《电子印章　第 2 部分：数字证书》（送审稿）编制说明

一、项目背景

为进一步优化营商环境，推动数字政府和智慧城市建设，2020 年深圳市建设并上线试运行深圳市统一电子印章管理系统（以下简称“电子印章系统”），进行政务电子印章和商事主体电子印章的发放和全面应用。经广东省政数局同意，还将在该系统基础上建设广东省电子印章系统深圳分中心。为全面推动电子印章的应用，2021 年 1 月 8 日，深圳市正式发布了《深圳市商事主体电子印章管理暂行办法》，通过电子印章系统为全市所有商事主体免费发放 1 套 4 枚电子印章（包括法定名称章、财务专用章、合同专用章、负责人章）。

电子印章系统面向深圳市 360 万以上的商事主体和相关自然人发放商事主体电子印章，面向数以千计的党政机关、事业单位、国有企业以及相关自然人发放政务电子印章，未来还将面向社会组织、工会和律师事务所等其他类型组织、所有自然人发放其他类型的电子印章。截至 2022 年 9 月底，我市已为 2000 余家党政机关和事业单位发放政务电子印章 7180 枚，用章量超过 1.39 亿次；为 98 万家商事主体发放印章 327 万枚；其中已主动领取电子印章的商事主体为 26 万家，领取的电子印章数量超过 67 万枚，用章量超过 3272 万次。

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。但是两者在技术架构和使用介质上有所区别，商事主体电子印章的密钥完全由用户掌握和控制，介质以手机端为主，而政务印章的密钥由电子印章管理系统控制，主要的介质是无介质（与政务用户的统一身份相关联）。

在实际应用中，根据不同的用户类型和业务需求，电子印章的名称、载体、形式、使用方法、技术要求也各不相同，例如印章类型就分为名称章、合同章、财务章等。深圳的电子印章既可以与共同符合 GB/T 38540—2020 的电子印章在

同一场景下使用，也可以和符合 PKI 相关国际标准数字签名或非标准（不符合 GB/T 38540—2020）电子印章共同使用。此外，深圳电子印章还与北京、上海、广州等地区在技术上实现了互信互认，也可以在同一场景下共同使用。

在商事主体方面，目前我国与电子印章最主要的国家标准就是 GB/T 38540—2020《信息安全技术　安全电子签章密码技术规范》，它规定了电子印章和电子签章的数据结构定义，以及相应的生成与验证流程。此外，电子印章密码技术和信息安全等相关的主要标准共有 66 项，其中国家标准 37 项；行业标准 21 项；广东省地方标准 3 项；此外还有 5 项重要的内部规范，包括 4 项关于统一电子印章的国家政务服务平台标准、1 项关于电子印章平台接入指引的广东省政务服务标准。在政务方面，目前电子印章在党政机关的应用已较为普及，国家层面也发布了 GB/T 33481—2016《党政机关电子印章应用规范》、ZWFW C0118 至 C0122《国家政务服务平台统一电子印章》系列内部标准和 GDZW 0016《广东省统一电子印章平台接入规范》内部标准。

深圳电子印章系统既包括政务电子印章也包括商事主体电子印章；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。《电子印章》系列地方标准旨在为深圳市全面推广和应用电子印章过程中，针对相关国家和行业标准中尚未明确规定或细节不明晰的基本概念、业务规则、技术要求、操作程序等，以及某些深圳电子印章特有的应用方法和模式，制订符合深圳市实际应用需求的地方标准，以解决电子印章应用推广过程中一些急需解决的难题。

因此，面对如此复杂多样的电子印章，非常有必要制订《电子印章　第 2 部分：数字证书》这一地方标准，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目前现有标准中未明确但工作中又急需的商事主体电子印章达成共识，二是有利于对深圳电子印章工作中所遇到的常规性问题予以明确，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、工作简况

（一）任务来源

《电子印章》系列地方标准在2021年4月依据《深圳市市场监督管理局关于下达2021年第一批深圳市地方标准计划项目任务的通知》而立项，由深圳市政务服务数据管理局提出并归口，由深圳市标准技术研究院负责牵头起草，深圳市信息安全管理中心、北京数字认证股份有限公司、广州金格数安科技有限公司、北京国脉信安科技有限公司、平安国际智慧城市科技股份有限公司、深圳市公安局参与起草。

本文件是《电子印章》系列地方标准的第2部分。

（二）主要起草过程

1．规划阶段：2021 年 1 月，《深圳市商事主体电子印章管理暂行办法》发布，起草单位根据我市电子印章的实际工作需要，提出编制《电子印章》系列地方标准的设想，并开展预研工作。

2．立项起草阶段：2021 年 4 月，深圳市市场监督管理局批准该标准制订任务。起草单位组织相关部门和人员正式成立编制组。

3．调研阶段：2021年6月至7月，起草单位对市内四家电子认证服务机构等相关方进行调研，详细了解各机构的证书格式、证书应用模式等现状。2021年 8 月至 9 月间，对首批试点单位进行市电子印章数字证书应用需求的现场调研。

4．编制阶段：2021年8月至2022年9月，编制组定期召开多次讨论会，对标准的各项内容进行多次详细讨论，完成第一版标准征求意见稿的编制。同时在市内四家证书认证机构中开展技术指南验证工作，论证了技术可行性。

5. 征求意见阶段：2022年10月至11月，编制组完成向深圳市信息安全管理中心的意见征求，并针对意见对标准进行修改。2022 年 12 月，编制组通过深圳市政务服务数据管理局发函征求全市各部门意见，其中本部分反馈无意见。2023 年 2 月起，编制组将通过深圳市政务服务数据管理局和市标准化主管部门面向社会公众公开征求意见。

6. 组织送审阶段（计划）：2023 年 3 月，编制组将完成标准送审稿的编制，

并提交市标准化主管部门进行审查。

三、标准编制依据

（一）工作原则

1. 遵循国家标准原则：本标准在 GB/T 20518—2006《信息安全技术　公钥基础设施　数字证书格式》、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》等国家技术标准基础上，对数字证书进行规范，以实现数字证书在全市范围内通用。

2. 标准兼容原则：在数字证书标准编制过程中，需要从长远考虑，尽量和已有的国家、行业以及相关标准兼容。

3. 需求主导原则：标准的制定必须充分考虑全市各共享部门的需求及现有的特点，所制定的数字证书标准应当满足全市范围内通用的管理、共享和服务的基本需求。

4. 可扩展性原则：对于各用户关键的、急需的，同时又容易达成一定共识的数据首先纳入本标准，对于仍存在不确定性、或很难达成共识的，选择恰当的时机在标准后续的修订过程中逐步纳入。

（二）技术原则

本部分在编制中引用了最新版本的国家及行业规范，如 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 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》等标准，并结合我市的实际情况和工作特点制定。

四、主要技术内容

范围（第 1 章）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，即电子印章中数字证书的签发和验证，和电子印章的制作、签署和验证。

规范性引用文件（第2章）根据编制需要，将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 32905-2016《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》列入本章。

在遵循本标准第一部分中通用的术语和定义的基础上，术语和定义（第 3 章）规定了本文件中适用的术语和定义，例如：“SM2 算法”“SM3 算法”“证书认证机构”等。其中，“SM2 算法”和“SM3 算法”都针对深圳市电子印章中数字证书的特性进行了修改，以更符合深圳市电子印章的实际工作。

缩略语（第 4 章）规定了本文件中通用的缩略语，如“对象标识符”“特定编码规则”“抽象语法表示法”“证书认证机构”。

数字证书的分类（第 5 章）和要求（第 6 章）章节的主要内容是在参考GB/T 20518—2006《信息安全技术 公钥基础设施　数字证书格式》、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》基础上，结合我市商事主体和政府的实际需求制定。

其中数字证书分类（第 5 章）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。

数字证书要求（第 6 章）章节中，在 GB/T 20518—2006 基础上，根据本市的实际特点，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。本标准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。

附录 A 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 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。以及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进行了具体示例说明。

五、知识产权问题

本文件不涉及专利等知识产权问题。

六、重大意见分歧的处理依据和结果

无。

七、实施标准的措施建议

标准发布之后，建议主管部门从以下几个方面开展标准推广与实施工作：

1. 开展宣贯培训活动。按照《深圳市地方标准管理办法》的相关要求，地方标准发布实施后，由主管部门组织和督导本部门、本行业开展地方标准的宣贯、培训和实施工作。可充分利用电视、网络、报纸等媒体，以多渠道、多手段，线上、线下多种形式向标准应用相关方推广宣传标准，确保标准应用相关方准确理解并实施标准。

2. 开展标准实施检查工作。制定标准实施检查制度及标准实施检查工作计划，开展标准实施检查工作，记录标准实施检查情况并形成实施检查报告。

3. 开展用户满意度评价。制定用户满意度评价表，完成用户满意度评价工作，编制用户满意度评价报告，不断完善电子印章工作，提升用户满意度。

4. 持续改进完善标准。在标准实施的过程中，按照标准化的基本理念，通过实施检查、重复验证、持续改进等方式，确保标准实施有效，对我市电子印章工作起到良好的指导作用。

八、其他需要说明的事项

无。