

T/ZIPS

浙江省知识产权协会团体标准

T/ZIPS XXXX—2024

数据知识产权存证平台建设与运行规范

Construction and Operation specification for Data intellectual property evidence
preservation platform

(报批稿)

XXXX - XX - XX 发布

XXXX - XX - XX 实施

浙江省知识产权协会 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 基本原则.....	2
5 数据知识产权存证平台.....	2
6 数据知识产权存证过程.....	3
7 数据知识产权存证平台对接要求.....	4
参考文献.....	6

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。

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。

本文件起草单位：杭州市余杭区市场监督管理局、浙江省知识产权研究与服务中心（国家知识产权局专利局杭州代办处）、杭州趣链科技有限公司、杭州链城数字科技有限公司、浙江省杭州市杭州互联网公证处、浙江省宁波市鄞源公证处、浙江省知识产权协会、浙知交（杭州）知识产权运营有限公司。

本文件主要起草人：钟华韵、沈姝逸、曹丽芬、范理、徐小军、孟君、许正鹏、谢杨洁、陈晓丰、尹可挺、徐小蔚、胡海波、张蕤文、李文莉、张潞潞

数据知识产权存证平台建设与运行规范

1 范围

本文件规定了数据知识产权存证平台、存证过程、存证平台对接要求的内容。
本文件适用于数据知识产权存证平台的管理。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 35274—2017 信息安全技术 大数据服务安全能力要求

T/CESA1048—2018 区块链存证应用指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据知识产权 data intellectual property

自然人、法人和非法人组织对依法依规获取、经过一定规则处理、具有实用价值和具有智力成果属性的数据集合，依法享有的权益。

3.2

数据知识产权存证 data intellectual property preservation

为了保证数据知识产权存证信息（电子数据）的完整性和真实性，采用区块链技术实现多节点共识的存证服务。

3.3

存证平台 evidence preservation platform

以网站、应用程序和编程接口等形式提供数据知识产权存证服务的软件或系统。

3.4

存证服务提供者 evidence preservation provider

通过存证平台提供存证服务的机构或组织。

3.5

存证服务使用者 evidence preservation user

使用存证平台存证服务的组织或个人。

4 基本原则

4.1 真实性

存证平台应确保各流程获取的信息和资料真实可靠。存证服务使用者确保数据真实、准确，符合客观实际。

4.2 合法性

存证平台、存证流程、存证证书等活动和内容应符合相应法律法规的要求。

4.3 有效性

存证平台应有能力进行数据变更查验。隐私保护算法处理数据时，应反映数据的真实状况，确保原始数据可验证。

4.4 安全性

存证平台应确保数据的传输、存储等环节安全可靠，全过程数据保持完整、一致，存证数据防篡改、防抵赖、可追溯，以实现可信存证。

5 数据知识产权存证平台

5.1 存证平台建立条件

5.1.1 存证服务提供者要求

存证服务提供者应符合以下要求：

- a) 应依法办理市场主体登记；涉及行政许可的，应当取得主管部门的行政许可；
- b) 应建立业务、财务、资产等管理制度，对工作人员的行为进行监督，建立过错责任追究制度；
- c) 应具备完善的存证服务所需设备，包括但不限于计算机软硬件、互联网设施、日常办公设备等；
- d) 有与存证服务经营规模相适应的管理人员、技术人员和服务人员；
- e) 禁止毁损、篡改存证数据；
- f) 禁止泄露在存证活动中知悉的有关存证服务使用者的信息；
- g) 禁止为“不真实、不合法、不合规”的数据存证；
- h) 法律、法规禁止从事的其他行为。

5.1.2 存证平台应取得的资格

存证平台应取得以下资格：

- a) 信息系统安全等级保护三级认证；
- b) 区块链服务备案许可（如国家互联网信息办公室发布的境内区块链信息服务备案情况等）；
- c) 可信区块链安全测试证书；
- d) 可信区块链性能测试证书。

5.2 存证平台安全

5.2.1 存证平台应建立健全风险监测、安全评估、安全教育等安全管理制度。

- 5.2.2 存证服务提供者应保障存证平台的系统或软件实时稳定运行。定期检查，防止网络攻击、病毒和网络代理的使用。
- 5.2.3 存证平台应采取有效措施，妥善保存平台的全部服务信息，保证信息的完整性、准确性和安全性。
- 5.2.4 存证平台宜采用符合国家密码管理局认证核准的密码技术对数据进行加密传输和存储，并对密钥采取必要的保护机制。相关系统接口及系统配置安全可靠，避免系统代码被反编译或篡改。
- 5.2.5 存证服务提供者应采取措施保障存证平台的安全，对信息泄露、毁损、丢失、篡改等非授权的访问或破坏的异常情况进行监测和预警，应具有防护措施和应急预案。
- 5.2.6 存证平台应具有隐私保护机制，对于隐私数据的访问采取严格的权限管理。
- 5.2.7 必要时，存证平台可设置异地灾备系统，建立灾难恢复体系。

5.3 数据可追溯

存证平台应建立安全可信、管理可控、可追溯、可验证的数据存证环境。

5.4 时间可信

存证平台的系统时间及生成的可信时间标识应从国家法定授时机构进行授时和守时。

5.5 存证规范

- 5.5.1 存证平台应建立自动识别功能，确保用户所存证的内容不涉及敏感、违规、不良用语等。
- 5.5.2 存证服务使用者不得存证违反国家法律法规或涉国家秘密的数据内容。
- 5.5.3 存证平台应承担合理谨慎的信息审查义务，对明显的侵权或违法信息，可依法及时进行必要处置，并告知存证服务使用者。
- 5.5.4 鼓励存证服务提供者依照本规范进行行业自律，支持有关行业组织对存证服务进行监督和协调。
- 5.5.5 鼓励行业协会设立警示制度，监督和约束有不良行为的存证服务提供者。
- 5.5.6 鼓励存证服务提供者成立行业自律组织，制定行规和行约，加强自律，推动存证服务的发展。

5.6 停止经营

存证平台暂停或其他原因终止经营的，应当提前三个月通知存证服务使用者，妥善处理暂停或终止的相关事宜，确保在合理期限内继续提供相应服务。

6 数据知识产权存证过程

6.1 通用要求

- 6.1.1 数据知识产权存证前，存证服务使用者应经过实名认证，并对使用存证服务及存证内容做出承诺。必要时，存证服务提供者可对存证服务使用者的资格进行审核。
- 6.1.2 数据知识产权存证时，存证服务使用者应将数据的存证信息以及完整性校验值、附属信息等同步传输至数据知识产权存证平台。
- 6.1.3 存证服务提供者应记录数据知识产权存证平台的硬件设备信息、软件系统信息、网络信息及过程数据等，并计算相关信息的完整性校验值。将记录的数据与对应的完整性校验值同时进行存证。
- 6.1.4 存证服务使用者需要进行原文存证的，应提交数据原文到数据知识产权存证平台或第三方数据存储平台；不需要进行原文存证的，存证平台应告知相关注意事项，避免存证服务使用者破坏完整性导致无法验证而产生纠纷。

6.1.5 存证平台设置服务期限的，至少应保证自提供存证服务使用者服务期限止三年内，相关存证信息能够查询。

6.1.6 必要时，存证服务使用者可对数据知识产权经处理前的数据和处理中的过程数据进行存证。

6.2 存证数据

6.2.1 存证平台的存证数据应包括静态记录数据和动态过程数据：

- a) 静态记录数据：即非源数据存证，一般以数据包形式进行存证；
- b) 动态过程数据：即实时源数据存证，如 API（应用程序编程接口）方式存证。

6.2.2 存证服务使用者需选择与自身需求相关的数据进行存证：

- a) 选择与存证服务使用者相关的数据作为存证数据；
- b) 选取的存证数据内容应满足可追溯的要求，且能够体现完整的信息；
- c) 选取的存证数据内容应能体现数据及算法的价值。

6.3 存证数据记录

6.3.1 存证平台应在存证服务使用者完成存证后出具格式规范的存证证书。

6.3.2 数据知识产权存证的记录应有唯一的存证标识码。

6.3.3 数据知识产权存证的记录应包括可信时间标识。

6.3.4 数据知识产权存证的记录应与存证服务使用者进行关联。

6.3.5 数据知识产权存证的记录应包括完整的日志信息、存证过程中关键节点的可信时间标识、用户、数据类别、数据描述、数据数量、所属区块链等信息。

6.3.6 存证平台存证原文的，数据知识产权存证的记录应包括原文以及附属信息。

6.4 存证查询

存证平台应保证存证服务使用者可检索其提交的存证数据，下载并打印存证证书。

6.5 存证数据验证

6.5.1 存证平台应提供验证服务，并给出验证结果。

6.5.2 验证结果应包括存证标识码、可信时间、存证用户信息、存证日志信息等。

6.6 隐私保护

存证平台应符合 GB/T 35273—2020 要求，并符合以下要求：

- a) 存证平台应仅采集和保存存证业务必需的用户信息；
- b) 存证服务使用者的检索结果中不应显示非其存证数据的存证信息。

7 数据知识产权存证平台对接要求

7.1 通用对接要求

7.1.1 存证服务提供者提供编程接口与其他存证平台或应用系统进行对接时，应对接入的存证平台或应用系统进行评估，确保其符合本标准的要求。

7.1.2 存证服务提供者与法院、仲裁等其它存证平台或应用系统进行对接时，应符合对接部门的要求。

7.1.3 存证平台对接应开放若干条用户数据，供相关机构审核与评估数据情况；对于其余数据，无密钥或存证服务使用者授权，存证平台或任何参与方不得查看。

7.2 与登记平台对接

7.2.1 存证平台接入数据知识产权登记平台时，应符合登记平台要求。

7.2.2 存证平台需按规范接口提供数据存证信息，以保证数据知识产权登记平台能准确获取到存证平台存证数据信息。

7.2.3 存证平台需保证接口的可用性、稳定性以及性能。

参考文献

- [1] 《中华人民共和国民法典》（第十三届全国人民代表大会第三次会议通过）
 - [2] 《中华人民共和国数据安全法》（第十三届全国人民代表大会常务委员会第二十九次会议通过）
 - [3] 《浙江省知识产权保护和促进条例》（浙江省第十三届人民代表大会常务委员会第三十八次会议通过）
 - [4] 《浙江省公共数据条例》（浙江省第十三届人民代表大会第六次会议通过）
 - [5] 《区块链信息服务管理规定》（国家互联网信息办公室室务会议审议通过）
 - [6] 《推动知识产权高质量发展年度工作指引（2020）》（国知发运字〔2020〕13号）
-