ICS 35.240.01
CCS L 67

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T 383.2—2023

电子印章
第 2 部分：数字证书

Electronic seal—
Part 2: Digital certificate

2023-11-02 发布　　2023-12-01 实施

深圳市市场监督管理局　　发 布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件是 DB4403/T 383—2023《电子印章》的第 2 部分。DB4403/T 383—2023 已经发布了以下部分：

——第 1 部分：通用要求；

——第 2 部分：数字证书；

——第 3 部分：业务办理和应用指南；

——第 4 部分：应用服务接口；

——第 5 部分：第三方应用接入要求和测试方法；

——第 6 部分：商事主体电子印章图像；

——第 7 部分：商事主体电子印章备案。

本文件由深圳市政务服务数据管理局提出并归口。

本文件起草单位：深圳市政务服务数据管理局、深圳市市场监督管理局、深圳市信息安全管理中心、深圳市标准技术研究院、北京数字认证股份有限公司、广东省电子商务认证有限公司。

本文件主要起草人：曾勇、陈胜、李苏、姚逸滨、程小茁、罗菁春、黄立、董安波、谷鹏、简超、周鑫、刘家雄、饶文刚、林宇群、张雯、周佩雯、穆端端、林雄杰、胡静、李强、王惠惠、赖慧诗、俞科、王志勇、陈慧铧、刘艳、周维、李玮。

电子印章
第2部分：数字证书

1 范围

本文件规定了电子印章中数字证书的分类和要求。

本文件适用于电子印章中数字证书的签发和验证，也可用于电子印章的制作、签署和验证。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。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 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB 32100—2015 法人和其他组织统一社会信用代码编码规则

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

ZWFW C 0120—2018 国家政务服务平台标准 统一电子印章 印章技术要求

DB4403/T 383.1—2023 电子印章 第1部分：通用要求

3 术语和定义

DB4403/T 383.1—2023界定的以及下列术语和定义适用于本文件。

3.1

SM2算法 SM2 algorithm

由GB/T 32918定义的一种椭圆曲线密码算法。

[来源：GB/T 38540—2020,3.8]

3.2

SM3算法 SM3 algorithm

由GB/T 32905定义的一种杂凑算法。

[来源：GB/T 38540—2020,3.9]

3.3

证书认证机构 certification authority

受用户信任，负责创建和分配数字证书的权威机构。

[来源：GB/T 20518—2018,3.5,有修改]

4 缩略语

下列缩略语适用于本文件。

ASN：抽象语法表示法（abstract syntax notation）
C：国家（country）
CA：证书认证机构（certification authority）
CN：通用名（common name）
DER：特定编码规则（distinguished encoding rules）
DN：可辨别名（distinguished name）
O：机构（organization）
OID：对象标识符（object identifier）
OU：机构单位（organization unit）

5 分类

5.1 制章者数字证书

制章者数字证书是由CA为电子印章制章者发放的数字证书，用于电子印章的制作。

5.2 印章所有者数字证书

印章所有者数字证书是由CA为电子印章所有者发放的数字证书，用于电子印章的制作和使用。

6 要求

6.1 制章者数字证书要求

制章者数字证书应符合GB/T 20518—2018的要求，按DER编码格式存放，其主体DN命名示例见A.1。

6.2 印章所有者数字证书要求

6.2.1 概述

6.2.1.1 印章所有者数字证书应符合GB/T 20518—2018的要求，按DER编码格式存放，其主体DN命名示例见A.2。
6.2.1.2 政务电子印章的印章所有者数字证书还应符合ZWFW C 0120—2018的规定。
6.2.1.3 商事主体和其他机构电子印章的印章所有者数字证书还应符合6.2.2至6.2.4的要求。

6.2.2 签名算法

数字证书采用的签名算法应符合以下要求：
a) 采用基于SM2和SM3签名算法，OID标识为1.2.156.10197.1.501；
b) 采用CA签发该证书所使用的密码算法的标识符，并与签名算法域中算法标识符一致；
c) 符合国家密码主管部门对密码算法的规定。

6.2.3 主体项

主体项描述了数字证书中公钥相对应的证书持有者信息。主体DN各项命名和编码规范见表1，示例见附录A。

表1　主体 DN 命名和编码规范

数据项类型	数据项名称	数据项定义（说明）	编码格式	备注
C	国家	CN	PrintableString	必选
S	省份	主体所在省份，用中文全称表示，如广东省	UTF8String	必选
L	城市	主体所在城市，用中文全称表示，如深圳市	UTF8String	必选
O	组织名称	对于政务电子印章，应为统一社会信用代码+组织名称。 对于商事主体和其他机构电子印章，采用智能移动终端为存储介质的，应为统一社会信用代码+组织名称；采用智能密码钥匙、服务器密码机、云服务器密码机为存储介质的，应为组织名称。	UTF8String	必选
OU	部门名称	组织内设部门的名称	UTF8String	可选
CN	名称	对于政务电子印章，应为印章编码。 对于商事主体和其他机构电子印章，采用智能移动终端为存储介质的，应为印章编码；采用智能密码钥匙、服务器密码机、云服务器密码机为存储介质的，电子公章应为商事主体用户及其他机构用户的名称，职务章、个人名章应为姓名。	UTF8String	必选

6.2.4　专用扩展项

6.2.4.1　实体唯一标识

专用扩展项中的实体唯一标识符合以下要求：

a)　实体唯一标识代表一个证书持有者身份的唯一编码，其 OID 标识应为 2.16.156.112548；

b)　实体唯一标识的 OID 编码结构应符合以下格式：用户编号+“@”+CA 编号（4 位）+证件号码类型代码（2 位）+安全标识（1 位）+证件号码。实体唯一标识的 OID 编码结构说明应符合附录 B 的要求，实体唯一标识的 OID 编码结构示例见附录 C；

c)　数据的总长度不应超过 128 字节；

d)　属性的编码应使用 UTF8String；

e)　该扩展项应签发。

6.2.4.2　统一社会信用代码

专用扩展项中的统一社会信用代码符合以下要求：

a)　OID 标识应为 1.2.86.11.7.7550243.1；

b)　编码规则应符合 GB 32100—2015 的要求；

c)　数据的总长度不应超过 128 字节；

d)　属性的编码应使用 UTF8String；

e)　该扩展项应签发。

附 录 A
（资料性）
主体 DN 命名示例

A.1 制章者数字证书示例

以深圳市市场监督管理局为例，其制章者数字证书的主体DN见表A.1。

表 A.1 制章者数字证书的主体 DN 示例

数据项类型	示例内容	数据项定义（说明）	备注
C（国家）	CN	CN	必选
S（身份）	广东省	主体所在省份	必选
L（城市）	深圳市	主体所在城市	必选
O（组织名称）	深圳市市场监督管理局	所在组织名称	必选
OU（部门名称）	/	所在部门名称	可选
CN（名称）	深圳市市场监督管理局	名称	必选

A.2 印章所有者数字证书示例

A.2.1 政务用户印章所有者数字证书

以深圳市市场监督管理局广告处为例，其印章所有者数字证书的主体DN见表A.2。

表 A.2 政务用户印章所有者数字证书的主体 DN 示例

数据项类型	示例内容	数据项定义（说明）	备注
C（国家）	CN	CN	必选
S（身份）	广东省	主体所在省份	必选
L（城市）	深圳市	主体所在城市	必选
O（组织名称）	11440300MB2C927392深圳市市场监督管理局	统一社会信用代码+所在组织名称	必选
OU（部门名称）	广告处	所在部门名称	可选
CN（名称）	1108*******0041	印章编码	必选

A.2.2 商事主体用户和其他机构用户印章所有者数字证书

A.2.2.1 智能移动终端数字证书

以深圳市某某某有限责任公司为例，采用智能移动终端时，其印章所有者数字证书的主体DN见表A.3。

表 A.3　商事主体用户和其他机构用户印章所有者数字证书的主体 DN 示例 1

数据项类型	示例内容	数据项定义（说明）	备注
C（国家）	CN	CN	必选
S（身份）	广东省	主体所在省份	必选
L（城市）	深圳市	主体所在城市	必选
O（组织名称）	91440300MA51234567深圳市某某某有限责任公司	统一社会信用代码+所在组织名称	必选
OU（部门名称）	/	所在部门名称	可选
CN（名称）	1108*******0051	印章编码	必选

A.2.2.2　智能密码钥匙、服务器密码机和云服务器密码机数字证书

A.2.2.2.1　电子公章

以深圳市某某某有限责任公司为例，其印章所有者数字证书的主体DN见表A.4。

表 A.4　商事主体用户和其他机构用户印章所有者数字证书的主体 DN 示例 2

数据项类型	示例内容	数据项定义（说明）	备注
C（国家）	CN	CN	必选
S（身份）	广东省	主体所在省份	必选
L（城市）	深圳市	主体所在城市	必选
O（组织名称）	深圳市某某某有限责任公司	所在组织名称	必选
OU（部门名称）	/	所在部门名称	可选
CN（名称）	深圳市某某某有限责任公司	所在组织名称	必选

A.2.2.2.2　职务章、个人名章

以深圳市某某某有限责任公司负责人张某某为例，其印章所有者数字证书的主体DN见表A.5。

表 A.5　商事主体用户和其他机构用户印章所有者数字证书的主体 DN 示例 3

数据项类型	示例内容	数据项定义（说明）	备注
C（国家）	CN	CN	必选
S（身份）	广东省	主体所在省份	必选
L（城市）	深圳市	主体所在城市	必选
O（组织名称）	深圳市某某某有限责任公司	所在组织名称	必选
OU（部门名称）	/	所在部门名称	可选
CN（名称）	张某某	姓名	必选

附 录 B
（规范性）
实体唯一标识的 OID 编码结构说明

印章所有者数字证书专用扩展项实体唯一标识的OID编码结构说明如下：

——用户编号：是证书持有者所持有证书的序号，用户编号宜采用阿拉伯数字，例如一个商事主体用户申请2个证书，则第一张证书的用户编码为1，第2张证书的用户编号为2，依次类推；

——CA编号：应为CA首次获取电子认证服务许可证上的“许可证编号”的后四位数字；

——证件类型代码：是证书持有者申请数字证书所使用证件的证件类型代码，证书类型和证件类型代码见表B.1；

——安全标识应符合以下要求：

- 电子公章数字证书中的统一社会信用代码采用明文格式签发；
- 职务章、个人名章数字证书中的证件号码采用哈希加密方式签发；
- 安全标识使用 1 位数字代表不同含义，“0”代表其后的“证件号码”为明文格式签发，“2”代表其后的“证件号码”为哈希加密方式签发。

表 B.1 证书类型与证件类型代码对应表

证书类型	办理证书时可使用的证件名称	证件号码类型名称	证件类型号码类型代码
电子公章数字证书	统一社会信用代码证/事业法人登记证/营业执照/社团登记证/民办非企业登记证/基金会登记证/工会登记证	统一社会信用代码号	XY
职务章、个人名章数字证书	身份证/军官证/士兵证/护照/回乡证/港澳台居民居住证	身份证号码/军官证号/士兵证号/护照号/回乡证号/港澳台居民居住证号	SF/JG/SB/HZ/HX/JZ

附 录 C
（资料性）
实体唯一标识的OID编码结构示例

印章所有者数字证书专用扩展项实体唯一标识的OID编码结构示例见表C.2。

表C.2 印章所有者证书专用扩展项实体唯一标识示例

证书类型	说明	安全标识	示例
电子公章数字证书	办理证书时提供的证件为统一社会信用代码，证件号为914403001234567890，CA编号为1001，该CA为用户签发的第1张数字证书。	0	1@1001XY0+914403001234567890
职务章、个人名章数字证书	办理证书时提供的证件为居民身份证，公民身份号码为342222********5678，CA编号为1001，该CA为用户签发的第1张数字证书。	2	1@1001SF2+HASH(342222********5678)

参 考 文 献

[1] GB/T 38540—2020 信息安全技术 安全电子签章密码技术规范