

## 《电子印章 第2部分：数字证书》解读

《电子印章 第2部分：数字证书》已于2023年11月2日发布，于2023年12月1日实施，现就编制背景、主要内容解读如下：

### 一、《电子印章 第2部分：数字证书》编制背景

自2019年开始，深圳就开始探索电子印章的推广应用，并于2021年1月正式印发《深圳市商事主体电子印章管理暂行办法》，同年3月上线试运行商事主体电子印章管理系统，实现了电子营业执照和电子印章的同步发放。全市商事主体均可免费申领电子营业执照和一套四枚电子印章，初步构建了以电子营业执照作为主体资格证明、以电子印章签章为行为确认的服务体系。另外，经广东省政务服务数据管理局同意，深圳还将建设广东省电子印章平台深圳分中心，实现政务电子印章的发放和管理。

为进一步整合资源，提升服务效率，深圳在上述系统的基础上建设了全市统一的电子印章管理平台，为全市党政机关、商事主体以及其他机构提供一体化的电子印章发放和管理服务，推动两种电子印章在同一应用场景的共同使用，构建既符合国家和广东省的法规标准要求、又具有深圳特色的统一电子印章管理和应用体系。

深圳电子印章系统所发放的政务电子印章和商事主体电子印章，均遵循 GB/T 38540—2020《信息安全技术 安全电子签章密码技术规范》的要求，可以在同一应用场景中进行使用，两者都通过电子印章管理系统进行统一管理和提供电子印章发放、验章、验签等服务；既要与符合 GB/T 38540—2020 的电子印章，也要与非标准的电子印章或数字签名共同使用；还要与北京、上海、广州等地区的电子印章实现互信互认。

因此，面对如此复杂多样的电子印章，制订《电子印章 第 2 部分：数字证书》这一地方标准，具有明显的必要性和紧迫性。针对电子印章各种可能的用户对象和储存介质，规定各类电子印章中的数字证书需要共同遵守的技术和业务规则，以协助各类用户准确快速理解电子印章中数字证书的技术特性。标准的编制一是有利于对现有国家和行业标准中未明确但工作中又急需的电子印章数字证书问题达成共识，二是有利于对深圳电子印章工作中所遇到的个性化问题予以明确，以全面推动电子印章在深圳市各类电子政务、公共服务、商业活动等领域的综合应用，改善和优化营商环境。

## **二、本文件的总体结构和主要内容说明**

《电子印章 第 2 部分：数字证书》标准结构包括 6 个章节，以下对标准中的主要条款进行简要说明。

### （一）第一章：范围

本章节规定了本文件的主要内容，即电子印章中数字证书的分类和要求；以及适用范围，即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。

### （二）第二章：规范性引用文件

本章节给出了标准编制过程中引用的相关文件，包括 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》、ZFW 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》和 DB4403/T 383.1《电子印章 第1部分：通用要求》等。

### （三）第三章：术语和定义

本章节给出了标准编制过程中涉及到的术语和定义，包括 SM2 算法、SM3 算法、证书认证机构。

### （四）第四章：缩略语

本章节规定了适用于本文件的 9 个缩略语，包括抽象语法表示法 (abstract syntax notation)、国家 (country)、证书认证机构 (certification authority)、通用名 (common name)、特定编码规则 (distinguished encoding rules)、

可辨别名 (distinguished name)、机构 (organization)、对象标识符 (object identifier)、机构单位 (organization unit)。

#### (五) 第五章：分类

本章节对深圳电子印章系统的数字证书进行了分类，明确了“制章者数字证书”和“印章所有者数字证书”的说明，本系列标准只包含这两类的要求。

#### (六) 第六章：要求

本章节陈述了数字证书应该满足的要求。在 GB/T 20518—2006 基础上，根据本市实际特点，对数字证书签名算法、主体和专用扩展域的取值进行规范，规定通用格式、必备项、主题命名规则等内容，确保不同 CA 体系下的数字证书能够在全市活动中进行通用。特别针对数字证书在不同存储介质的实际情况，通过定义主体 DN 数据项中的名称 (CN) 和组织名称 (O) 的具体规则解决了各家 CA 的证书格式不完全一致的问题。本文件设置了数字证书的专用扩展项，新增了实体唯一标识和统一社会信用代码。同时新增了对于实体唯一标识中的职务章\个人名章数字证书中的证件号码采用哈希加密方式签发，并增加了哈希加密方式安全标识，体现了对个人隐私的保护。

#### (七) 附录

附录 A（资料性）主体 DN 命名示例，对主体 DN 进行了示例说明，对“制章者数字证书”和“印章所有者数字证书”具体举例，其中印章所有者证书针对数字证书在不同存储介质的实际情况做出了分类举例。附录 B（规范性）实体唯一标识的 OID 编码结构说明，对专用扩展项中的实体唯一标识的 OID 编码结构进行了具体说明。附录 C（资料性）实体唯一标识的 OID 编码结构示例，对印章所有者证书专用扩展项实体唯一标识按照证书类型给出了具体示例。

### 三、附则

本文件由深圳市政务服务数据管理局提出并归口，由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参与起草。