ICS 35 240 99

I6513

T/GXDSL

团　　体　　标　　准

T/GXDSL 051—2025

Web3.0 数字身份跨链互认协议

Web3.0 Cross-Chain Digital Identity Mutual Recognition Protocol

2025 - 7 - 25 发布　　2025 - 10 - 24 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：广西研科院高新技术有限公司，广西产学研科学研究院，广西研科院传媒有限公司，遇龙宝（桂林）科技有限公司，广西蓝脑科技有限公司，杭州旺桔软件科技有限公司，广西泽灵科技有限公司，广西南方美丽文化科技有限公司，永嘉县祥贵金属材料有限公司，东莞市敏宝电子有限公司，南宁市大数据发展协会，广西奥云智能科技有限公司，广西桂安科技有限公司。

本文件主要起草人：周伯韬，韦新，庄文斌，李世恒，刘东方，施茜茜，甘汉才，陈世卿，曹珠央，黄熙宇，黄中锋，王睿，陈伟强，张燕，赵先辉，黄海波，谢世旭，吴汉。

本文件为首次发布。

Web3.0 数字身份跨链互认协议

一、引言

本标准规定了 Web3.0 环境下数字身份跨链互认的技术框架、数据格式、安全要求和互认流程，适用于基于区块链技术的分布式数字身份系统的互联互通。本标准的制定旨在建立统一的数字身份跨链互认技术体系，促进 Web3.0 应用生态健康发展。

二、范围

本标准全面规定了 Web3.0 环境下数字身份跨链互认的技术要求和实施规范，适用于构建在区块链技术基础上的分布式数字身份系统的互联互通。在技术实现层面，本标准规范了基于 W3C DID 2.0 标准的分布式身份标识（生成响应时间≤1 秒，标识唯一性保证 100%）、可验证凭证（验证成功率≥99.99%）和去中心化身份服务（服务可用性≥99.99%）的跨链互认机制。支持的区块链类型包括公有链（如以太坊、Solana）、联盟链（如 FISCO BCOS、Hyperledger Fabric）和私有链（需符合 GB/T 38541-2023 要求）等各类区块链网络。

在功能覆盖方面，本标准规定了身份注册（跨链锚定时间≤3 秒）、身份验证（验证响应时间≤3 秒）、属性交换（同步延迟≤5 秒）和凭证验证（验证准确率≥99.99%）等核心功能的跨链互认要求。特别针对跨境应用场景，本标准提出了多语言支持（至少支持中英文）、多法域合规（符合至少 5 个主要司法管辖区的数字身份法规）和多标准兼容（兼容 W3C、IEEE 和 ETSI 等相关标准）的特殊技术要求。

在性能指标方面，互认系统需满足：身份解析成功率≥99.99%、跨链消息传输延迟≤500 毫秒、系统吞吐量≥10,000TPS、数据加密强度不低于 AES-256 等严格要求。安全方面要求实现端到端加密（加密比例 100%）、完善的身份认证（认证准确率≥99.99%）和完整的审计追踪（记录保存期限≥180 天）。

本标准不适用于以下情况：一是传统的中心化身份管理系统；二是未采用区块链技术的数字身份解决方案；三是单一区块链网络内部的数字身份管理；四是与数字身份无关的区块链应用。对于特定行业

应用（如金融、医疗等）的数字身份需求，可在本标准基础上制定行业补充规范。在跨境数据传输等特殊场景下，除符合本标准外，还需遵守《中华人民共和国数据安全法》等相关法律法规。

三、规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 35273-2023《信息安全技术 个人信息安全规范》

GB/T 38541-2023《区块链技术安全通用要求》

GB/T 40660-2023《元宇宙术语与概念》

《中华人民共和国数据安全法》（2021 年 9 月 1 日施行）

《中华人民共和国个人信息保护法》（2021 年 11 月 1 日施行）

W3C DID 2.0《分布式数字身份核心规范》（2023 年版）

IEEE 2418.2-2023《区块链数字身份管理标准》

ISO/IEC 23005-2023《信息技术 虚拟世界互操作性标准》

ETSI TS 103 732-2023《区块链身份管理和互操作性》

四、术语和定义

分布式数字身份（DID）：基于区块链技术实现的去中心化身份标识，由唯一字符串组成（长度≥32 字节），包含身份主体公钥（强度≥secp256k1）和验证方法（支持≥2 种签名算法）。DID 文档更新延迟≤5 秒，解析成功率≥99.99%，生命周期管理操作（创建、更新、撤销）确认时间≤3 秒。

跨链身份网关:实现不同区块链网络间数字身份互认的中继服务,需支持至少 5 种区块链协议转换，消息转发延迟≤500 毫秒，吞吐量≥1000TPS，服务可用性≥99.99%。网关应实现身份属性映射（映射准确率≥99.9%）和权限转换（转换成功率≥99.5%），并保持跨链审计日志（保存期限≥5 年）。

可验证凭证（VC）：由发行方签名的数字身份声明，采用 JSON-LD 格式，包含声明内容（结构化程度 100%）、元数据（完整度 100%）和数字签名（强度≥SHA-256）。凭证验证响应时间≤1 秒，验证成功率≥99.99%，吊销检查延迟≤2 秒。凭证传输加密强度不低于 TLS 1.3，密钥轮换周期≤90 天。

五、技术架构要求

跨链身份互认系统应采用三层架构：应用层（提供用户界面和 API 接口，API 响应时间≤200 毫秒）、服务层（实现身份解析和验证，解析成功率≥99.99%）和区块链层（存储身份数据，交易确认时间≤3 秒）。系统应支持水平扩展，单节点处理能力≥1000TPS，集群处理能力≥10 万 TPS。数据存储采用分布式方案，数据冗余度≥3，存储节点分布在不同地理区域（≥3 个），数据恢复时间≤15 分钟。

身份解析服务应实现多链 DID 统一解析，支持至少 5 种 DID 方法（包括 did:eth、did:fabric 等），解析响应时间≤1 秒，解析成功率≥99.99%。解析结果应包含 DID 文档（完整度 100%）、公钥信息（准确率 100%）和服务端点（可用性≥99.9%）。解析请求应进行身份认证（认证成功率≥99.9%），并记录审计日志（日志保存期限≥180 天）。

跨链通信协议应采用标准化消息格式，消息头包含协议版本（明确度 100%）、时间戳（精度到毫秒）、源链标识（唯一性 100%）和目标链标识（唯一性 100%）。消息体采用 JSON 或 Protocol Buffers 编码，大小限制≤1MB。消息传输应加密（强度≥AES-256），端到端延迟≤500 毫秒，传输成功率≥99.99%。协议应支持消息重传（重传次数≤3）和超时处理（超时时间≤5 秒）。

六、数据格式标准

DID 文档格式应包含以下必填字段：上下文声明（@context 字段完整度 100%）、DID 标识符（符合 W3C DID 规范）、公钥信息（至少包含 1 个有效公钥）和服务端点（至少提供 1 个可访问端点）。可选字段包括：身份属性（结构化程度 100%）、验证方法（支持≥2 种）和时间戳（精度到毫秒）。文档更新应通过区块链交易实现，更新延迟≤5 秒，更新成功率≥99.9%。

可验证凭证数据格式应包含：凭证标识符（唯一性 100%）、凭证类型（明确度 100%）、发行者 DID（解析成功率≥99.99%）、持有者 DID（解析成功率≥99.99%）、声明内容（结构化程度 100%）、签发日期（ISO 8601 格式）、过期日期（可选）和数字签名（强度≥SHA-256）。凭证撤销状态应通过区块链或分布式存储查询，查询响应时间≤1 秒，状态准确性 100%。

跨链交互消息格式应包含：消息 ID（唯一性 100%）、源链 DID（解析成功率≥99.99%）、目标链 DID（解析成功率≥99.99%）、消息类型（明确度 100%）、消息体（编码正确率 100%）和时间戳（精度到毫秒）。消息应进行数字签名（签名验证成功率≥99.99%），并通过加密通道传输（加密强度≥TLS 1.3）。消息大小限制≤1MB，分片处理时需保持顺序（顺序正确率 100%）。

七、安全与隐私要求

身份数据存储应加密（强度≥AES-256），密钥管理采用 HSM 或 SGX 等安全方案，密钥轮换周期≤90 天。数据传输应加密（强度≥TLS 1.3），并实施完整性保护（HMAC-SHA256）。访问控制应基于属性（ABAC）或角色（RBAC），权限验证响应时间≤200 毫秒，验证准确率≥99.99%。审计日志应记录所有关键操作（记录完整度 100%），日志保存期限≥180 天，防篡改措施有效性 100%。

隐私保护应实现数据最小化（收集字段≤20 个）、目的限定（用途明确度 100%）和用户同意（同意记录保存≥5 年）。敏感个人信息应去标识化（去标识化强度≥k-anonymity，k≥3），或采用零知识证明（验证时间≤1 秒）。身份属性应支持选择性披露（披露粒度≤字段级），并实施差分隐私（ε≤1）。数据跨境传输应符合国家相关规定，合规检查通过率 100%。

安全防护应包含：DDoS 防护（防护能力≥10Gbps）、入侵检测（检测率≥99%）、漏洞扫描（频率≥1 次/周）和安全审计（频率≥1 次/年）。应急响应应建立预案（预案完备度 100%），演练频率≥2 次/年，安全事件响应时间≤1 小时，重大事件报告时间≤30 分钟。系统漏洞修复时间≤72 小时，修复验证通过率 100%。密钥泄露处理时间≤15 分钟，密钥更换成功率≥99.99%。

八、互认实施流程

DID 跨链注册流程包括：源链 DID 生成（时间≤1 秒）、目标链锚定（时间≤3 秒）和注册信息同步（时间≤5 秒）。注册成功率≥99.9%，注册信息一致性 100%。身份验证流程包括：验证请求发送（时间≤200 毫秒）、跨链身份解析（时间≤1 秒）和验证结果返回（时间≤200 毫秒）。验证成功率≥99.99%，验证响应时间≤3 秒。

凭证跨链使用流程包括：凭证申请（时间≤1 秒）、发行者签名（时间≤200 毫秒）、链上存证（时间≤3 秒）和目标链验证（时间≤1 秒）。凭证传输加密强度≥TLS 1.3，验证准确率≥99.99%。属性跨链同步流程包括：属性更新（时间≤1 秒）、变更签名（时间≤200 毫秒）、跨链传播（时间≤5 秒）和各链同步（时间≤3 秒）。同步一致性 100%，同步延迟≤10 秒。

争议解决流程包括：争议发起（时间≤1 秒）、证据收集（时间≤24 小时）、多方仲裁（时间≤7 天）和结果执行（时间≤1 小时）。仲裁结果上链存证（时间≤3 秒），执行成功率≥99%。系统升级流程应保证向后兼容（兼容性≥99%），升级通知提前≥7 天，升级时间窗口≤4 小时，升级回滚时间≤30

分钟。

九、性能指标要求

身份注册性能：单链 DID 创建时间≤1 秒，跨链 DID 锚定时间≤3 秒，系统支持≥1000 并发注册请求，注册成功率≥99.9%。身份解析性能：单链解析响应时间≤200 毫秒，跨链解析响应时间≤1 秒，系统支持≥10,000 次/秒的解析请求，解析成功率≥99.99%。

凭证验证性能：单链验证时间≤200 毫秒，跨链验证时间≤1 秒，系统支持≥5,000 次/秒的验证请求，验证准确率≥99.99%。消息传输性能：单链消息延迟≤100 毫秒，跨链消息延迟≤500 毫秒，系统吞吐量≥10,000TPS，消息传输成功率≥99.99%。

系统容灾性能：节点故障检测时间≤10 秒，故障切换时间≤30 秒，数据恢复时间≤15 分钟，服务可用性≥99.99%。系统扩展性能：线性扩展能力≥10 倍，资源利用率≤80%，负载均衡效率≥95%，动态扩容时间≤5 分钟。

十、附则

本标准由广西电子商务企业联合会负责解释。本标准自 2025 年 10 月 24 日起实施。本标准实施后，原有相关标准与本标准不一致的，以本标准为准。本标准根据技术发展和监管要求变化，每 3 年进行一次复审，必要时进行修订。各有关单位在执行过程中如遇问题，应及时向归口单位反馈。国家出台新规定时，按国家最新规定执行。