《区域性股权市场分布式数字身份技术规范（征求意见稿）》编制说明

《区域性股权市场分布式数字身份技术规范》

起草工作组

二〇二三年十月

一、背景及意义

区域性股权市场作为资本市场的塔基，是我国多层次资本市场的重要组成部分。分散自治的区域性股权市场具有市场主体多样、信息多源异构的特点，因此需要相应的身份管理标准作为支撑，以规范和指导区域性股权市场数字身份的系统建设和实施。

此外，随着个人信息保护法、数据安全法等法律条款的落地，数据作为一种生产要素也要同时满足持有人侧的数据所有权，因此面临着行业监管与个人隐私的矛盾。区域性股权市场分布式数字身份技术具有保证监管获取的市场数据真实可信、保护市场参与者隐私安全等特点，特别是每个市场主体的身份不是由可信第三方控制，而是由其自身控制，市场主体可以自主管理自己的身份；身份相关数据存储在区块链上，具备身份的安全性和自解释性，认证的过程也不需要依赖于提供身份的应用方；同时可以在区域性股权市场不同的应用场景中进行身份信息的交叉验证和查询。因此，区域性股权市场分布式数字身份技术能够有效解决和平衡监管部门以及市场参与者数据权益的要求。

本标准在W3C分布式数字身份和可验证凭证规范的基础上，结合区域性股权市场的特点，明确了区域性股权市场分布式数字身份的双层系统架构，规定了市场主体的编码规则、身份凭证的基本属性及管理流程，给出了分布式数字身份和可验证凭证在身份管理和数据流通中的应用示例。上述工作通过对分布式数字身份数据结构的规范定义来促进身份的互认互信和互联互通，通过引入可信凭证来解决数据流通中的认证授权和可信验证问题，从而为区域性股权市场分布式数字身份建设提供具体的技术指导。

二、工作简况

（一）组织保障

本文件起草单位：中证信息技术服务有限责任公司、中国证券监督管理委员会科技监管局、中国证券监督管理委员会市场二部、深圳证券通信有限公司、上海股权托管交易中心股份有限公司、北京交通大学、同济大学、山东省计算中心（国家超级计算济南中心）、北京邮电大学、南京大学、中证数据有限责任公司、

上海边界智能科技有限公司 、中诚区块链研究院（南京）有限公司、梧桐链数字科技研究院(苏州)有限公司、南京数字金融产业研究院有限公司、深圳市金证科技股份有限公司。

姚前、王建平、罗凯、蒋东兴、李宇、陈炜：标准战略指导；

蒋国庆、陈柏峰、路一、刘彬：标准制定方向指导、制订指导；

张大伟、彭枫：主笔人；王凤冬、杨博、马小峰、马宾、咸永锦、周琳娜、陈莹、陈强、李福琴、李彬、奚海峰、曹恒、张业龙、谷新萍、李智、柴荔、柴鄢旭、赵滨：标准主要起草人、制订人；

陈小泉、刘翔宇、张鸣谦、周耀亮、龚生智、叶蔚、黄玮、王伟、张海龙：标准试验负责人。

1. 预研

（1）2022 年 6 月，中证技术与北京交通大学、同济大学等单位组织区域性股权市场分布式数字第一次工作会议，启动分布式数字身份的规范建设。

（2）2022年7月，调研国内分布式身份的应用情况，参考W3C基本VC应用案例场景，通过分析讨论初步确定给出了分布式数字身份和可验证凭证的定义及结构，规定了分布式数字身份应用的关键业务流程，设计了基于分布式数字身份和可验证凭证的数据流通机制,形成分布式身份技术方案。

（3）2022 年 7 月至 9 月，根据分布式数字身份的技术方案文档，上海股权交易中心与上海市联合征信有限公司开展区域性股权市场 DID 分布式数字身份建设试点工作，通过 DID 分布式数字身份解决数据授权采集、融合使用问题，有效解决数据授权认证问题、简化数据交互、加强数据隐私保护。通过引入企业征信服务对 DID 数字身份证明进行在线解析和验证。

（4）2022 年 10 月至 2023 年 1 月，准备标准草案稿，准备标准立项相关材料。

（5）2023 年 2 月，立项申报，发起征求意见 69 个，收到回函数据量 51 个，同意立项数量 51 个，其中有建议或意见 0 个。

2. 立项

2023 年 8 月，开展标准项目立项的必要性和可行性研究，编写标准立项建

议书及相关请示材料，并由证标委秘书处下达标准立项计划（项目计划编号：P2023001）。

3. 起草

（1）2023 年 8 月至 9 月，中证技术基于负责的“基于区块链的区域性股权市场可靠监管技术研究”课题研究工作，结合区域性股权市场区块链试点项目建设成果开展标准草案编写，形成工作组讨论稿。

（2）2023 年 10 月至 2023 年 11 月，针对标准工作组讨论稿进行组内交叉复核，提出修订意见，完善标准草案稿。

4. 征求意见

（1）2023 年 11 月，完善标准草案，形成标准征求意见稿和编制说明，提交证标委秘书处。

5. 送审

6. 报批

三、编制主要内容

《区域性股权市场分布式数字身份技术规范》规定了区域性股权市场分布式数字身份和可验证凭证的定义及结构，规定了分布式数字身份应用的关键业务流程，设计了基于分布式数字身份和可验证凭证的数据流通机制：

1. 明确了区域性股权市场分布式数字身份的整体架构，包括：

（1）分布式数字身份中的基本组件及其关系；

（2）区域性股权市场相关主体的 DID 编码规则，相关主体主要包括市场服务企业、投资者、区域性股权市场运营机构、地方政府机构和监管机构；

（3）区域性股权市场 DID 存储及解析架构；

（4）区域性股权市场 DID 解析接口，包括：解析请求方式、解析返回结果、DID 解析元数据属性、DID 文档元数据属性等。

2. 明确了区域性股权市场 DID 文档及其属性，包括：

（1）DID 文档，DID 文档包含与 DID 相关联的信息。它通常包括验证方法以及与 DID 主体交互相关的服务，并在附录给出了 DID 文档示例；

（2）DID 文档中的相关属性，包括：标识、别名、控制着、验证方法、认

证、声明方法、服务等内容。

3. 明确了区域性股权市场可验证凭证及其属性，包括：

（1）可验证凭证 VC，是由相关机构颁发的用来描述实体在特定场景中身份属性信息的数字凭证，给出可验证凭证的使用过程中涉及到凭证的颁发者、凭证的持有者和凭证的验证者三方角色之间的关系；

（2）可验证凭证中的属性，包括：标识、类型、颁发者、颁发日期、失效日期、凭证状态、凭证主题、证明。

4. 明确了区域性股权市场可验证表述及其属性，包括：

（1）可验证表述 VP，可验证表述包括一或多个可验证凭证及其持有证明。凭证持有者通过可验证表述向凭证验证者出示其凭证数据并证明其正确的持有关系；

（2）可验证表述中的属性，包括：类型、持有者、可验证凭证、证明。

5. 明确了区域性股权市场分布式数字身份的关键业务流程，包括：

（1）DID 的创建

（2）DID 的撤销

（3）DID 的验证

（4）VC 的颁发

（5）VC 的验证

（6）VP 的验证

（7）VC 的撤销

6. 明确了以数据主体为中心、机构代理模式和以机构为中心的基于 DID 和 VC 的数据流通机制。

四、主要试验（或验证）分析

在本文件的研制过程中，上海股权交易中心采用该文件中涉及的规范成果进行实施并取得了成功，示例如下：

上海股权交易中心与上海市联合征信有限公司开展区域性股权市场 DID 分布式数字身份建设试点工作，通过 DID 分布式数字身份解决数据授权采集、融合使用问题，有效解决数据授权认证问题、简化数据交互、加强数据隐私保护。

通过引入企业征信服务对 DID 数字身份证明进行在线解析和验证。

五、与现行法律、法规、政策及其他标准的关系

本文件遵守中华人民共和国现行的法律、法规，并且符合 GB/T 1《标准化工作导则》系列标准的要求。

本文件规范性引用文件如下：

GB/T 25069 信息安全技术 术语

GB 32100 法人和其他组织统一社会信用代码编码规则

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

JR/T 0184 金融分布式账本技术安全规范

W3C Decentralized Identifiers (DIDs) v1.0

W3C Verifiable Credentials Data Model v1.1

W3C JSON-LD 1.1

W3C XML Schema Definition Language (XSD) 1.1 Part 2:Datatypes

RDF Dataset Normalization https://github.com/w3c-ccg/rdf-dataset-canonicalization

RFC 3986 Uniform Resource Identifier (URI): Generic Syntax

RFC 4648 The Base16, Base32, and Base64 Data Encodings

RFC 7517 JSON Web Key (JWK)

RFC 7797 JSON Web Signature (JWS) Unencoded Payload Option

RFC 8259 The JavaScript Object Notation (JSON) Data Interchange Format

六、重大分歧意见的处理经过和依据

在本文件的编写过程中，区域性股权市场分布式数字身份规范工作组成员对针对规范的内容进行了充分地研究和讨论，并多次征求各领域专家意见，在编制过程中并未出现重大分歧意见。

七、贯彻标准的要求和建议措施

本文件所涉及的内容适用于区域性股权市场分布式数字身份系统的建设。可用于指导、规范区域性股权市场分布式数字身份的设计、开发和应用。

八、行业标准属性的建议

鉴于本文件的内容未涉及强制性标准或强制性条文的内容及要求，因此建议本文件作为推荐性行业标准。

九、废止有关现行标准的建议

无。

十、其它说明事项

无。