以及下列术语和定义适用于本文件。

3.1

编码 coding

给事物或概念赋予代码的过程。
[GB/T 10113—2003,定义 2.2.1]

3.2

代码 code

表示特征事物或概念的一个或一组字符。
注:这些字符可以是阿拉伯数字、拉丁字母或便于人和机器识别与处理的其他符号。
[GB/T 10113—2003,定义 2.2.5]

3.3

对象标识符 object identifier

与无歧义地标识它的客体相关的全局唯一值。
[GB/T 16262.1—2006,定义 3.6.47]

3.4

电子证照标识 electronic certificate identifier

赋予电子证照的唯一代码。

4 缩略语

下列缩略语适用于本文件。
OID:对象标识符(object identifier)

5 编码规则

5.1 标识结构

电子证照标识采用组合编码方式生成，各部分由数字、英文大写字母以及点分隔符“.”（GB/T 1988—1998 规定的编码为 2E）组成。

标识的组成部分从左至右依次为：电子证照根代码、证照类型代码、证照颁发机构代码、流水号、版本号 and 校验位，各部分之间用点分隔符“.”分隔。具体结构见图 1。

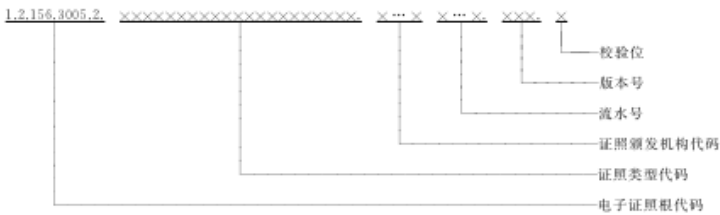


图 1 电子证照标识结构

5.2 电子证照根代码

用于区分证照和其他种类电子文件的代码，电子证照根代码的 OID 取值固定为“1.2.156.3005.2”。

5.3 证照类型代码

见 GB/T 36902—2018 的 5.2.2“证照类型代码”。

5.4 证照颁发机构代码

见 GB/T 36903—2018 的 5.2.6“证照颁发机构代码”。

5.5 流水号

流水号应在该证照类型及颁发机构下唯一，可使用“证照编号”（见 GB/T 36903—2018 中 5.2.3）元数据项的取值或其部分内容，也可以另行定义流水号编号规则。

证照信息如有变更，可根据业务需求保持流水号不变。

5.6 版本号

电子文件版本的标识号，3 位阿拉伯数字。因年检、续期等业务操作而形成新的电子证照文件时，如证照编号和流水号均不变，则应产生一个新的递增版本号加以区分。

5.7 校验位

校验位为 1 位数字或英文大写字母，用以检验证照标识的正确性。校验位按照 GB/T 17710—2008 定义的“ISO/IEC 7064 MOD37,36”规则计算，验证式如下：

$$(((M + a_n) \parallel M \cdot 2 \mid_{(M+1)} + a_{(n-1)}) \parallel M \cdot 2) \mid_{(M+1)} + \dots + a_1) \parallel M = 1$$

式中：

M ——模数，串所有可用字符的总个数；

- n ——含校验位的串位数；
 i ——从右侧计算的字符所在串的位置序号；
 a_i ——英文字母数字串从左到右分别为 a_0 到 a_{n-1} ，其中 a_{n-1} 为校验位；
 $\parallel_M$ ——除以 M 后的余数，如果为 0，则应替换为 M ；
 $\parallel_{(M+1)}$ ——除以 $(M+1)$ 后的余数，不会为 0。
- 注：电子证照根代码和各组成部分之间的分隔符不参与校验码计算。
标识校验位计算的示例参见附录 A。

6 标识的生成与管理要求

- 电子证照文件标识生成和管理要求包括：
- a) 电子证照的标识由证照颁发机构按规则生成，并保证其唯一性；
 - b) 电子证照标识生成后，在交换、存档等过程中应保持不变。



附录 A
(资料性附录)
校验位的计算示例

假设××市某单位的建筑工程施工许可证,待计算校验位的字符串为“1.2.156.3005.2.11100000000013338W002.11320482014138860P.201807250201.001.X”,其用于计算校验位的字符串序列为“11100000000013338W00211320482014138860P201807250201001”,校验位为 X。采用 5.7 中要求的“ISO/IEC 7064 MOD37,36”计算得到校验位取值为 22,对应字符为 L,则完整的证照标识为“1.2.156.3005.2.11100000000013338W002.11320482014138860P.201807250201.001.L”,具体计算过程见表 A.1。

表 A.1 校验位计算示例

步骤	乘积	+	下一字符值	—	中间和	调整中间和	×	2	—	结果	调整后下次 计算值的乘积
	P_j	+	a_{n-j+1}	—	S_j	$S_j \parallel M$	×	2	—	P_{j+1}	$P_{j+1} \parallel (M+1)$
1	M	+	1	—	1	1	×	2	—	2	2
2	2	+	1	—	3	3	×	2	—	6	6
3	6	+	1	—	7	7	×	2	—	14	14
4	14	+	0	—	14	14	×	2	—	28	28
5	28	+	0	—	28	28	×	2	—	56	19
6	19	+	0	—	19	19	×	2	—	38	1
7	1	+	0	—	1	1	×	2	—	2	2
8	2	+	0	—	2	2	×	2	—	4	4
9	4	+	0	—	4	4	×	2	—	8	8
10	8	+	0	—	8	8	×	2	—	16	16
11	16	+	0	—	16	16	×	2	—	32	32
12	32	+	0	—	32	32	×	2	—	64	27
13	27	+	1	—	28	28	×	2	—	56	19
14	19	+	3	—	22	22	×	2	—	44	7
15	7	+	3	—	10	10	×	2	—	20	20
16	20	+	3	—	23	23	×	2	—	46	9
17	9	+	8	—	17	17	×	2	—	34	34
18	34	+	33	—	30	30	×	2	—	60	23
19	23	+	0	—	23	23	×	2	—	46	9
20	9	+	0	—	9	9	×	2	—	18	18
21	18	+	2	—	20	20	×	2	—	40	3
22	3	+	1	—	4	4	×	2	—	8	8
23	8	+	1	—	9	9	×	2	—	18	18

表 A.1 (续)

步骤	乘积	+	下一字符值	—	中间和	调整中间和	×	2	—	结果	调整后下次 计算值的乘积
	P_j	+	a_{n-j+1}	—	S_j	$S_j \parallel M$	×	2	—	P_{j+1}	$P_{j+1} \parallel (M+1)$
24	18	+	3	—	21	21	×	2	—	42	5
25	5	+	2	—	7	7	×	2	—	14	14
26	14	+	0	—	14	14	×	2	—	28	28
27	28	+	4	—	32	32	×	2	—	64	27
28	27	+	8	—	35	35	×	2	—	70	33
29	33	+	2	—	35	35	×	2	—	70	33
30	33	+	0	—	33	33	×	2	—	66	29
31	29	+	1	—	30	30	×	2	—	60	23
32	23	+	4	—	27	27	×	2	—	54	17
33	17	+	1	—	18	18	×	2	—	36	36
34	36	+	3	—	3	3	×	2	—	6	6
35	6	+	8	—	14	14	×	2	—	28	28
36	28	+	8	—	36	36	×	2	—	72	35
37	35	+	6	—	5	5	×	2	—	10	10
38	10	+	0	—	10	10	×	2	—	20	20
39	20	+	26	—	9	9	×	2	—	18	18
40	18	+	2	—	20	20	×	2	—	40	3
41	3	+	0	—	3	3	×	2	—	6	6
42	6	+	1	—	7	7	×	2	—	14	14
43	14	+	8	—	22	22	×	2	—	44	7
44	7	+	0	—	7	7	×	2	—	14	14
45	14	+	7	—	21	21	×	2	—	42	7
46	7	+	2	—	7	7	×	2	—	14	14
47	14	+	5	—	19	19	×	2	—	38	1
48	1	+	0	—	1	1	×	2	—	2	2
49	2	+	2	—	4	4	×	2	—	8	8
50	8	+	0	—	8	8	×	2	—	16	16
51	16	+	1	—	17	17	×	2	—	34	34
52	34	+	0	—	34	34	×	2	—	68	31
53	31	+	0	—	31	31	×	2	—	62	25
54	25	+	1	—	26	26	×	2	—	52	15
55	15	+	校验位值(22)	—	37	要求 $S_i \bmod M=1$					

参 考 文 献

- [1] GB/T 10113—2003 分类与编码通用术语
 - [2] GB/T 16262.1—2006 信息技术 抽象语法记法—(ASN.1) 第1部分:基本记法规范
-