ICS 03.060
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T XXXX—XXXX

区域性股权市场区块链跨链安全认证规范

Specifications for regional equity markets cross-chain authentication security

（送审稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国证券监督管理委员会　　发 布

目　　次

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。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC　180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC　180）归口。

本文件起草单位：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、中证信息技术服务有限责任公司、深圳证券通信有限公司、中证机构间报价系统股份有限公司、北京股权交易中心有限公司、江苏股权交易中心有限责任公司、上海股权托管交易中心股份有限公司、浙江省股权交易中心有限公司、深圳前海股权交易中心有限公司、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、南京数字金融产业研究院有限公司、北京共识数信科技有限公司、苏州同济区块链研究院有限公司、中钞信用卡产业发展有限公司、杭州区块链技术研究院。

本文件主要起草人：姚前、王建平、罗凯、蒋东兴、李宇、蒋国庆、彭枫、王继伟、陈柏峰、周云晖、王凤冬、刘彬、王少清、杨博、马堃、李思颖、陈小泉、刘翔宇、王亚军、王守超、王强、朱培、周耀亮、林智辰、葛浩、陶祖国、邵洪峰、孙北北、胡爽峰、肖东、奚海峰、曹恒、谷新萍、张业龙、赵滨、许明县、曹春峰、陈莹、邵俊杰、迟云蔚、马小峰、万强、叶蔚、张一锋、蔡伟鑫。

引　言

区域性股权市场是我国资本市场的重要组成部分，是多层次资本市场体系的基石。区块链技术与区域性股权市场分散特征天然匹配，从新型金融基础设施层面为场外参与各方提供公共的可信服务，以技术手段完善市场基础条件，弥补区域性短板，解决登记效力不足、信用支撑不足、连通性和透明规范性不足等基础性问题，更好地发挥区域性股权市场的灵活优势，激发创新活力。基于监管链和地方业务链的双层架构，可以更好地支持区域性股权市场登记业务、交易报告库等业务和监管创新。监管链跨链对接各区域股权市场地方业务链，以监管链治理地方业务链，同时为地方业务链赋能，支持业务创新和监管创新。从建立逻辑统一、互联互通的区域性股权市场新型金融基础设施出发，有必要定义监管链与各地方业务链的跨链对接安全认证技术标准。

区域性股权市场区块链跨链认证安全规范

1 范围

本文件规定了区域性股权市场中地方业务链与监管链跨链对接的安全认证技术与系统实现要求，包括国密证书、业务数据要求、地方业务链安全要求、地方业务系统安全要求、跨链机制要求及跨链安全要求。

本文件适用于在区域性股权市场中进行地方业务链及与地方业务链对接的地方业务系统建设或服务运营的机构。

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 11457—2006 信息技术 软件工程术语

GB/T 25069—2010 信息安全技术 术语

GB/T 32905-2016 信息安全技术SM3密码杂凑算法

GB/T 32918—2016 SM2椭圆曲线公钥密码算法

GM/T 0015—2012 基于SM2密码算法的数字证书格式规范

GM/T 0004—2012 SM3密码杂凑算法

JR/T 0184—2020 金融分布式账本技术安全规范

3 术语和定义

GB/T 11457—2006、GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

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。

[来源：JR/T 0193—2020，3.1]

3.2

区块 block

区块链中存储数据的单元。

[来源：JR/T 0193—2020，3.2]

3.3

网（络） network

对各实体及其互连所做的一种安排。
[来源：GB/T 5271.18—2008，2.18.01.01]

3.4

子网 subnetwork;subnet

在网络中，在元素间有一组共同特征，有明确界限，本身又能视为网络的一部分。
[来源：GB/T 5271.18—2008，2.18.01.05]

3.5

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖
[来源：GB/T 25069—2010，2.2.2.176]

3.6

数字证书 digital certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构进行数字签名的一个可信数字化文件。

3.7

证书认证机构 certificate authority

负责产生、签发和管理证书的、受用户信任的权威机构。用户可以选择该机构为其创建特定密钥
[来源：GB/T 25069—2010，2.2.2.218]

3.8

证书撤销列表 certificate revocation list

CA对撤销的证书而签发的一个列表文件。

3.9

共识协议 consensus protocol

分布式账本系统中各节点为达成一致采用的计算方法。
[来源：JR/T 0184—2020，3.17]

3.10

拜占庭容错 byzantine fault tolerance

在不可信环境中，即使系统部分组件失效或存在恶意角色，分布式系统仍然能够保持一致性要求的能力。
[来源：ITU-T X.1400-2020，6.11，有修改]

3.11

跨链 cross chain

实现在区块链之间的双向信息交互、信息验证与服务调用的技术。

3.12

交易 transaction

区块链上的一次原子性账本数据状态变更及其过程和结果记录，由交易标识符唯一标识。
[来源：ITU-T X.1400-2020，6.65，有修改]

3.13

监管链 global regulation blockchain

以全局服务和监管为目的构建的区块链系统。

3.14

地方业务链 regional business blockchain

各地方以服务区域性股权市场业务和生态为目的构建的区块链系统。

3.15

地方业务系统 regional business system

与地方业务链对接,实现数据传输到地方业务链的业务系统,包括区域性股权交易中心业务系统等。

3.16

业务数据 business data

地方业务系统存储和处理的数据。

3.17

业务数据主体 business data owner

业务参与方直接操作生成的数据，并作为该数据所有者的个人和机构。

3.18

智能合约 smart contract

一种旨在以信息化方式传播、验证或执行合同的计算机协议，其在分布式账本上体现为可自动执行的计算机程序。

4 缩略语

ECC：椭圆曲线加密（Elliptic Curve Cryptography）
VPC：虚拟私有云网络（Virtual Private Cloud）
VPN：虚拟专用网络（Virtual Private Network）
RPC：远程过程调用（Remote Procedure Call）

API：应用程序编程接口（Application Programming Interface）

5 国密证书

国密证书公钥算法采用ECC算法，公钥参数采用SM2国密算法。证书使用ASN.1编码，证书文件以二进制或Base64格式存放。证书中应包含证书版本、序列号、颁发者、使用者主体信息、使用者公钥、有效期、证书扩展项、算法标识等信息。

国密证书的公钥算法ECC算法标识、公钥参数SM2国密算法标识、证书签名算法标识、摘要算法标识应符合GB/T 32905—2016 和GB/T 32918—2016等相关国家标准以及GM/T0015—2012、GM/T0004-2012、JR/T 0184—2020等相关行业标准。

6 业务数据要求

6.1 生成主体明确

地方业务系统应在业务数据主体生成数据前，通过证件信息、数字证书等方式对业务数据主体的实名身份进行认证。

地方业务系统应采用技术手段认证业务数据主体的真实意愿性。

地方业务系统应对上述认证结果留痕，并采用技术手段对留痕信息防泄漏、防篡改。

6.2 数据生成时间明确

业务数据生成的时间应明确。

应对获取业务数据时间的操作进行日志留痕。留痕的日志信息应采取防篡改、防灭失等技术保护手段。

6.3 业务数据提取手段可靠

业务数据提取手段应可靠，通过采集的数据包内容应第一时间进行固化，采取数字签名、时间戳、数字摘要、区块链等技术手段进行完整性保护，修改后可被发现。

6.4 业务数据传输安全

应采取加密算法确保业务数据的机密性，加密算法应采用国产密码算法，密钥协商、密钥保护手段应安全，应使用具备密码产品认证的产品。

应采取数字摘要、数字签名、HMAC等密码技术确保业务数据传输的完整性，密码算法应采用国产密码算法。

6.5 业务数据的存储可靠

应确保业务数据存储的可靠性。应提供安全、可靠的存储环境，并具备备份、容灾技术手段和运维能力以及运维制度。

业务数据的保存时限不低于60个月。对于有特殊要求或规定的，从其规定。

业务数据应支持结构化和非结构化数据类型。

应采取电子签名、区块链、数字摘要等技术手段确保业务数据完整性。对相关数据进行修改后，应能发现。

应具备健全的信息安全保护制度、内部人员安全管理制度，确保不泄露。

6.6 数据完整性保护手段可靠

业务数据完整性保护手段应可靠，可通过技术手段验证业务数据的生成主体身份、生成时间、操作的规范性、数据的完整性。

7 地方业务链安全要求

7.1 数据操作安全

地方业务链应具备查询区块平均生成时间、总区块数以及指定区块中事务明细的功能。通过使用这些功能，应能获得一致、可靠的链上数据。

7.2 身份信息安全

地方业务链应能确保用户身份标识唯一性和可鉴别性。

地方业务链的校验鉴别信息应具有加密算法和数字签名的安全机制，确保区块链中不存在重复身份标识、身份鉴别信息不被冒用。

地方业务链应具有身份认证失败处理机制。

7.3 访问控制

7.3.1 访问控制功能

地方业务链应具有访问控制功能，依据安全策略控制用户对数据的访问。

7.3.2 访问控制覆盖范围

地方业务链访问控制的覆盖范围应包括：区块链访问相关的主体、区块链访问相关的客体以及区块链访问相关资源之间的操作。

7.3.3 访问控制策略和权限

地方业务链应用应由授权主体配置访问控制策略，并按照权限最小化、相互制约原则，为账户分配访问权限。

7.4 链间访问控制

7.4.1 链间访问控制功能

地方业务链应具有访问控制功能，依据安全策略控制其他区块链系统对本区块链数据的访问。

7.4.2 链间访问控制覆盖范围

地方业务链的链间访问控制的覆盖范围应包括：其他区块链系统对本区块链访问相关的主体、区块链访问相关的客体以及区块链访问相关资源之间的操作。

7.4.3 访问控制策略和权限

地方业务链应用应由授权主体配置其他区块链的访问控制策略，并按照权限最小化、相互制约原则，为账户分配访问权限。

7.4.4 共识协议

地方业务链需要采用支持节点拜占庭容错的共识算法，至少支持 1/3 节点容错。
地方业务链的节点不可全部部署到某一机构的服务器或单一云平台服务器上。
地方业务链应确保节点数据的一致性、可靠性和可拓展性。

7.5 智能合约

7.5.1 智能合约执行

地方业务链的智能合约的执行结果应明确，可通过逻辑推理得出与实际结果一致的执行结果。

7.5.2 查询支持

地方业务链的智能合约应支持索引、区间、历史查询等功能。

7.5.3 智能合约更新

地方业务链的智能合约应具有动态更新的功能；更新过程前后，地方业务链应运行稳定。

7.5.4 合约的冻结或终止

地方业务链的智能合约应具有冻结/终止功能。

7.6 稳定性

地方业务链应运行稳定，在始终有未确认交易的场景下，地方业务链仍能平稳运行。

8 地方业务系统安全要求

8.1 入侵防范

地方业务系统应能在关键网络节点处检测、防止或限制内外部发起的网络攻击行为；当检测到攻击行为时，地方业务系统应记录攻击信息，包括源网络地址、攻击类型、攻击范围、攻击时间。

8.2 恶意代码防范

地方业务系统应能检测并清除恶意代码，同时应维护对恶意代码的防护机制、升级和更新。

8.3 程序可信执行

地方业务系统应具备可信验证机制，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。地方业务系统应在检测到其完整性受到破坏时采取恢复措施。

8.4 访问控制

地方业务系统应做好用户访问控制管理，应对登录的用户分配相应的账户和权限。
地方业务系统的权限管理应遵从最小权限原则。
地方业务系统的访问控制粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级。

8.5 安全策略和管理制度

地方业务系统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。

地方业务系统应对安全管理活动中的各类管理内容建立安全管理制度。

地方业务系统应对要求管理人员或操作人员执行的日常管理操作建立操作规程。

地方业务系统应形成由安全策略、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。

9 跨链机制要求

地方业务链和监管链跨链对接要求：

a) 应采用公证人机制技术、哈希锁定技术、侧链/中继技术或其他安全的跨链技术；
b) 应提供跨链消息的输入、输出口径和真实性证明，跨链消息的有效路由；
c) 应构建跨链消息的统一格式，定义消息来源和去处以及消息的内容，跨链消息验证，以保障跨链之后的结果安全可信。

10 跨链传输信道安全要求

10.1 通过证券期货行业专线网络访问

在监管链和地方业务链之间建立专线，地方业务链与监管链通过证券期货行业专线进行通信。

10.2 通过 VPC 专线网络访问

在监管链和地方业务链之间建立专线，地方业务链与监管链通过专线进行通信。

10.3 通过 VPN 网络访问

在监管链和地方业务链之间建立VPN连接，监管链通过地方业务链局域网地址调用地方业务链RPC接口，此方式下通过互联网传输加密后的数据。

10.4 对 RPC 接口增加 API 鉴权

在地方业务链节点之上增加网关等鉴权服务，用于地方业务链RPC接口鉴权。监管链通过HTTPS方式访问鉴权服务，鉴权服务验证用户身份通过后，可转发到地方业务链RPC接口，鉴权服务只对调用者身份进行识别，不对接口返回数据进行任何修改。

10.5 IP 白名单

地方业务链应具备IP白名单机制，限制访问节点RPC接口IP。

11 跨链数据安全要求

11.1 基本要求

地方业务链和监管链跨链对接时，应保证数据传输的安全性与可靠性，所访问的数据，在地方链及监管链上的数据结果应确保一致。

11.2 数据访问时的要求

在监管链访问地方业务链数据时，应当完成数据校验，保障所传输的数据一致。

11.3 数据传输时的要求

在地方业务链向监管链传输数据时，应在传输完成后，进行数据完整性一致性的检查，保障所传输的数据一致。

11.4 智能合约调用时的要求

需要检验智能合约调用时的数据，以及智能合约返回的数据。保障跨链调研智能合约的结果，与本地调用时的结果一致。

参 考 文 献

[1] 中华人民共和国电子签名法