知识产权领域电子证据应用规范

Specifications for the application of digital evidence in the field of intellectual property

2024-4-10 发布　　2024-4-10 实施

目　　次

前言

党的十八大以来，知识产权保护工作进入到一个全新时期。新技术的快速发展，为知识产权保护工作带来全新挑战的同时，也为知识产权系统性保护工作提供了有力抓手。特别是在电子证据的获取与应用方面，应用技术的不断提升与迭代发展，已经突破了原有的传统模式。2018 年，北京互联网法院成立后审理的“第一案”，对通过区块链系统进行电子取证的证据效力予以认定，新型电子证据的应用逐渐扩大规模，拓展至知识产权全行业领域。

习近平总书记指出，要强化知识产权全链条保护，要综合运用法律、行政、经济、技术、社会治理等多种手段，从审查授权、行政执法、司法保护、仲裁调解、行业自律、公民诚信等环节完善保护体系，加强协同配合，构建大保护工作格局。为进一步强化社会共治格局，在北京市委宣传部领导下，针对版权领域的行政司法协同治理工作机制正式成立。在该机制下，将充分发挥司法机关、行业协会、政府部门、公证服务机构等多方优势，构建全链条保护体系，形成治理合力。

证据是知识产权保护工作的核心，更是各类主体开展维权、应诉等工作的重中之重。为规范知识产权领域电子证据的取证、存证应用，保证电子证据的效率、可靠性，减少出错机率，提高知识产权领域电子证据应用的规范性，结合国家行业相关技术规范，参照行政司法协同治理工作机制的运行模式，特制定本标准。

本标准对知识产权领域电子证据，取证、存证的应用架构和技术要求等内容进行了规定。

本标准按照GB/T1.1-2009《标准化工作导则》给出的规则起草。

本标准发起单位：中国信息通信研究院、中国文物交流中心、北京互联网法院、首都版权协会。

本标准起草单位：中国信息通信研究院、中国文物交流中心、北京互联网法院、首都版权协会、北京市长安公证处、北京市东方公证处、北京市国信公证处、中创文贸（北京）文物艺术品有限公司、北京路浩知识产权代理有限公司、北京獬豸云网络科技有限公司。

本标准主要起草人：

谭平　赵长新　闫坤　聂鹏　李文宇　崔伟　冯华　华楠　陈浩哲　张浩　王继华　刘娟　李德新　杨靖涛　姜波　王莹　张晶　赵亮　肖东

1 范围

本标准规定了基于知识产权领域电子证据应用规范的术语定义、体系框架和规范性要求等内容。

本标准适用于基于知识产权领域电子证据的取证、存证应用，其他场合的电子证据的取证、存证应用可参照执行。

2 规范性引用文件

GB/T 1.1-2009《标准化工作导则》

GB/T 19451.1-2004《电子签名技术规范》

GB/T 19451.2-2004《电子签名应用规范》

GB/T 19451.3-2004《电子签名第三方服务规范》

GB/T 22198-2008《信息安全技术 公钥基础设施 PKI 系统安全保护技术规范》

GB/T 22199-2008《信息安全技术 公钥基础设施 PKI 系统安全测评规范》

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 22240-2008《信息安全技术 信息系统安全等级保护实施指南》

GB/T 22241-2008《信息安全技术 信息系统安全等级保护测评要求》

GB/T 22242-2008《信息安全技术 信息系统安全等级保护测评方

法》

GB/T 22243-2008《信息安全技术 信息系统安全等级保护安全设计技术要求》

GB/T 22244-2008《信息安全技术 信息系统安全等级保护安全实施技术要求》

GB/T 22245-2008《信息安全技术 信息系统安全等级保护安全运维技术要求》

GB/T 22246-2008《信息安全技术 信息系统安全等级保护安全测评技术要求》

GB/T 22247-2008《信息安全技术 信息系统安全等级保护安全培训技术要求》

GB/T 22248-2008《信息安全技术 信息系统安全等级保护安全监管技术要求》

GB/T 22249-2008《信息安全技术 信息系统安全等级保护安全测评管理技术要求》

GB/T 22250-2008《信息安全技术 信息系统安全等级保护安全监管管理技术要求》

GB/T 22251-2008《信息安全技术 信息系统安全等级保护安全培训管理技术要求》

GB/T 22252-2008《信息安全技术 信息系统安全等级保护安全设计管理技术要求》

GB/T 22253-2008《信息安全技术 信息系统安全等级保护安全实

施管理技术要求》

GB/T 22254-2008《信息安全技术 信息系统安全等级保护安全运维管理技术要求》

GB/T 37043-2018《智慧城市 术语》

SF/T 0076—2020 《电子数据存证技术规范》

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1 电子证据取证 Digital Evidence Acquisition

利用专业的网络技术和工具，在信息网络环境中对电子数据进行收集、提取、分析和保存，以获取能够作为法律证据使用的网络信息的过程。

3.2 电子证据存证 Digital Evidence Preservation

通过信息网络向用户提供电子数据证据保管和验证的服务

3.3 公证机构 Notary Office

公证机构是依法设立，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。公证机构根据自然人、法人或者其他组织的申请，办理保全证据公证等公证事项。

3.4 公证机构服务器 Notary Office Server

公证机构服务器指由公证机构通过采购或租赁方式，拥有所有权、使用权和管理权，用于固定、存储和管理电子证据的服务器。

3.5 电子证据存取证平台 Digital Evidence Collection and Storage Platform

由公证机构及其他公立电子证据取证、存证机构向使用者以网站、应用程序和编程接口等形式提供电子数据存证服务的软件或系统。

3.6 区块链系统 Blockchain Systems

一种在对等网络环境下，通过透明和可信规则,构建不可伪造、不可篡改和可追溯的块链式数据结构,实现和管理事务处理的模式。

3.7 PKI 技术 Public Key Infrastructure technology

公钥基础设施，是提供公钥加密和数字签名服务的系统，实现自动管理密钥和证书，保证网上数字信息传输的机密性真实性、完整性和不可否认性。

3.8 电子签名技术 Electronic Signature Technology

使用公钥密码学原理，通过数字签名实现电子文档的签名和认证。

3.9 可信时间标识 Trusted Timestamp

唯一的标识某一刻时间的字符序列。电子证据存证的系统时间及生成的可信时间标识应从国家可信时间源进行授时和守时。

注：该标识不仅可以标识出行为的发生时间，还可以通过时间的先后顺序构建带时序的证据链条。

3.10 数据接口和编程接口 Data Interface and Programming Interface

对不同来源、格式的数据进行转换处理，用于电子证据上链的数据转换和编程接口。

3.11 开放性校验 Open Check

通过开放接口实现电子证据的校验功能。

3.12 司法区块链 Judicial Blockchain

指以北京互联网法院“天平链 ”为代表的，由司法机关主导建设、管理及运营的区块链系统。司法区块链的重要意义在于：通过充分运用区块链数据防篡改技术，提升司法公信力；充分发挥区块链优化业务流程的重要作用，提高司法效率；充分挖掘区块链互通联动的巨大潜力，增强司法协同能力；充分利用区块链联盟互认可信的价值属性，服务社会治理需求。

3.13 天平链 Tianping Blockchain Introduction

天平链通过利用区块链本身技术特点以及制定应用接入技术及管理规范，实现了电子证据的可信存证、高效验证，降低了当事人的维权成本，提升了法官采信电子证据的效率。天平链由北京互联网法院联合北京市高级人民法院、司法鉴定机构、公证机构等司法机构以及行业组织、央企、金融机构、互联网平台作为其节点共同组建。

3.14 元数据 Metadata

描述数据的数据，用于支持数据的管理和检索功能。元数据包括数据属性、数据源信息、数据转换描述、数据存储位置、历史数据、资源查找、文件记录等。

4 规范性要求

4.1 电子证据取证

电子证据存取证平台应提供电子取证功能，支持对至少一种电子证据的识别提取，确保取证过程符合现行法律、法规的相关规定,保障取证数据的合法性、客观性、关联性和完整性。取证环境应进行清洁性检查，确保取证环境中无非法程序。取证范围可覆盖证据持有方自有的数据源、网络信息、事实证明性信息等。固定关键的证据信息,保留必要的元数据,生成标准格式的电子证据记录。取证过程宜制定完整、规范的操作流程,并保留完整的操作日志,以支持取证行为的审查。

4.2 电子证据存证

电子数据存取证平台应提供电子证据存证功能，系统主要功能宜分为业务层、逻辑层和存储层。系统通过业务层接收电子证据数据后，借助逻辑层的存证逻辑，将电子证据数据存储在存储层，以实现对电子证据的提取、存证和长期保存。

电子证据存证功能的系统架构可基于司法区块链的电子证据存证系统架构实现，主要功能可分为业务层、逻辑层、智能合约层、区

块链层，以与区块链系统相对应。可通过智能合约形成电子证据的存证智能合约，将电子证据数据分片存储在司法区块链上。业务层中的电子证据提取模块可接入各证据来源，识别并提取证据相关信息，生成电子证据记录。逻辑层的证据存证模块可利用智能合约在司法区块链上完成证据的存证，并生成证据指纹。存储层的证据长期保存模块可复制证据到存储设备。

公证机构及其他公立电子证据取证、存证机构可以通过标准接口接入系统,提出证据存证请求,完成司法认证程序,有助于电子证据的司法认可。

4.3 电子证据完整性

.电子证据存取证系统应保障存储的电子证据的完整性，保障方式可综合运用下列技术手段,确保证据的真实性、完整性和不可篡改性。

4.3.1 电子签名技术。利用数字证书认证机构(CA)颁发的电子签名证书，验证证据内容的签名是否来自证明方。

4.3.2 可信时间标识技术。对证据增加可信时间标识，确定证据生成时间。

4.3.3 认证技术。在取证或存证时加入证据主体认证环节，确保证据主体非冒用。

4.3.4 完整性校验技术。取证或存证时，使用完整性校验算法计算证据的完整性校验值并保存。

4.3.5 开放性校验技术。支持通过第三方开放接口查询证据内容，

保证开放性校验。

4.4 证据链保障

4.4.1 电子证据存取证平台生成的所有电子证据原文件，可存储在公证机构及其他公立电子证据取证、存证机构的文件服务器上。公证机构及其他公立电子证据取证、存证机构可以随时根据存储的电子证据原文件，出具相关的电子证据证明文件。

4.4.2 电子证据证明文件中可包含证据原文件存储路径，宜包含证据检验方法、证据关键信息摘要等内容，确保能够追溯验证电子证据的完整性。

4.4.3 所有证据基础信息，可包括原始电子证据文件存储记录、证据元数据、证据证明信息等，宜记录在安全存储系统中，以形成完整的证据生命周期记录，确保证据信息的可追溯性。

4.4.4 电子证据存取证平台宜提供的证据核验功能，可充分利用司法区块链系统，支持当事人和法官在线核验通过区块链存储的电子证据的真实性，提升电子证据认定的效率和质量。

4.5 证据获取

4.5.1 电子数据存取证平台宜支持获取包括电子合同、电子邮件、电子账本、电子监控记录、网络访问日志等多种格式的电子数据。

4.5.2 获取渠道可包含证据持有企业的各类电子系统、公共云服务系统中的数据资料、网络服务提供商的使用日志等。

4.5.3 获取证据时应遵守相关法律规定，确保获取行为合规、获

取内容真实完整。

4.5.4 应收集证据类型、来源、获取时间等标准元数据。可加密存档原始证据，保证后续审核和证据链追踪时信息完整。

4.6 证据存储

4.6.1 原始电子证据文件可存储在公证机构及其他公立电子证据取证、存证机构的数据中心内的确权存储服务器上，服务器应为内部独立管理。

4.6.2 应在存储系统中存储证据文件内容哈希值、可信时间标识等元数据。

4.6.3 存储服务器应具备安全稳定的系统软硬件，设置访问控制权限及加密机制，满足防篡改和长期保存需要。

4.6.4 应采取存储多份副本的冗余备份机制，并可使用区块链、可信时间标识等防篡改措施。

4.6.5 原始电子证据文件在存储完成后的第一时间存储数字摘要值到电子证据存取证平台，平台返回存证编号。

4.7 证据校验

4.7.1 支持对证据文件进行数字签名验证，确保签名来源真实有效，保护内容不被篡改。

4.7.2 通过比较证据文件的当前哈希值与存入系统时的哈希值，检查文件内容是否被非法修改。

4.7.3 对证据文件及操作记录均打上可信时间标识，并检查时间

连续性，防止时间伪造。

4.7.4 系统可生成效验报告,说明效验过程、结果等，提供给司法机构作为证据效力的依判断据。

4.7.5 司法审判机关、调解组织及相关人员，可以在系统对外服务页面，使用电子证据文件的存证编号或哈希值，在线勘验电子数据的真实性。

4.8 证据安全

4.8.1 电子数据存取证平台应设置基于角色的访问控制机制，区分操作人员、管理人员、审核人员等不同权限级别。

4.8.2 应启用日志审计、网络入侵检测等手段，监控证据传输与存储全流程，发现异常及时报警。

4.8.3 电子证据存取证平台的服务器宜与外网隔离，启用数据加密、访问认证、防篡改算法等技术措施。

4.8.4 公证机构及其他公立电子证据取证、存证机构宜制定完备的管理制度，明确证据处理标准流程和操作规范,对人员进行安全意识培训。