

**SF**

# 中华人民共和国司法行政行业标准

SF/T 0034—2019

---

## 公证数据要求与规范

Notarization data requirements and specifications

2019-5-5 发布

2019-5-20 实施

---

中华人民共和国司法部 发布

# 目 次

前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 术语、定义和缩略语.....	1
4 数据特征.....	2
5 数据采集.....	3
6 数据加密.....	6
7 数据存储.....	6
8 数据证明.....	10
9 数据应用.....	11

## 前 言

本标准按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本标准由司法部公共法律服务管理局、中国公证协会提出。

本标准由司法部信息中心归口。

本标准起草单位：中国公证协会。

# 公证数据要求与规范

## 1 范围

本标准规定了公证数据特征、数据采集、数据加密、数据存储、数据证明和数据应用等要求及相关规定。

本标准适用于司法行政公证管理部门、公证协会及各公证机构对公证数据的管理、利用和其他业务操作。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 18894-2016 电子文件归档与管理规范

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 33716.1-2017 电子存档 第1部分:为保存电子信息针对信息系统设计和运行的规范

GB/T 35285-2017 信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求

SF/T 0023-2019 全国公证综合管理信息系统技术规范

SF/T 0036-2019 公证信息安全技术规范

SF/T 0037-2019 公证档案数字化规范

## 3 术语、定义和缩略语

### 3.1 术语和定义

下列术语和定义适用于本文件。

#### 3.1.1

**公证** notarization

公证机构根据自然人、法人或者其他组织的申请,依照法定程序对民事法律行为、有法律意义的事实和文书的真实性、合法性予以证明的活动。

#### 3.1.2

**公证机构** notarial institutions

依法设立,不以营利为目的,依法独立行使公证职能、承担民事责任的证明机构。

#### 3.1.3

**公证事项** notarial matters

依据《中华人民共和国公证法》第十一条的规定,公证机构所办理的证明业务。

### 3.1.4

#### 公证事务 notarial affairs

依据《中华人民共和国公证法》第十二条的规定，公证机构所办理的非证明业务。

### 3.1.5

#### 公证数据 notarial data

公证机构及公证人员在公证执业活动过程中，按照法定程序与法定办证规则的要求，所采集、加工、处理的与公证活动相关的数据。

注：以电子形式存储的公证数据，既包括传统形式公证所形成的公证数据转换成电子形式所存储的数据，也包括以电子公证形式所形成的公证数据。

### 3.1.6

#### 公证书 notarial certificate

公证机构根据当事人的申请，按照规定程序和格式所出具的、证明相关民事法律行为、有法律意义的事实和文书的真实性、合法性的证明文书。

注：包括以电子形式存储和展现的具有法律效力的公证书。

## 3.2 缩略语

下列缩略语适用于本文件。

CA 证书认证机构 (Certificate Authority)

FC 光纤通道 (Fiber Channel)

MD5 消息摘要算法 (MD5 Message-Digest Algorithm)

NAS 网络附属存储 (Network Attached Storage)

OCR 光学字符识别 (Optical Character Recognition)

PDF 便携式文档格式 (Portable Document Format)

RAID 独立冗余磁盘阵列 (Redundant Arrays of Independent Disks)

SAN 存储区域网络 (Storage Area Network)

SATA 串行高级技术附件 (Serial Advanced Technology Attachment)

## 4 数据特征

### 4.1 主体特定

公证机构及其公证人员应是公证数据采集和加密的主体。

### 4.2 程序法定

公证数据的采集和加密是公证机构及其公证人员在公证活动过程中，借助于电子设备、软件工具，按照法律法规所规定的程序及业务规则进行。

### 4.3 直接性

公证数据应直接来源于公证执业活动。

### 4.4 安全性

公证数据的存储与应用应遵循GB/T 22239-2008的要求，以保证公证执业活动过程及其结果的保密性、防篡改性、不可抵赖性。

#### 4.5 可检验性

公证数据的采集、加密和存储过程应能完整地记录公证执业活动的全过程，且能够按照预设的程序与条件重现整个公证执业活动的过程，并保持一致结果。

#### 4.6 完整性

公证数据在采集、加密、存储、证明和应用过程中，应确保数据的完整，并符合有关法律认定其有效的要求。

### 5 数据采集

#### 5.1 采集来源

##### 5.1.1 来源分类

本标准数据采集来源主要为：纸质卷宗和电子文档。

##### 5.1.2 纸质卷宗

纸质卷宗应为公证机构在线下办理公证业务时所建立的公证卷宗。

##### 5.1.3 电子文档

电子文档应主要从公证办证系统、在线公证办证系统、电子数据保管系统和其他公证业务信息系统进行采集。

#### 5.2 采集流程

##### 5.2.1 纸质卷宗电子化数据采集流程

纸质卷宗电子化数据采集应遵循以下流程进行：

编目——卷宗扫描——电子文档修整——电子文档结构化处理（可选）——数据封存归档。其中：

- a) 编目：数据采集人员对卷宗数据建立案件索引，以便数据查询；
- b) 卷宗扫描：数据采集人员利用扫描设备，将纸质卷宗扫描成电子文档进行存储；
- c) 电子文档修整：数据采集人员对经扫描的卷宗图片进行技术处理，使卷宗图片整洁便于识别；
- d) 电子文档数据结构化处理：有条件的公证机构，利用技术手段（例如：OCR技术等）对经扫描、修整后的电子文档进行文字识别，对非结构化数据进行结构化处理，并对其建立索引，以便对相关数据的检索、查询与利用；
- e) 数据封存归档：公证档案管理人员对经处理后的卷宗数据，通过相应技术手段，对公证数据进行封存归档。

##### 5.2.2 电子文档数据采集流程

###### 5.2.2.1 公证办证信息系统的信息采集流程

通过公证办证信息系统办理的公证业务应按以下流程进行：

申请——受理——审查——出证——领取和发送——归档。其中：

- a) 申请：公证人员根据当事人的公证申请对相关的申请进行数据录入；
- b) 受理：公证人员对当事人的公证申请确认给予办理；
- c) 审查：公证人员根据相关的办证规则，对当事人的公证申请进行审查，对于当事人补充提交的证明材料及调查核实的证明材料进行录入；
- d) 出证：公证人员对经审查通过的公证申请制作公证书；
- e) 领取和发送：通过短信、电话和邮件等方式向当事人通知公证书的领取和发送信息；
- f) 归档：公证人员对办证过程中采集、录入的数据进行分类整理，并交由专业档案人员进行归档。

#### 5.2.2.2 在线公证办证系统的数据采集流程

通过在线公证办证系统办理的公证业务应按以下流程进行：

提交申请——初步审核——线下确认当事人身份以及核实证明材料（或通过线上系统对接等方式核实）——出证——发送——归档。其中：

- a) 提交申请：当事人在系统中提出公证业务申请；
- b) 初步审核：系统接入第三方平台（例如：公安系统等）对当事人提交的身份信息及证明材料进行初步审核；
- c) 线下确认当事人身份以及核实证明材料：公证人员根据系统录入的信息，在线下确认当事人身份并核实相关证明材料；
- d) 出证：公证人员对经审查通过的公证申请制作公证书的过程；
- e) 发送：通过在线方式向当事人发送公证书信息；
- f) 归档：公证人员对办证过程中采集、录入的数据进行分类整理，并交由专业档案人员进行归档的过程。

#### 5.2.2.3 电子数据保管系统的数据采集流程

通过电子数据保管系统办理的公证业务应按以下流程进行：

当事人身份注册——在公证机构监督下取证——对数据进行加密——提交保管——公证机构出具数据保管凭证。其中：

- a) 当事人身份注册：当事人根据公证机构的要求依据，使用可确认其身份的信息向公证机构申请注册帐户；
- b) 在公证机构监督下取证：当事人利用公证机构控制的平台或工具对电子数据进行采集；
- c) 对数据进行加密：当事人及公证员对所保管的数据进行电子签名，应使用加密算法（例如：MD5加密算法等）对原始数据以及电子签名进行加密；
- d) 提交保管：当事人将数据提交至公证机构所控制的系统进行保管；
- e) 公证机构出具数据保管凭证：公证机构在对当事人的电子数据进行保管后，向当事人出具保管凭证。

### 5.2.3 电子化数据采集要求

#### 5.2.3.1 纸质卷宗电子化数据采集要求

纸质卷宗电子化数据采集要求如下：

- a) 纸质卷宗扫描应保持纸质卷宗原貌，必要时应对纸质卷宗作相应的描述（例如：档案内证明材料为原件的应备注说明为原件）；

- b) 档案修整过程应保持电子文档与纸质卷宗的一致性,对卷宗的清洁化等处理不应影响卷宗的原貌,所进行的技术性修整应是出于整洁的需要;
- c) 对电子文档进行结构化处理时,应建立严格的核验制度,任何进行结构化处理的数据应经人工确认,并应使结构化处理的数据与原非结构化数据建立一一对应关系,以供查询;
- d) 公证机构对非结构化公证数据进行结构化处理的,可对以下内容进行结构化处理:身份信息、婚姻状况信息、亲属关系信息、房产信息(坐落、权属人)等。

### 5.2.3.2 电子文档数据采集要求

电子文档数据采集要求如下:

- a) 公证机构使用公证办证系统、在线公证办证系统和电子数据保管系统办理公证业务时,应对采集过程进行同步记录并与所采集的数据一并存储;
- b) 申请环节应录入以下数据:申请日期、申请人身份信息、公证事项或公正事物、公证用途、当事人提交的证明材料及其初核情况、经当事人确认的公证申请表;
- c) 公证机构应采用线上线下相结合的方式对当事人的线上身份进行核实确认,经核实的当事人线上帐号,应按照电子签名法的相关规定,为当事人颁发数字证书。持有公证机构颁发的数据证书的当事人通过线上申请公证的,应对当事人的数字证书进行记录。相关的身份信息不得任意修改,任何修改均应给予明确记录;
- d) 受理环节应录入公证笔录(含线上受理中,当事人与线上受理系统的交互内容)、公证告知、公证人员代拟的公证书及受理通知书(含线上受理中,受理通知记录);
- e) 在公证审查阶段中,公证人员对调查核实的证明材料应在电子数据中对其来源进行备注说明;
- f) 在出证阶段,公证机构应将交付打印制作的公证书最终电子文档给予保存,具备条件的公证机构应使用可信的电子签章制作公证书;
- g) 数据封存归档时,应记录数据采集时间、数据封存时间、数据封存人姓名等;
- h) 公证机构使用电子数据保管系统办理公证业务时,所借助的技术工具应是公证机构可控制的,并且相关数据应由该工具直接采集,采集的数据应由公证机构持有与保管;
- i) 使用电子数据保管系统办理公证业务时应使用CA证书机制,为公证人员及当事人颁发CA证书。公证人员的办证操作过程及数据应进行电子签名,特别是出具电子公证书的公证机构,其电子公证书的电子签名技术应遵循 GB/T 35285-2017 的要求;
- j) 当事人提交保管的电子数据如非当事人自己制作的数据,而是来源于第三方,该数据的取得过程应在公证机构或公证机构控制的服务器监督/控制下进行,公证机构或其控制的服务器应对该电子数据的取得过程进行必要而详细的记录,并将相关的记录与电子数据共同保存。公证机构用于监督及记录电子数据提取过程的软件、服务器应符合 GB/T 33716.1-2017 的要求;
- k) 当事人将电子数据提交公证机构保管时,应由当事人及公证机构分别对该电子数据进行数据加密,以确保数据的安全性;
- l) 公证机构在保管当事人的电子数据时,不对当事人的电子数据内容进行审查;
- m) 实现全电子化办证的公证机构,对当事人所提交的证明材料电子文本及申请、受理环节中需要当事人签字确认的公证书,应由当事人进行数字签名并由核对的公证人员同步进行电子签名。

## 5.3 采集内容

### 5.3.1 卷宗数据采集内容

卷宗数据应包含以下采集内容:

- a) 当事人信息(姓名/名称,身份信息/证照信息);



- b) 公证事项（公证事务）；
- c) 受理日期；
- d) 公证机构名称；
- e) 公证员及公证助理人员姓名；
- f) 公证书编号；
- g) 出证日期；
- h) 公证申请表内容；
- i) 询问笔录；
- j) 公证书；
- k) 其他文书；
- l) 证明材料；
- m) 工作记录；
- n) 领取和发送情况；
- o) 档案保密要求；
- p) 保管期限。

### 5.3.2 电子化办证采集内容

电子化办证应包含以下采集内容：

- a) CA 证书；
- b) 电子签名；
- c) 申请日期；
- d) 申请人身份信息；
- e) 公证事项（公证事务）；
- f) 公证用途；
- g) 当事人提交的证明材料及其核对情况；
- h) 经当事人确认的公证申请表、受理通知书；
- i) 询问笔录、公证告知；
- j) 代拟的公证证词；
- k) 采集时间；
- l) 数据封存时间；
- m) 数据封存人姓名；
- n) 采集过程记录。

## 6 数据加密

数据加密要求如下：

- a) 公证机构对所采集的数据，应采取相应的技术手段对数据进行特征化处理（例如：提取其 MD5 值等），使其区别于其他电子数据，以确保数据的唯一性、可识别与可校验；
- b) 公证机构对所采集的当事人尚未向公证机构公开的数据（例如：电子数据保管系统中的数据）及属于应特殊保密处理的数据，还应对数据采取必要的加密措施；
- c) 归档的公证数据应使用公证机构的数字证书进行封签。

## 7 数据存储

## 7.1 数据存储

数据存储要求如下：

- a) 公证数据应遵循 GB/T 22239-2008 的要求，进行存储与备份；
- b) 公证机构应遵循 GB/T 22239-2008 的要求对公证数据建立定期备份机制，确保数据的存储安全；
- c) 公证数据的存储应区分内部网络与公共网络，存储于内部网络及公共网络的公证数据，应采取相应的加密措施，确保数据的安全；
- d) 公证数据存储期限应按照公证档案的保管期限规定进行保管；
- e) 公证数据不应与其他数据混同存储，应进行独立存储。

## 7.2 存储介质

### 7.2.1 存储介质类型

存储介质类型主要分为硬盘和光盘。硬盘是电子数据的主要存储设备。

### 7.2.2 硬盘技术指标

#### 7.2.2.1 服务器硬盘

服务器硬盘技术指标要求如下：

- a) 服务器硬盘应使用具有高可靠性的高速硬盘，每分钟转速应不小于 10000 转/每分钟，配置不小于 32MB 的回写缓存，内部传输速率（写速度）不小于 60MB 每秒，容量不低于 1TB；
- b) 硬盘接口应为 SCSI、SATA、FC 或 SAS 等，具体接口选择应符合系统性能需求，应与系统硬件相兼容；
- c) 硬盘应支持热插拔技术。

#### 7.2.2.2 归档硬盘

归档硬盘技术指标要求如下：

- a) 应遵循 GB/T 18894-2016 中的要求进行存放、备份、检验和转存；
- b) 容量应不小于 5TB，接口应为 SCSI、SATA、FC 或 SAS 等，具有高稳定性，平均故障间隔时间不少于 80 万小时。

#### 7.2.2.3 硬盘性能指标

运行时应对硬盘设备及磁盘控制器进行实时监控，具体性能指标要求如下：

- a) 硬盘设备
  - 1) 使用率：高于硬盘使用总量的 80% 时需预警；
  - 2) 饱和度：高于存储容量的 80% 时需预警；
  - 3) 错误：出现错误时需预警且记录日志；
  - 4) 响应时间：超过 5 秒时需预警。
- b) 磁盘控制器
  - 1) 使用率：当前值对比最大吞吐量使用率超过 90% 时需预警；
  - 2) 饱和度：由于控制器饱和造成的 I/O（输入输出）等待程度饱和度超过 90% 时需预警；
  - 3) 错误：控制器出现错误时需预警且记录日志。

#### 7.2.2.4 存储方式

硬盘存储分为NAS、SAN、磁盘阵列三种方式，具体要求如下：

- a) NAS方式：公证数据共享及备份应使用NAS存储方式，并使用专用NAS设备；
- b) SAN方式：公证数据库服务器应使用SAN存储方式，并使用专用SAN设备；
- c) 磁盘阵列方式：磁盘阵列也称为RAID，RAID又分为RAID 0、RAID 1、RAID 01、RAID 2、RAID 3、RAID 4、RAID 5、RAID 6、RAID 7等。公证数据存储应采用RAID 1方式，RAID 1的镜像磁盘可直接作为一份备份拷贝，并在数据归档至硬盘或光盘后反复使用。

### 7.2.3 光盘技术指标

光盘技术指标要求如下：

- a) 电子文件采用光盘归档时，应使用档案级光盘。档案级光盘应满足以下指标要求：
  - 1) 记录前，寻轨错误 $\leq 0.45$ ；
  - 2) 记录前，聚焦错误 $\leq 0.5$ ；
  - 3) 记录后，奇偶校验内码错误 $< 80$ ；奇偶校验外码失败 $= 0$ ；
  - 4) 记录后，信号对称性  $\beta = -0.15 \sim 0.15$ ；
  - 5) 记录后，数据对时钟抖动 $< 8$ ；
  - 6) 光盘温湿度耐候试验，在温度 $55^{\circ}\text{C}$ 、相对湿度50%的环境条件下，放置96小时，奇偶校验内码错误 $< 180$ ，奇偶校验外码失败 $= 0$ ；
  - 7) 光盘驱动器接口应为SATA或USB（通用串行总线）。
- b) 电子文件采用光盘归档需刻录时，应使用光盘刻录机。光盘刻录机应满足以下要求：
  - 1) 应使用经检测性能优良的光盘刻录机；
  - 2) CD-R光盘和DVD±R光盘的数据刻录应分别选用专用刻录机；
  - 3) 选用的刻录机应能识别档案级光盘的最佳写功率和写策略。
- c) 电子文件采用光盘归档时，应将数据刻录至光盘。数据刻录时应满足以下要求：
  - 1) 归档光盘的数据刻录工作环境应符合有关标准，并有良好的通风条件。光盘刻录前，应在工作环境中放置2小时以上；
  - 2) 光盘数据刻录时，采用中速刻录，即CD-R光盘采用24-40倍速刻录速度，DVD±R光盘采用8-12倍速刻录速度；
  - 3) 光盘数据刻录应采用全盘一次刻完方式；
  - 4) 归档光盘数据刻录完成后应设置成禁止写操作的状态，不能再对光盘数据进行增减。

## 7.3 存储格式

### 7.3.1 结构化数据存储格式

结构化数据存储格式应存储于数据库，具体格式应遵循SF/T 0023-2019中7.2-7.4的规定。

### 7.3.2 非结构化数据存储格式

非结构化数据存储格式要求如下：

- a) 应以文件形式存储于专用的、带有文件系统的存储服务器中，每个非结构化数据文件应有唯一全局索引；
- b) 包括当事人提供的图像、音频、视频、办公文档、纯文本文件以及其他文件。对纸质或其他形式的材料的数字化存储具体见SF/T 0037-2019；
- c) 各类非结构化数据的存储格式具体要求如下：

- 1) 图像：应使用 JPEG（联合图像专家组）、TIFF（标签图像文件格式）、PNG（可移植网络图形格式）、PDF 等作为通用格式。若无法将原格式文件转换为通用格式文件，应将相关软件一并存储；
- 2) 音频：应使用 WAV（窗波）、MP3（动态影像专家压缩标准音频层面 3）等作为通用格式，并收集其属性标识、参数。若无法将原格式文件转换为通用格式文件，应将相关软件一并存储；
- 3) 视频：应使用 AVI（音频视频交错格式）、MPEG、MR、MP4（便携式视频播放器）、WMV（窗口媒体视频）等作为通用格式，并收集其属性标识、参数。若无法将原格式文件转换为通用格式文件，应将相关软件一并存储；
- 4) 办公文档：应使用 PDF、wps、doc、docx、ppt、pptx、xls、xlsx 等作为通用格式。若无法将原格式文件转换为通用格式文件，应将相关软件一并存储；
- 5) 纯文本文件：编码应使用 UTF-8（万国码）；
- 6) 其它文件：应以 zip 等通用格式打包存储。

## 7.4 存储安全

### 7.4.1 基本要求

存储安全宜遵循 SF/T 0036-2019 中的规定。

### 7.4.2 物理安全

存储物理安全要求如下：

- a) 存储介质的存放环境应干燥、洁净、稳固、凉爽、无强光、无电磁辐射、无化学污染；
- b) 存储介质搬运应注意轻拿轻放，避免挤压和强烈震动；
- c) 应按照介质的说明方法正确使用，使用正确的物理接口，避免介质和相关设备损坏；
- d) 存储服务器应安放在满足 GB/T 22239-2008 的第三级防护要求的机房中。

### 7.4.3 系统安全

存储系统安全的保护措施包括身份鉴别、访问控制、安全审计等，具体见 SF/T 0036-2019 中 8 和 9 的内容。

### 7.4.4 数据安全

数据安全措施要求如下：

- a) 宜使用区块链技术对数据进行共识以及存储；
- b) 应使用加密算法获取相应数据的数据指纹；
- c) 应使用专用硬件设备完成数据的加密、共识以及存储等过程。

### 7.4.5 安全管理

存储安全管理要求如下：

- a) 应建立完善的管理规章制度，具体如下：
  - 1) 应规范存储介质的采购、有效期、存档、转存、错误检查、数据恢复、介质标签、服务器使用等事项；
  - 2) 应规定不同数据介质的使用期限、转存和错误检查期限，定期执行相关操作；

- 3) 应规定需依据机房安全要求、服务器操作规范、存储介质使用指南制定工作人员管理规范，确保各项工作职责落实到位，必要时应设立多人共同责任制度。
- b) 应制定完善的存储介质要求，具体如下：
  - 1) 存储介质的采购应满足实际性能需求、技术要求、接口规范、价格合理并且生产日期较新，采购后应采取相关措施检验产品合格性；
  - 2) 存储介质标签应包含介质编号、数据存入日期、备份介质编号等信息，有序存放于安全环境。介质的使用、销毁、移动等操作应记录在案。

## 7.5 存储运维

### 7.5.1 标签

按照标签使用的存储介质，分为归档硬盘标签与归档光盘标签，具体要求如下：

- a) 归档硬盘标签：应书写在硬盘外壳上及包装盒上，标签应包含硬盘生产日期、数据录入日期、档案编号等信息，应有序存放；
- b) 归档光盘标签：应使用专用的光盘标签笔或喷墨打印条形码，不应直接在光盘上贴标签。标签应包含光盘生产日期、刻录日期、档案编号等信息，应有序存放。

### 7.5.2 备份

归档的存储设备按查阅使用频度，分成普通级（不高于1年）和频繁级（高于1年），具体要求如下：

- a) 普通级归档存储设备应一式3份，一份供查阅使用，一份封存保管，一份异地保存；
- b) 频繁级归档存储设备应一式4份（或更多），两份供查阅使用，一份封存保管，一份异地保存。

### 7.5.3 检验与转存

应根据存储介质的质量年限技术指标制定相对应的检验与转存策略，确保数据的一致性与正确性，具体要求如下：

- a) 应按照检验策略，每隔2年对特定介质进行抽查检验，若数据错误率高于规定值，则应进行数据修复并转存；
- b) 应按照转存策略，达到6年转存期限的数据应立即转存。

## 8 数据证明

数据证明要求如下：

- a) 非经公证机构审查并确保来源可靠的电子数据，公证机构不应对电子证据的真实性进行证明，并且应在公证书中对其真实性给予排除；
- b) 当事人事先提交保管的电子数据，公证机构在根据当事人申请出具公证书时，应经当事人对电子数据进行解密，从公证办证系统中提取该电子数据及完整记录该电子数据的产生及保管过程的记录，并对所提取的电子数据与当事人提交保管的电子数据的一致性进行比对，确保其一致性；
- c) 公证机构应根据有关办证规则，对当事人申请出具公证书的电子数据，应对其身份、固定该电子数据的缘由、过程、当事人取得该电子数据的行为环境及公证书所需要达到目的，特别是当事人取得该电子数据的行为的合法性进行审查；

- d) 公证书应按照法定格式制作，除纸质公证书内所附的实物证据外，电子公证书内容应与纸质公证书一致，对含有实物证据等无法在电子公证书中体现的内容，应在电子公证书中对该部分内容进行备注说明，必要时可以附加音像文件；
- e) 在电子公证书附加有当事人的电子签名、公证机构及公证员的电子签名时，非经法定事由及程序，不应修改电子公证书内容；
- f) 公证机构所出具的电子公证书应可验证，并经公开渠道提供给接收单位与使用单位进行验证；
- g) 公证机构在出具电子公证书时，应同时将电子公证书上传至公证管理系统；
- h) 公证机构根据当事人的需要出具电子公证书后，应通过与当事人约定的电子邮件等电子送达方式，将电子公证书发送当事人，并告知当事人查验电子公证书的方法；
- i) 公证行业应建立全行业统一的公证 CA 认证中心，由公证管理系统向公证机构、公证人员颁发公证机构及公证人员的电子签名，由公证机构向当事人颁发电子签名；
- j) 公证行业应建立统一安全的电子公证书制作制度。

## 9 数据应用

### 9.1 公证数据的应用分类

#### 9.1.1 根据数据的保密级别与公开范围的分类

根据数据的保密级别与公开范围，公证数据可分为以下 5 类：

- a) 可公开类：对于不涉及国家秘密、商业秘密或者个人隐私应向不特定公众进行公示的数据，如公证抵（质）押登记信息，此类信息在公开公示时，应对数据作必要的去隐私化处理；
- b) 特定公开类：仅向单一对象公开的公证数据，此类数据公开对象一般为当事人，公开的数据范围为当事人所提供的证明材料或公证机构出具的公证书；
- c) 定向公开类：根据数据保密级别仅向特定范围对象进行公开的电子数据，此类数据公开对象一般为公证书的使用单位，数据范围为公证书；
- d) 行业公开类：面向公证行业内部公开的数据；
- e) 不予公开类：涉及国家秘密、商业秘密或者个人隐私的数据及行业专有数据。

#### 9.1.2 根据数据的使用和利用方式的分类

根据数据的使用和利用方式，公证数据可分为以下 5 类：

- a) 查阅：单位或个人依法对公证数据进行查阅；
- b) 核验：公证书的持有人/使用人通过与公证机构所保存的公证数据进行对比，核验公证书的真实性；
- c) 登记：公证机构根据有关法律规定或办证规则的规定，对抵押、质押等相关信息单独记录在相应登记平台的行为；
- d) 公示：公证机构根据有关法律规定或办证规则的规定，对抵押、质押等相关信息进行公开公示的行为；
- e) 数据分析与挖掘：公证机构根据公证业务的需要，对其所存储的公证数据进行分析与挖掘的行为。

### 9.2 公证数据的查阅

公证数据查阅要求如下：

- a) 非因法定事由及经法定程序，任何单位及个人均不应查阅公证数据；

- b) 公证案件的当事人对归属于其提交的公证数据有权申请查阅，有关办证流程等信息，公证机构应对当事人开放查阅；
- c) 当事人提交公证机构保管的电子数据，公证机构不应许可除当事人之外的其他人查阅该部分电子数据，除非当事人许可；
- d) 涉密的公证数据查阅，应按照国家有关涉密信息的管理规定执行；
- e) 公证机构及公证行业监督指导部门因业务监督与指导需要，查阅相关公证数据的，应根据相关规定办理公证数据查阅手续，并登记记录；
- f) 公证机构之间可以相互查阅公证数据，但应坚守保密义务，不应泄露国家秘密、商业秘密或者个人隐私。

### 9.3 公证书的核验

公证书核验要求如下：

- a) 公证机构可向公证书的使用单位提供核验服务，但应采取相应的数据安全措施；
- b) 根据公证书使用单位的请求，公证机构在征得当事人同意后（事前/事后），可向公证书使用单位开放查阅/推送相关部分的公证数据；
- c) 公证机构之间可以相互核验公证书，应做好相应的核验记录；
- d) 核验涉及保密的公证书数据应履行法律规定的程序。

### 9.4 公证数据的登记与公示

公证数据登记与公示要求如下：

- a) 公证机构对抵押、质押等相关信息进行公示前，应对当事人信息进行脱密处理，并提供查询渠道；
- b) 公证行业应建立统一的公示平台，对抵押、质押等信息进行统一公示。

### 9.5 公证数据分析与挖掘

公证数据分析与挖掘要求如下：

- a) 公证数据分析与挖掘应由公证机构或公证行业监督管理部门进行，其他组织和个人非因法定事由并经法定程序均不应对公证数据进行分析与挖掘；
  - b) 对公证数据分析与挖掘时，应做好数据的去隐私化，不应将当事人的隐私信息用于数据分析与挖掘。
-