ICS 35.020
CCS A 90

# DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T XXX.3—2023

# 电子印章
# 第3部分：应用指南

Electronic seal—
Part3: Application guidelines

（送审稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 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 XXX《电子印章》的第 3 部分。DB4403/T XXX 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：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信息。

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专利的责任。

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：深圳市标准技术研究院、深圳市信息安全管理中心、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、王志勇、张报建、周鑫、黄立、简超、刘家雄、林雄杰、颜海龙、朱彦、李桂珠、黄浈婷、梁晓波、陈慧铧、马玮珣、陈胜、周维。

# 电子印章
# 第3部分：应用指南

## 1 范围

本文件规定了电子印章业务和应用的总体框架、电子印章业务的办理、电子印章在4类典型应用场景下的应用指南。

本文件适用于商事主体用户、政务用户、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，也适用于应用单位将电子印章服务整合到其业务或信息系统之中，供其用户在相应的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 党政机关电子印章应用规范

GB/T 38540 信息安全技术 安全电子签章密码技术规范

DB4403/T XXX.1 电子印章 通用要求

DB4403/T XXX.2 电子印章 数字证书

DB4403/T XXX.4 电子印章 应用服务接口

DB4403/T XXX.5 电子印章 第三方应用接入要求和测试方法

## 3 术语和定义

DB4403/T XXX.1和DB4403/T XXX.2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**

由应用单位（3.1）按照业务需要开发的，包含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或PKI体系 trusted electronic seal system or PKI system**

已与深圳市电子印章主管部门达成互认互信的其他电子印章体系或公钥基础设施（PKI）体系的统称。

3.4

**电子印章服务系统 electronic seal service system**

是电子印章系统的子系统，为用户提供电子印章服务，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。

## 4 电子印章业务和应用的总体框架

电子印章业务和应用的总体框架如图 1 所示，具体包括：

——电子印章管理服务机构通过电子印章系统为用户发放电子印章，提供电子印章相关服务。用户可通过电子印章服务系统申请和使用电子印章；

——电子印章系统通过电子印章服务接口为第三方应用系统提供电子印章应用支撑服务，应用单位可以通过与电子印章系统对接，为其用户提供包含电子印章功能的相关业务服务。电子印章应用服务接口应符合 DB4403/T XXX.4 中的规定；

——电子印章系统通过对接广东省统一电子印章平台、深圳市公安电子印章备案库，实现所发放的电子印章的备案管理；

——电子印章系统通过对接在深圳市内具备运营服务资质的 CA 机构，为用户提供电子印章所必须的 CA 服务；

——通过与深圳市电子印章主管部门签订互认互信协议，电子印章系统与受信任的电子印章体系或 PKI 体系实现互认。

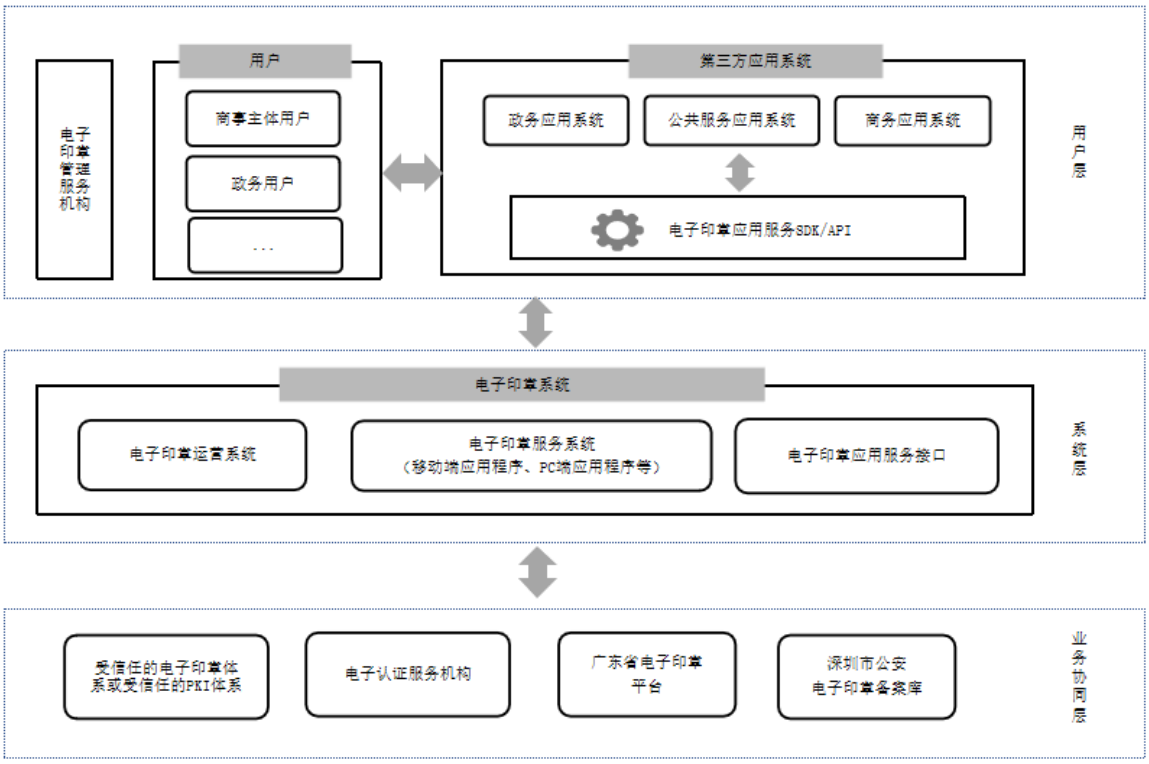


图 1 电子印章业务和应用的总体框架

## 5 电子印章业务

### 5.1 概述

用户应通过电子印章服务系统或电子印章管理服务机构的服务窗口办理电子印章业务，包括申请、领取、变更、更换、存储介质保护口令重置、冻结和解冻、续期及注销等，也可根据需要将电子印章授权给适当的人员进行管理和操作。

## 5.2 电子印章业务办理

### 5.2.1 申请

#### 5.2.1.1 申请用户

电子印章申请用户分为政务用户和商事主体用户：

——需要办理电子印章的政务用户，应先获得上级印章审批单位的准许后，再按流程和要求向电子印章管理服务机构申请政务部门电子印章；

——需要办理电子印章的商事主体用户，应按流程和要求向电子印章管理服务机构申请商事主体电子印章：

- 对于新设立商事主体，在其登记设立的同时，电子印章系统同步完成一套共四枚（法定名称章、财务专用章、合同专用章、负责人章）的电子公章和电子名章的发放，用户无需另行申请；
- 对于仍未获得电子印章的存量商事主体，可向电子印章管理服务机构申请，申请时应提供商事主体及负责人的法定身份证明材料。

#### 5.2.1.2 申请方式

电子印章申请方式分为在线申请和窗口申请：

——在线申请：商事主体用户或政务用户的负责人通过电子印章服务系统，在线完成电子印章申请，申请过程中须在线核验商事主体或政务部门及其负责人的身份；

——窗口申请：

- 对于无法完成在线申请的商事主体用户，其负责人可自行或委派其机构成员通过电子印章服务系统的移动端应用程序填报申请信息，并由商事主体的负责人按要求携带相关材料到电子印章管理服务机构服务窗口办理；
- 对于无法完成在线申请的政务用户，其负责人可自行或委派其机构成员通过电子印章服务系统的 Web 端应用程序填报申请信息，并由被委托的机构成员按要求携带相关材料到电子印章管理服务机构服务窗口办理。

### 5.2.2 领取

#### 5.2.2.1 介质

商事主体用户或政务用户完成电子印章申请后，需领取后才能使用电子印章。商事主体用户可根据需要通过智能移动终端、智能密码钥匙（USBKey）、服务器密码机（物理或云服务器密码机）等介质领取电子印章。政务用户可根据需要采用无介质，或通过USBKey和服务器密码机介质领取电子印章。

#### 5.2.2.2 领取方式

根据所使用的不同介质，电子印章领取方式包括以下几种：

——智能移动终端：商事主体用户印章操作人可通过电子印章服务系统的移动端应用程序，在线完成电子印章的领取；

——USBKey：用户在领取前应向依法设立的证书认证机构申请载有数字证书的USBKey，其中数字证书应符合DB4403/T XXX.2的规定：

- 对于商事主体用户，其负责人或印章管理员应通过电子印章服务系统的 Web 端应用程序完成电子印章的领取；
- 对于政务用户，其印章管理员应通过电子印章服务系统的 Web 端应用程序完成电子印章的

领取；

——服务器密码机：商事主体用户应先通过电子印章服务系统的Web端应用程序完成应用接入申请和服务器密码机备案，并向依法设立的证书认证机构申请数字证书，其中数字证书应符合DB4403/T XXX.2的规定。之后商事主体用户的负责人或经授权的加密机管理员可通过电子印章服务系统的Web端应用程序完成电子印章的领取。

### 5.2.3 变更

5.2.3.1 当商事主体用户的单位名称、负责人或单位类型（指内资企业转外资企业、外资企业转内资企业）发生变更时，原有商事主体电子印章自动失效，该商事主体用户应按照5.2.1和5.2.2节的要求重新申请和领取电子印章。

5.2.3.2 当政务用户的单位名称、负责人或单位类型发生变更时，原有政务部门电子印章自动失效，该政务用户应按照5.2.1和5.2.2节的要求重新申请和领取电子印章。

### 5.2.4 介质更换

用户因电子印章存储介质损坏、密钥泄露、被盗或丢失等原因需要更换存储介质的，应办理介质更换：

——若存储介质为智能移动终端，用户应向电子印章管理服务机构提交更换申请，并按照 5.2.2节的要求重新领取；

——若存储介质为USBKey或服务器密码机，用户应先在电子印章服务系统解除绑定，并向依法设立的证书认证机构申请更换，完成更换后再按照5.2.2节的要求重新领取。

### 5.2.5 存储介质保护口令重置

用户因电子印章存储介质保护口令忘记或锁死等原因需要重置保护口令的,应根据存储介质类型办理保护口令重置：

——若存储介质为智能移动终端,用户应通过电子印章服务系统的移动端应用程序完成保护口令重置；

——若存储介质为USBKey或服务器密码机,用户应向依法设立的证书认证机构申请保护口令重置。

### 5.2.6 冻结和解冻

用户因业务需要希望暂停使用电子印章，或短期内不使用电子印章的，可向电子印章管理服务机构申请冻结电子印章。

冻结电子印章后，用户可根据业务需要向电子印章管理服务机构申请解冻电子印章。

### 5.2.7 续期

续期业务是指与电子印章绑定的数字证书的续期：

——对于持有智能移动终端介质的商事主体用户，印章操作人应在数字证书有效期届满90日内通过电子印章服务系统的移动端应用程序完成电子印章续期；

——对于持有USBKey或服务器密码机介质的商事主体用户或政务用户，其负责人或印章管理员应在数字证书有效期届满90日内，向依法设立的证书认证机构完成数字证书的续期，再重新领取电子印章。

### 5.2.8 注销

电子印章注销是永久性注销，不可以进行恢复：

——对于单位注销或者撤销合并的商事主体用户或政务用户，原有电子印章自动失效；
——对于不再使用电子印章的商事主体用户或政务用户，可通过电子印章服务系统申请注销电子印章。

### 5.3 电子印章的授权

#### 5.3.1 一般要求

5.3.1.1 商事主体用户的负责人具有印章管理员和印章操作人的所有权限，也可授权其机构成员为印章管理员和印章操作人；政务部门负责人具有印章管理员的所有权限，也可授权其机构成员为印章管理员。
5.3.1.2 商事主体用户和政务用户应建立健全完善的电子印章内部管理制度，确保被授权人对电子印章的使用代表了负责人的意愿。
5.3.1.3 一枚电子印章可同时绑定多种介质类型，同一种绑定介质类型同时只能授权一位印章操作人持有。

#### 5.3.2 授权方式

授权方式分为在线授权和窗口授权：
——在线授权：
- 商事主体用户的负责人可通过电子印章服务系统的移动端应用程序完成在线授权；
- 政务用户的印章管理员可通过电子印章服务系统的 Web 端应用程序完成在线授权。

——窗口授权：
- 商事主体用户负责人也可携带相关材料到电子印章管理服务机构服务窗口办理授权业务；
- 政务用户可委托其机构成员按要求携带相关材料到电子印章管理服务机构服务窗口办理授权业务。

## 6 电子印章应用

### 6.1 概述

电子印章应用场景包括单方用章、在线用章、批量文件用章和混合用章：
——单方用章是指印章操作人利用电子印章系统所提供的PC端应用程序或移动端应用程序，对其存放在PC或智能移动终端上的待签章文件或签章文件进行签章和验章；
——在线用章是指第三方应用系统通过调用电子印章系统的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；
——批量文件用章是指用户对其存放在其所拥有的PC或服务器密码机上的多个待签章文件进行批量签章；
——混合用章是指深圳市电子印章与受信任的电子印章体系或PKI体系的电子印章或数字签名交叉使用。

### 6.2 单方用章

#### 6.2.1 用章文件

用章文件包括待签章文件和待验章文件：

——待签章文件应是由用户通过文本编辑工具软件自行创建或编辑的电子文件，文件格式可为doc、docx、xls、xlsx等流式文件格式，也可为pdf、ofd等版式文件格式；

——待验章文件格式应为pdf、ofd等版式文件格式。

#### 6.2.2 用章环境

商事主体用户可对存放在PC或智能移动终端上的文件进行用章，政务用户可对存放在PC的文件进行用章，具体要求为：

——PC端环境：PC端的操作系统应为Windows10及以上版本的操作系统，应安装电子印章PC客户端或使用Web浏览器，具备互联网连接功能，Web浏览器应是市场上主流浏览器；

——智能移动终端环境：智能移动终端的操作系统可为Android、iOS中的一种，具备互联网连接功能。

#### 6.2.3 用章方式

根据不同的用章环境，单方用章的方式也有所不同：

——智能移动终端：

- 签章：用户应通过电子印章服务系统的移动端应用程序，对存放在智能移动终端上的文件进行签章；
- 验章：用户应通过电子印章服务系统的移动端应用程序，对存放在智能移动终端上的文件进行验章。验章要求见附录 A。

——PC端：

- 签章：用户应通过电子印章服务系统的 PC 端应用程序，对存放在 PC 上的文件进行签章。电子印章的介质既可以是智能移动终端，也可以是 USBKey。用户还可根据需要选择单页签章、多页签章、骑缝章签章、撤章等用章功能；
- 验章：用户应通过电子印章服务系统的 PC 端应用程序完成验章。验章要求见附录 A；
- 撤章：用户应通过电子印章服务系统的 PC 客户端完成撤章。只有签章文件最近一次加盖的电子印章才能被撤章，且只能由印章操作人本人进行撤章。

### 6.3 在线用章

#### 6.3.1 用章文件

第三方应用系统的用户应按照第三方应用系统的要求提供用章文件。

第三方应用系统应按DB4403/T XXX.5规定的接入和测试要求提供用章文件，用章文件应为pdf或ofd的版式文件格式。

#### 6.3.2 用章环境

应用单位应按照DB4403/T XXX.4的要求申请应用接入，并按照DB4403/T XXX.5的要求完成第三方应用系统的接入和测试。

#### 6.3.3 用章方式

##### 6.3.3.1 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。

##### 6.3.3.2 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，印章操作人通过指定的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PC客户端，按照第三方应用系统指引插入USBKey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PC客户端接收签章任务后，按照第三方应用系统指引插入USBKey完成签章。

### 6.3.3.3 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，对待验章文件进行验证。验章要求见附录A。

### 6.3.3.4 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章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签名功能，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

用户可采用USBKey对待签名文件完成数字签名。

## 6.4 批量文件用章

### 6.4.1 用章文件

待签章文件的格式应为pdf或ofd版式文件格式。

### 6.4.2 用章环境

批量文件用章环境的具体要求为：

——PC端要求：电脑的操作系统应为Windows10及以上版本的操作系统，应安装好电子印章PC客户端程序，具备互联网连接功能；

——服务器密码机及用章服务器要求：应用单位应提前申请并报备服务器密码机，用章服务器应已完成与电子印章系统的对接并集成了批量签章功能，可参考6.3节在线用章场景。

### 6.4.3 签章介质选择

用户应根据不同的业务需求和应用场景，选择相应的签章介质：

——对于单次批量签章文件数量≤10个，且单个文件大小≤50 M的场景，应使用智能移动终端介质配合PC客户端对多个文件的批量签章；

——对于单次批量签章文件数量≤100个，且单个文件大小≤500 M的场景，应使用USBKey介质在电子印章PC客户端对批量文件集中签章；

——服务器密码机介质不限制文件数量和大小。

#### 6.4.4 用章方式

##### 6.4.4.1 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客户端完成批量签章。

##### 6.4.4.2 系统对接

第三方应用系统应通过调用电子印章系统的签章接口，完成多个文件的批量签章。使用系统对接方式的商事主体用户应配备服务器密码机。服务器密码机应符合DB4403/T XXX.1的要求。

### 6.5 混合用章

#### 6.5.1 受信任的电子印章体系和PKI体系

可与电子印章进行混合用章的受信任电子印章体系和PKI体系应满足以下要求：

——受信任电子印章体系：

- 其电子印章和电子签章符合国家及相关行业标准；
- 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文件；
- 与深圳市电子印章主管部门达成互认互信协议。

——受信任的PKI体系：

- 其数字证书和数字签名符合国家及相关行业标准；
- 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

6.5.2.1 受信任的电子印章体系或PKI体系的用户应使用其体系指定的系统对文件进行签章。

6.5.2.2 深圳市电子印章用户应使用深圳市电子印章系统对签章文件进行验章。受信任的电子印章体系或PKI体系的用户应使用其体系指定的系统对签章文件进行验章。验章要求见附录A。

# 附 录 A
（规范性）
验章要求

## A.1 电子印章验章要求

用户可通过电子印章系统对已使用电子印章签署的文件进行验章。验章应符合以下要求：

——电子印章系统应按照GB/T 38540和GB/T 33481的要求对该文件中印章所有者证书的合法性、有效性以及完整性进行验证；

——电子印章验章应验证以下内容：

- 签章文件有无被篡改；
- 印章信息，见表 A.1；
- 签章信息，见表 A.1；
- 数字证书信息，见表 A.1。

——不论验章通过与否，电子印章系统应展示验证结果。若验证失败，电子印章系统应给出相应提示。

**表 A.1 电子印章验证信息表**

| 序号 | 验证信息分类 | 验证项 |
|---|---|---|
| 1 | 印章信息 | 机构名称 |
| 2 | | 统一社会信用代码 |
| 3 | | 印章类型 |
| 4 | | 印章编码 |
| 5 | | 制章者名称[a] |
| 6 | | 印章图像 |
| 7 | 签章信息 | 签章文件名称 |
| 8 | | 文件内容摘要 |
| 9 | | 印章操作人姓名[b] |
| 10 | | 文件内容摘要 |
| 11 | | 签章时间 |
| 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或PKI体系内的，则显示未知。<br>b：展示验证结果时应将印章操作人姓名进行脱敏处理。 | | |

## A.2 数字签名验签要求

用户可通过电子印章系统对已使用数字签名签署的文件进行验章。验章应符合以下要求：

——电子印章系统应对该文件中数字签名的合法性、有效性以及完整性进行验证；

——数字签名验签应验证以下内容：

- 签名文件有无被篡改；
- 签名信息，见表 A.2；
- 数字证书信息，见表 A.2。

——不论验签通过与否，电子印章系统应展示验证结果。若验证失败，电子印章系统应给出相应提示。

**表 A.2　数字签名验证信息表**

| 序号 | 验证信息分类 | 验证项 |
|---|---|---|
| 1 | 签名信息 | 签名者 |
| 2 | | 签名时间 |
| 3 | 数字证书信息 | 证书版本号 |
| 4 | | 证书序列号 |
| 5 | | 签名算法 |
| 6 | | 证书颁发者 |
| 7 | | 证书使用者 |
| 8 | | 有效期限 |

# 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] ZWFW 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