

DB4403

深圳市地方标准

DB4403/T 383.3—2023

电子印章 第3部分：业务办理和应用指南

Electronic seal—
Part 3: Business and application guidelines

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	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 电子印章系统框架	2
5 电子印章业务办理	2
6 电子印章应用	3
附录 A（规范性） 验章结果展示要求	7
参考文献	9

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3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、深圳市不动产登记中心、中国建设银行股份有限公司深圳市分行、深圳市水务（集团）有限公司、深圳市南山区政务服务数据管理局、上海浦东发展银行股份有限公司深圳分行。

本文件主要起草人：俞科、曾勇、李苏、姚逸滨、王志勇、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、颜海龙、朱彦、李桂珠、黄浚婷、梁晓波、陈胜、陈慧铨、马玮珣、张报建、周维、李玮。

电子印章

第3部分：业务办理和应用指南

1 范围

本文件规定了电子印章系统框架、电子印章主要业务的办理流程，以及电子印章的典型应用模式。

本文件适用于政务用户、商事主体用户、其他机构用户办理电子印章各项业务，在政务、商务、公共服务等领域使用电子印章，也适用于应用单位在其业务或信息系统中整合电子印章服务功能，供用户在其业务或信息系统中使用电子印章。

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 33481—2016 党政机关电子印章应用规范
- GB/T 38540—2020 信息安全技术 安全电子签章密码技术规范
- GM/T 0031—2014 安全电子签章密码技术规范
- DB4403/T 383.1—2023 电子印章 第1部分：通用要求
- DB4403/T 383.2—2023 电子印章 第2部分：数字证书

3 术语和定义

DB4403/T 383.1—2023和DB4403/T 383.2—2023界定的以及下列术语和定义适用于本文件。

3.1

应用单位 application organization

在其信息系统中整合了电子印章服务功能的单位。

3.2

第三方应用系统 third-party application system

应用单位（3.1）按照业务需要开发的，整合了电子印章服务功能的信息系统。

3.3

受信任的电子印章体系和PKI体系 trusted electronic seal system and PKI system

与电子印章系统实现互认互信的其他电子印章体系和公钥基础设施（PKI）体系的统称。

3.4

电子印章服务系统 electronic seal service system

电子印章系统的子系统，为用户提供电子印章服务。

注：包括移动端应用程序（APP客户端、小程序）和PC端应用程序（PC客户端、Web端）等。

3.5

验章 validation signature

对签章结果文件的真实性和完整性进行验证的过程。

[来源：GA/T 1106—2013, 3.5, 有修改]

4 电子印章系统框架

电子印章系统框架如图 1 所示，具体包括：

- 电子印章系统由电子印章运营系统、电子印章服务系统、电子印章应用服务接口三部分组成。电子印章系统与广东省电子印章平台、深圳市公安电子印章备案库对接，实现电子印章的备案管理；与符合深圳市电子政务电子认证管理相关要求的 CA 对接，为用户提供电子印章所需的 CA 服务；与受信任的电子印章体系和 PKI 体系对接，实现电子印章跨区域、跨层级、跨部门互认互信；
- 电子印章管理服务机构通过电子印章运营系统提供电子印章运营管理相关服务；
- 用户通过电子印章服务系统申请、管理、使用和验证电子印章，也可以通过第三方应用系统使用和验证电子印章；
- 第三方应用系统通过电子印章应用服务接口实现与电子印章系统对接，在其业务中整合电子印章服务功能。

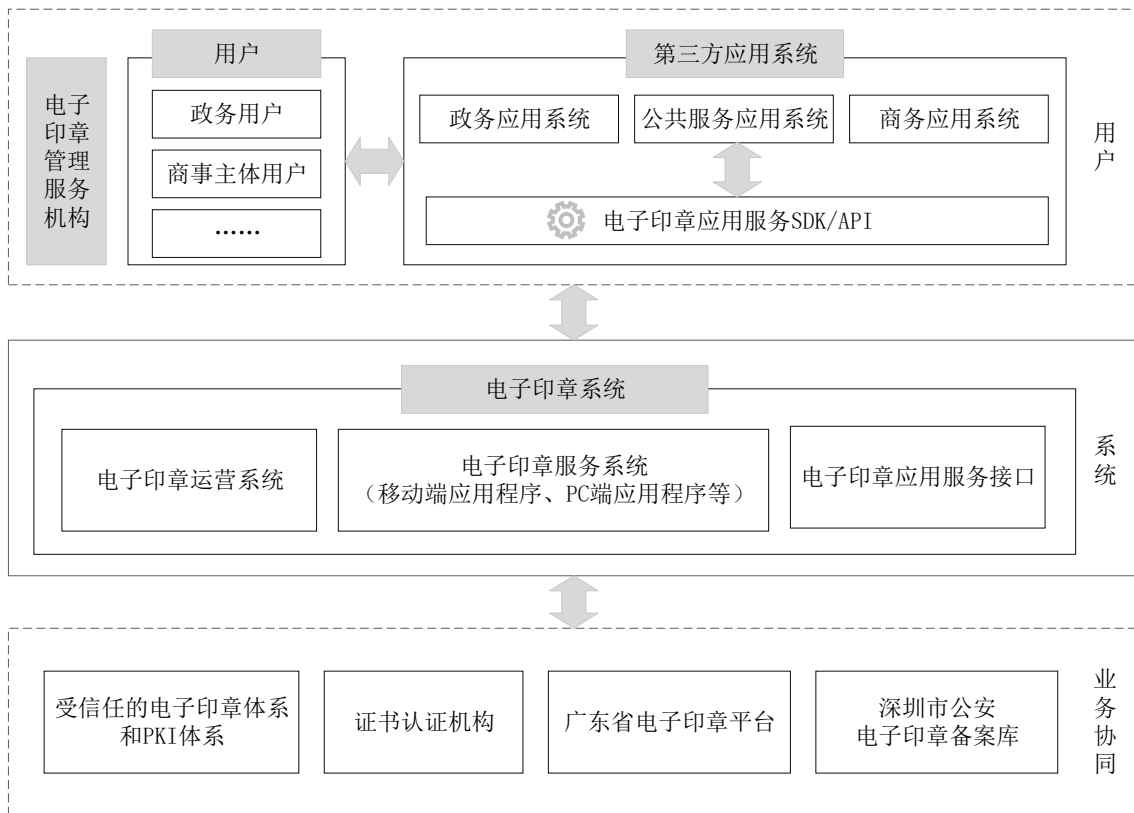


图 1 电子印章系统框架

5 电子印章业务办理

5.1 概述

电子印章业务办理包括申请、领取、授权、变更和注销等。

5.2 申请

5.2.1 需要电子印章的用户，应按照相关管理规定向电子印章管理服务机构申请电子印章。

5.2.2 申请电子公章的，应提供机构、机构负责人以及经办人的合法身份证明材料；政务用户申请法定名称章的，还应提供上级主管部门批准同意的证明材料；需要制作包含外文的电子印章的，还应提供经本机构确认的翻译文本。

5.2.3 申请电子职务章的，应提供持有人、所在机构、机构负责人以及经办人的合法身份证明材料。

5.2.4 对于新设立商事主体，在完成登记设立的同时，电子印章系统同步完成一套共四枚电子印章（包括法定名称章、财务专用章、合同专用章、负责人章）的申请，商事主体无需另行提交申请。

5.3 领取

用户完成电子印章申请后，需领取才能使用电子印章。

5.4 授权

5.4.1 机构负责人是机构电子公章和负责人名章的管理员，具有电子印章的所有权限，也可授权他人作为电子印章管理员和电子印章操作人；电子职务章由持有人自行保管和使用。

5.4.2 需要将电子印章授权给他人的用户，应按照相关管理要求向电子印章管理服务机构申请，申请时应提供所在机构、机构负责人以及经办人的合法身份证明材料。

5.4.3 用户应建立内部管理制度，明确电子印章的管理员和操作人、审批和使用流程。电子公章和负责人名章的使用审批流程应与实物印章的使用审批流程保持一致，应严格按照审批权限使用电子印章。

5.5 变更

当用户的机构名称、负责人或机构类型发生变更时（机构类型变更指商事主体内资企业转外资企业、外资企业转内资企业），原电子印章自动失效，应按照5.2和5.3节的要求重新申请和领取电子印章。

5.6 注销

用户因以下情形的，应向电子印章管理服务机构申请注销电子印章：

——对于机构注销或撤并的用户，原有电子印章自动失效；

——对于不再使用电子印章的用户，机构负责人或电子职务章持有人应通过电子印章服务系统申请注销电子印章：

- 注销电子印章时应提供机构、负责人以及经办人的合法身份证明材料；
- 注销电子职务章时也可仅由印章持有人提供其合法身份证明材料。

6 电子印章应用

6.1 概述

电子印章应用模式主要包括以下四种：

——分散式用章：用户利用电子印章服务系统对电子文件进行签章或验章；

——批量式用章：用户利用电子印章服务系统的PC客户端，或在其应用系统中集成批量签章功能，对多个电子文件进行集中批量签章；

——应用集成用章：第三方应用系统通过整合电子印章系统的SDK/API应用服务接口，为其用户提供单页签章、多页签章、骑缝章签章、多文件签章等签章服务和验章服务，以及用户身份认证、数字签名和验签服务；

——混合用章：深圳市电子印章与受信任的电子印章体系和PKI体系的电子印章或数字签名交叉使用。

6.2 分散式用章

6.2.1 用章文件

分散式用章支持的电子文件格式有：

- 待签章电子文件格式应为流式文件格式，如doc、docx、xls、xlsx等，或版式文件格式，如pdf、ofd等；
- 待验证电子文件格式应为pdf、ofd等版式文件格式。

6.2.2 用章环境

分散式用章对终端环境要求如下：

- PC端：PC端应安装电子印章PC客户端或Web浏览器，具备互联网连接功能。PC端支持所有用户的分散式用章；
- 智能移动终端：智能移动终端应安装电子印章移动端应用程序，具备互联网连接功能。智能移动终端仅支持商事主体用户的分散式用章。

6.2.3 用章方式

根据用章环境不同，分散式用章的方式有如下几种：

- PC端：用户可通过电子印章服务系统的PC端应用程序，对电子文件进行签章、验章、撤章等操作。支持的用章功能包括单页签章、多页签章、骑缝章签章、撤章等；撤章应由印章操作人本人完成，且只支持撤销最后一次加盖的电子印章；
- 智能移动终端：用户可通过电子印章服务系统的移动端应用程序，对电子文件进行签章、验章操作。

6.3 批量式用章

6.3.1 用章文件

批量式用章支持的待签章文件应为版式文件格式，如pdf、ofd等。

6.3.2 用章环境

批量式用章对终端环境的要求如下：

- PC端：PC端应安装电子印章PC客户端应用程序，具备互联网连接功能；
- 服务器密码机：服务器密码机应符合DB4403/T 383.1的要求并提前在电子印章系统备案，用户的第三方应用系统应已完成与电子印章应用服务接口和服务器密码机的对接，集成批量签章功能。

6.3.3 签章介质选择

用户根据以下业务需求和应用场景，选择相应的签章介质：

- 对于单批次签章文件数量 ≤ 10 份，且单份文件大小 ≤ 50 M的场景，宜使用智能移动终端介质配合电子印章PC客户端应用程序对批量文件集中签章；
- 对于单批次签章文件数量 ≤ 100 份，且单份文件大小 ≤ 500 M的场景，宜使用USBKey介质配合电子印章PC客户端应用程序对批量文件集中签章；

——服务器密码机介质适用的单批次文件数量和单份文件大小不受限制。

6.3.4 用章方式

6.3.4.1 PC 客户端

用户可根据需求选择智能移动终端或USBKey,通过使用电子印章服务系统的PC客户端应用程序完成对多个电子文件的批量签章。

6.3.4.2 系统对接

用户的第三方应用系统可通过集成和调用电子印章系统的应用服务接口,完成对多个电子文件的批量签章。使用系统对接方式的商事主体用户应自行配备服务器密码机。

6.4 应用集成用章

6.4.1 用章文件

用户应按照第三方应用系统的要求准备用章文件。

6.4.2 用章环境

用户应按照第三方应用系统的要求准备用章环境。

6.4.3 用章方式

6.4.3.1 身份认证

用户应通过扫描第三方应用系统提供的登录二维码或调用移动端应用程序完成身份认证。

6.4.3.2 签章

6.3.3.2.1 智能移动终端用户签章

用户可通过第三方应用系统提供的以下方式进行签章:

- 扫码签章:通过扫描第三方应用系统所提供的签章二维码完成签章;
- 调用移动端应用程序签章:在第三方应用系统中选择签章功能,第三方应用系统通过调用指定的移动端应用程序完成签章;
- 推送签章:发起签章任务的人在第三方应用系统中选择签章功能,第三方应用系统将待签章任务发送至印章操作人,印章操作人通过移动端应用程序完成签章。

6.3.3.2.2 USBKey 用户签章

用户可通过第三方应用系统提供的以下方式进行签章:

- 直接对文件签章:打开电子印章服务系统的PC客户端应用程序,插入USBKey,按照第三方应用系统指引完成签章;
- 推送签章:发起签章任务的人在第三方应用系统中选择签章功能,第三方应用系统将待签章任务发送至印章操作人,印章操作人打开电子印章服务系统的PC客户端应用程序接收签章任务,插入USBKey,按照系统指引完成签章。

6.4.3.3 验章

用户在第三方应用系统中选择验章功能，第三方应用系统通过调用电子印章系统验章接口，对待验证文件进行验章。验章结果展示应符合附录A的要求。

6.4.3.4 数字签名

6.3.3.4.1 智能移动终端用户签名

用户可通过第三方应用系统提供的以下方式完成数字签名：

- 扫码签名：通过扫描第三方应用系统所提供的签名二维码完成数字签名；
- 调用移动端应用程序签名：在第三方应用系统中选择数字签名相关功能，第三方应用系统调用指定的移动端应用程序，完成数字签名。

6.3.3.4.2 USBKey 用户签名

用户可在第三方应用系统中采用USBKey对电子文件或数据进行数字签名。

6.5 混合用章

6.5.1 受信任的电子印章体系和 PKI 体系

以下体系可与电子印章进行混合用章：

——满足以下要求的受信任电子印章体系：

- 其电子印章和电子签章至少符合 GB/T 38540—2020 或 GM/T 0031—2014 或 GB/T 33481—2016 的要求；
- 是政府认可的公共电子印章服务体系；
- 其应用系统能够有效识别和验证深圳市电子印章签署的电子文件；
- 与深圳市电子印章主管部门达成互认互信协议。

——满足以下要求的受信任PKI体系：

- 其数字证书和数字签名至少符合 GB/T 38540—2020 或 GM/T 0031—2014 或 GB/T 33481—2016 的要求；
- 数字证书由国家认可的证书认证机构发放；
- 其应用系统能够有效识别和验证深圳市电子印章签署的电子文件；
- 得到深圳市电子印章主管部门的认可。

6.5.2 用章方式

受信任的电子印章体系和PKI体系的用户应使用其体系指定的系统对电子文件进行签章和验章，深圳市电子印章用户应使用深圳市电子印章系统对电子文件进行签章和验章。混合用章后的签章文件验章结果展示应符合附录A的要求。

附录 A
(规范性)
验章结果展示要求

用户可通过电子印章服务系统、第三方应用系统对待验证电子文件进行验章，相关信息系统提供的验章功能除支持对深圳市电子印章系统用户签章后的电子文件验证外，还应支持对受信任的电子印章体系和PKI体系用户签章或数字签名后的电子文件的验证。验章结果展示包含以下内容：

- 展示电子文件名称、验证结果、签章和签名数量，若验证不通过，应给出不通过原因；
- 展示电子文件中每个电子签章或数字签名的验证结果是否通过，若验证不通过，应给出相应提示；
- 展示电子文件中每个电子签章验证信息，如签章为受信任的电子印章体系电子印章签章，应给出标识，电子签章验证结果展示信息符合表 A.1 的要求；
- 展示电子文件中每个数字签名验证信息，如数字签名为受信任的 PKI 体系数字签名，应给出标识，数字签名验证结果展示信息符合表 A.2 的要求。

表 A.1 电子签章验证结果展示信息表

序号	信息分类	验证结果信息项
1	签章信息	签章时间
2		是否使用时间戳
3		签章状态
4		验证结果
5	印章信息	机构名称
6		统一社会信用代码
7		印章类型
8		印章编码
9		印章图像
10		制章者名称
11		受信任的电子印章体系标识 ^a
12	数字证书信息	证书版本号
13		证书序列号
14		签名算法
15		证书颁发者
16		证书使用者
17		有效期限

^a 若制章者未在受信任的电子印章体系内，应显示“签章者身份有效性未知”。

表 A.2 数字签名验证结果展示信息表

序号	信息分类	验证结果信息项
1	数字签名信息	签名时间
2		是否使用时间戳
3		签名状态
4		验证结果
5	数字证书信息	证书版本号
6		证书序列号
7		签名算法
8		证书颁发者
9		证书使用者
10		有效期限
11		受信任的PKI体系标识 ^a
^a 若数字证书未在受信任的PKI体系内的，应显示“签名者身份有效性未知”。		

参 考 文 献

- [1] GA/T 1106—2013 信息安全技术 电子签章产品安全技术要求
 - [2] ZFW C 0118—2018 国家政务服务平台标准 统一电子印章 总体技术架构
 - [3] GDZW 0016—2019 广东省统一电子印章平台接入规范
-