

北京互联网法院天平链标准

BICB-002-2019

天平链应用接入技术规范

2019 - 12 - 2 发布

2019 - 12- 2 实施

北京互联网法院 发布

目 次

前 言.....	II
引 言.....	III
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
3.1 时间戳.....	1
3.2 数字证书.....	1
3.3 区块链.....	1
3.4 电子数据摘要.....	1
3.5 电子签名.....	1
4 技术规范.....	2
4.1 技术规范概述.....	2
4.2 系统安全性要求.....	2
4.2.1 入侵防范.....	2
4.2.2 恶意代码防范.....	2
4.2.3 程序可信执行.....	2
4.2.4 数据完整性.....	2
4.2.5 数据保密性.....	3
4.2.6 访问控制.....	3
4.2.7 安全策略和管理制度.....	3
4.2.8 日志.....	3
4.3 电子数据合规性要求.....	4
4.3.1 电子数据生成主体.....	4
4.3.2 电子数据生成时间.....	5
4.3.3 电子数据提取与固定.....	5
4.3.4 电子数据传输.....	5
4.3.5 电子数据存储.....	6
4.3.6 电子数据验证.....	6
4.3.7 版本管理.....	6
4.4 区块链安全性测评.....	7
4.4.1 稳定性.....	7
4.4.2 共识算法.....	7
4.4.3 权限控制.....	7
4.4.4 节点.....	7
4.4.5 可管可控.....	7
4.4.6 智能合约安全.....	8
参 考 文 献.....	9

前 言

在北京互联网法院的互联网诉讼模式中，天平链是基于区块链技术的司法联盟链，实现电子证据的可信存证、高效验证，从而降低当事人的维权成本，提升法官采信电子证据的效率。

区块链技术只能够确保数据上链存储后不可篡改和不可删除，为解决数据上链前合规性的问题，制定了本规范和《天平链应用接入管理规范》，旨在加强对司法行业的电子数据及平台建设合规性的管理，切实保障天平链安全、稳定地运行。本规范规定了接入平台申请接入天平链前需进行的技术测评要求，《天平链应用接入管理规范》则规定了申请接入平台的意向申请、正式申请和受理、组织评审、接入许可与公布等流程管理要求。

本标准由北京互联网法院提出并归口。

本标准起草单位：北京互联网法院、国家工业信息安全发展研究中心、北京信任度科技有限公司、标新科技（北京）有限公司司法鉴定所、中国电子信息产业发展研究院、中国电子技术标准化研究院、国家信息中心、公安部第一研究所、中国信息通信研究院。

本标准主要起草人：潘妍、孙伟、朱晔、马臣云、张寅、万晨阳、雷虎、张羽、李炜祎、李文宇、文静、李嘉露、刘玄、毛立明、王佳慧、白雪燕。

本标准为首次发布。

引 言

北京互联网法院天平链应用接入技术规范规定了接入平台申请接入天平链前需进行的技术测评要求，为接入平台接入天平链提供具体指导。

天平链应用接入技术规范

1 范围

本规范规定了接入天平链的申请接入单位在系统安全性、电子数据合规性、区块链安全性三个方面的基本技术要求。

本规范适用于天平链的申请接入平台,为申请平台接入天平链所需进行的安全性和合规性建设提供技术指导。本规范同样适用于对天平链申请接入平台进行测评的测评机构和评审组,为其测评提供技术依据。

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。

天平链应用接入管理规范

GB/T 28449-2019 信息安全技术网络安全等级保护基本要求

GB/T 20520-2006 信息安全技术 公钥基础设施 时间戳规范

GB/T 25064-2010 信息安全技术 公钥基础设施 电子签名格式规范

GB/T 29361-2012 电子物证文件一致性检验规程

GA/T 756-2008 数字化设备证据数据发现提取固定方法

3 术语和定义

下列术语和定义适用于本文件。

3.1 时间戳

使用数字签名技术产生的数据,签名的对象包括了原始文件信息、签名参数、签名时间等信息。时间戳机构对此对象进行数字签名产生时间戳,以证明原始文件在签名时间之前已经存在。

3.2 数字证书

第三方电子认证机构签发的电子签名认证证书,用于实现对证书持有者身份的认证。

3.3 区块链

是一种由多方共同维护,使用密码学保证传输和访问安全,能够实现数据一致存储、防篡改、防抵赖的技术体系。

3.4 电子数据摘要

即哈希值(HASH),是对文件内容数据通过逻辑运算得到不可逆的唯一数据散列值

3.5 电子签名

是指数字电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。电子签章为电子签名可视化表现形式。

4 技术规范

4.1 技术规范概述

技术规范主要从系统安全性、电子数据合规性、区块链安全性三个方面对申请接入平台进行规范。

4.2 系统安全性要求

系统安全性要求。申请接入单位的接入平台应通过信息安全等级保护三级认证,确保电子数据生成、收集、存储、传输所依赖的计算机系统等硬件、软件环境安全、可靠。下述指标项要求在测评报告中结果为符合:包括入侵防范、恶意代码防范、程序可信执行、数据完整性、数据保密性、访问控制、安全策略和管理制度等。

4.2.1 入侵防范

指标项	技术要求
入侵防范	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为; 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为; 应采取技术措施对网络行为进行分析,实现对网络攻击特别是新型网络攻击行为的分析; 当检测到攻击行为时,记录攻击源 IP、攻击类型、攻击目的、攻击时间,在发生严重入侵时间时应提供报警。

4.2.2 恶意代码防范

指标项	技术要求
恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除,并维持恶意代码防护机制的升级和更新。

4.2.3 程序可信执行

指标项	技术要求
程序可信执行	具备可信验证机制,对系统程序、应用程序和重要配置文件/参数进行可信执行验证; 应在检测到其完整性受到破坏时采取恢复措施等手段。

4.2.4 数据完整性

指标项	技术要求
数据完整性	应采用校验技术或密码技术保证重要数据在传输过程中的完整性; 应采用校验技术或密码技术等保证重要数据在存储过程中的完整性; (数据包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等)。

4.2.5 数据保密性

指标项	技术要求
数据保密性	应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

4.2.6 访问控制

指标项	技术要求
访问控制	应对登录的用户分配账户和权限； 应授予管理用户所需的最小权限，实现管理用户的权限分离； 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。

4.2.7 安全策略和管理制度

指标项	技术要求
安全策略	应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。
管理制度	应对安全管理活动中的各类管理内容建立安全管理制度； 应对管理人员或操作人员执行的日常管理操作建立操作规程； 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系等。

4.2.8 日志

测评项	测评内容
日志集中管控	应部署日志服务器对日志进行收集等。

4.3 电子数据合规性要求

合规性要求。申请接入单位的接入平台应通过天平链备案测评机构合规性评估。合规性的基本要求包括电子数据的生成主体明确、数据生成时间明确、电子数据提取手段可靠、电子数据传输安全、电子数据的存储可靠、数据完整性保护手段可靠等。测评机构测评时应覆盖此技术要求。

4.3.1 电子数据生成主体

4.3.1.1 账户实名

指标项	技术要求
个人实名	个人用户在法律、法规规定需要进行实名认证的业务或服务请求之前，应根据相关法律、法规或管理制度要求进行实名核验； 核验信息应利用政府权威部门的数据库或取得政府权威部门授权或认可的数据库，或者采用生物特征识别技术或其他安全有效的技术手段等进行人证合一的确认。
企业实名	企业用户在法律、法规规定需要进行实名认证的业务或服务请求之前，应根据相关法律、法规或管理制度要求先行进行实名核验；核验信息应利用政府权威部门的数据库或取得政府权威部门授权或认可的数据库，或者采用其他安全有效的技术手段等进行企业证件、资料等的真实性确认。
认证过程及结果留痕	应对认证结果留痕； 应对认证过程日志信息采取防篡改、防灭失等技术保护手段。

4.3.1.2 账户认证

指标项	技术要求
账户安全认证方案	应保证账户安全认证的强度，应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
账户安全及密码产品的资质	使用的安全认证产品应具备公安部颁发的计算机信息系统安全专用产品销售许可证； 涉及密码技术的平台，应具备国家密码局颁发的商用密码产品型号证书； 拥有其安全能力的其他证书。
账户操作日志留痕	对账户的操作应留痕，留痕信息应采取防篡改、防灭失等技术保护手段。

4.3.1.3 电子签名

指标项	技术要求
可靠电子签名	应满足《电子签名法》中有关可靠电子签名的要求。
可靠电子签名产品的资质	电子签名产品应支持国产密码算法； 电子签名产品应具备国家密码局颁发的密码产品型号证书； 密码产品型号应遵循相应类别的安全等级标准。
签名人数字证书	签名人数字证书应当合规和有效。

4.3.2 电子数据生成时间

4.3.2.1 时间源

指标项	技术要求
时间来源	时间来源应当可靠； 时间来源具备权威性，来自于国家授时中心的授时。
时间源获取日志留痕	应对获取时间操作留痕，留痕信息应采取防篡改、防灭失等技术保护手段。

4.3.2.2 时间戳

指标项	技术要求
可靠性	时间戳技术具备可靠性； 采取类如数字证书签名、区块链等技术手段形成可靠的时间戳数据。
权威性	基于 CA 的时间戳，其时间戳签发机构的具备相关资质。

4.3.3 电子数据提取与固定

4.3.3.1 取证工具

指标项	技术要求
取证工具	取证工具可靠； 具备清洁度检查功能； 取证过程可以追溯； 取证工具具备第三方安全测评报告。
取证过程留痕	取证过程应留痕，包括清洁度检查操作过程、数据采集日志、数据存储日志等； 留痕信息应采取防篡改、防灭失等技术保护手段。

4.3.3.2 数据固定

指标项	技术要求
数据固定	通过取证工具采集的数据内容不可以修改，或者修改后能否被发现； 采取数字签名、时间戳、电子数据摘要、区块链等技术手段进行固定。

4.3.4 电子数据传输

指标项	技术要求
传输机密性	应采取加密手段确保数据机密性； 加密算法支持国产应密码算法； 密钥协商、密钥保护手段安全； 使用具备密码产品型号的产品。
传输完整性	应采用电子数据摘要、数字签名、HMAC 等密码技术手段确保数据完整性； 不应采用 MD5、RSA1024、DES 等弱安全等级算法；

指标项	技术要求
	密码算法支持国产密码算法； 使用具备密码产品型号的产品。
传输设备的安全保障能力	电子数据传输设备应满足电子数据传输要求的安全功能、并且已正确启用和配置相关功能，并且日常运维流程中有保障此范围内功能的条款，且具备有效的执行记录。

4.3.5 电子数据存储

指标项	技术要求
存储可靠性	检查提供安全、可靠的存储环境。
存储时限	作为证据的原始数据，保存时限不低于 60 个月； 对于行业主管部门有特殊要求或规定的，应对标相关管理规定。
不可篡改	应采取电子签名、区块链、电子数据摘要等技术手段确保数据不可篡改； 或者数据修改后能否被发现。
安全管理	应具备健全的信息安全保护制度、内部人员安全管理制度，以及相关流程制度执行的相关记录等，确保无信息泄露。
敏感信息过滤	除了需要承诺不存储反动、暴力、色情等相关内容。还应当有技术手段保障敏感信息的过滤功能。
数据规范性	欲接入天平链存入的数字摘要对应的数据原文信息，应该包括明确的主体、时间以及相关附属信息。
日志信息	应有完整的日志信息。日志中所记录的数据采集、存储、时间戳、账户认证等关键操作相关联的时间、进程、账户名称、操作内容、对象、存储路径等信息准确完备。

4.3.6 电子数据验证

指标项	技术要求
数据验证	生成、提取、固化的电子数据可以通过技术手段验证其生成主体身份结果、生成时间、操作的规范性、数据的不可篡改性等。

4.3.7 版本管理

指标项	技术要求
接入平台版本管理	接入平台应具备相应的软件版本管理制度及技术，并在每次升级后将版本信息固化。

4.4 区块链安全性测评

区块链安全性要求。申请接入单位的接入平台如采用区块链技术跨链对接天平链的，应通过天平链备案测评机构进行区块链安全性测评。区块链安全性基本要求包括稳定性、共识算法、权限控制、节点、可管可控、智能合约安全等。测评机构测评时应覆盖此技术要求。

4.4.1 稳定性

指标项	技术要求
高压力稳定性	保持始终有未确认交易的压力，评估区块链系统高压力下的稳定性以及峰值处理能力等。
低压力稳定性	保持所有交易均可完成，评估区块链系统低压力下的稳定性以及平均处理速度等。

4.4.2 共识算法

指标项	技术要求
多节点共识	具备多节点互不信任的基础上达成共识； 确保节点上链数据打包区块的计算能收敛并达到最终一致性等。
共识抗攻击与容错	有明确的抗恶意攻击指标等； 能保证当任意不超过区块链平台声明数量的节点发生故障，整个系统工作正常。

4.4.3 权限控制

指标项	技术要求
节点权限	区块链系统可以建立管理节点，履行管理责任； 节点的接入应具备权限控制等。
用户权限	用户的接入应具备权限控制等。

4.4.4 节点

指标项	技术要求
节点数	节点数量应大于等于4。
节点单位资质	节点各单位应具有相应资质和能力； 节点单位不能具有关联关系等。

4.4.5 可管可控

指标项	技术要求
管理能力	区块链平台应具备管理能力； 应具备节点状态监测、权限管理、告警查看、处置违规节点、应急处置等功能。

指标项	技术要求
存证内容管控	区块链平台应具备存证内容管控能力； 应建立用户实名认证管理制度； 应具备信息发布审核能力； 应建立信息巡查机制，定期对区块链应用用户可见信息进行巡查，及时发现处置违法有害信息； 建立用户网络行为日志留存机制，通过对用户行为日志的审计实现对区块链违规用户行为的溯源。

4.4.6 智能合约安全

指标项	技术要求
运行环境安全	合约应支持图灵完备语言； 应能够处理异常调用等。
合约实现安全	不应存在溢出漏洞； 关键逻辑判断不依赖区块链系统的变量（区块哈希、时间戳等）等。
合约交互安全	合约与外部应用的交互安全等。

参 考 文 献

- [1] 工业和信息化部信息中心. 2018 年中国区块链产业白皮书, 2018.
 - [2] 中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书, 2018.
 - [3] ISO/AWI 23257 Blockchain and Distributed Ledger Technologies—Reference Architecture, 2018.
 - [4] The Ethereum Foundation. Ethereum Homestead Documentaion, <http://www.ethdocs.org/en/latest>. 2018.
-