ICS 35.240.99
CCS R 85

团　　体　　标　　准

T/SZBA 001—2021

基于区块链的海运从业人员身份管理规范

Specification for identity management of maritime practitioners based on blockchain

（征求意见稿）

（本稿完成日期：2021.12.21）

2021－12－01 发布　　2022－02－01 实施

深圳市信息服务业区块链协会　　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。

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。

本文件由深圳百纳维科技有限公司提出。

本文件由深圳市信息服务业区块链协会归口。

本文件起草单位：深圳百纳维科技有限公司、深圳市信息服务业区块链协会。

本文件主要起草人：XXX、XXX。

本文件为首次发布。

基于区块链的海运从业人员身份管理规范

1 范围

本文件规定了基于区块链的海运从业人员身份管理的术语和定义、技术要求、基本要求。

本文件适用于基于区块链的海运从业人员身份管理。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25058 信息安全技术 网络安全等级保护实施指南

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

JR/T 0184-2020 金融分布式账本技术安全规范

JR/T 0193-2020 区块链技术金融应用 评估规则

《中华人民共和国电子签名法》

3 术语和定义

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。

注：典型的区块链是以块链结构实现数据存储的。

[来源：JR/T 0193-2020，3.1]

3.2

节点 node

提供分布式账本的所有功能或者部分功能的实体。

[来源：JR/T 0184-2020，3.22]

3.3

电子签名技术 electronic signature technology

电子签名技术是指数据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数据的技术。

3.4

共识算法 consensus algorithm

区块链系统中各节点间为达成一致采用的计算方法。

3.5

数字身份证书

由普通用户提交、身份生成机构生成的包含用户身份信息、公钥、数字签名及其他信息的身份凭证，存储于区块链中用以证明用户身份，并可授权处理相关事务。

3.6

可信执行环境 trusted execution environment

可信执行环境（TEE）通过一组硬件和软件的组合，保证各种敏感数据在其中被安全传输、存储、处理，保证执行的机密性、完整性和数据访问权限端到端的安全。

[来源：JR/T 0156－2017，5.3]

4 技术要求

4.1 共识机制

4.1.1 依据海运从业人员众多、系统多样的特点，特别设计异步等待时间共识算法（asyc-PoET）。本算法把区块链事务分成区块构造和数据提交两个异步操作，涉及一条区块构造辅链和一条数据主链，具体步骤如下：

a) 所有参与节点可随时向区块构造辅链提出预定区块请求，请求信息包含：请求者 ID、预定时间等；

b) 请求通过点对点网络协议 Gossip 广播到每一个区块协助构建节点；

c) 收到请求的区块链节点若支持使用时间等待证明机制（英特尔处理器），则通过时间等待机制算法来构造预定区块。预定区块包含：请求节点 ID、预定时间、构造时间、构造节点 ID 等相关信息。

4.1.2 事务提交节点检查自己是否在区块构造辅链上有剩余的预定区块，若有，则从预定区块中获取其所有权的信息，与提交数据一起打包成数据区块，请求其节点添加到数据主链中；若无，则须向预定区块辅链请求确定区块。

4.1.3 数据主链的其它节点接收到新的数据区块后，需检查该数据区块的合法性，验证通过后添加到该节点的数据主链上。

4.2 分布式账本

区块链中分布式数据的存储机制，通过不同节点对账本的共同记录与维护，形成区块链系统中数据的公共管理、防篡改、可信任的机制。账本记录应包括以下功能：

a) 支持持久化存储账本记录；

b) 支持多节点拥有完整的数据记录；

c） 支持向获得授权者提供真实的数据记录；
d） 确保有相同账本记录的各节点的数据一致性。

4.3 时序服务

对于区块链系统中的行为或数据需记录相应的一致性的时序，可以选择特定的时序机制或工具。区块链系统时序服务应包括以下功能：

a） 支持统一账本记录时序；
b） 支持系统实现一定程度的时序容错；
c） 保证区块时间的可信，应至少采用以下方式的一种：
- 对必要的一些区块，采用锚定可信时间等方式；
- 节点采用可信时间源；
- 其他能够提供可信时间的方法。

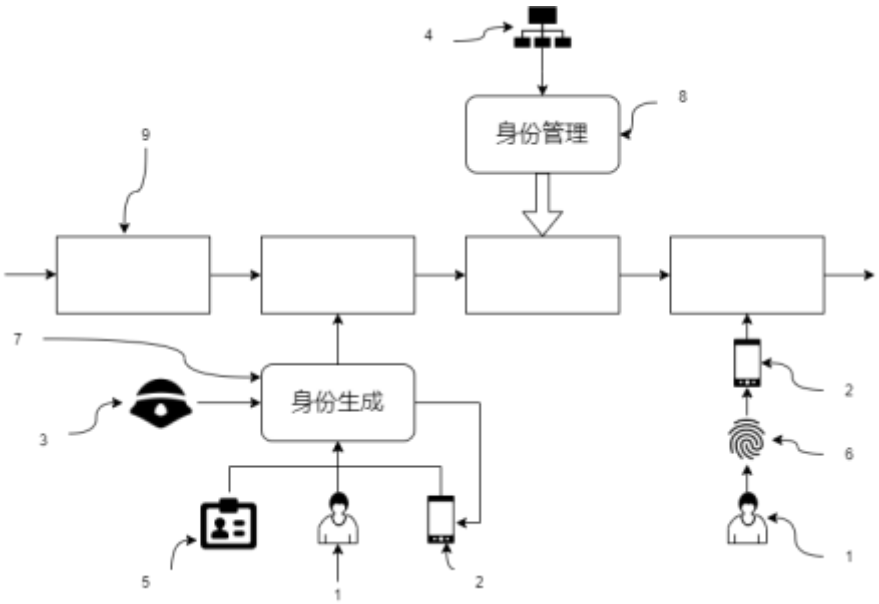
4.4 KPI 技术

PKI (Public Key Infrastructure)是基于公开密码理论建立起的安全基础设施，是电子签名的一种，在区块链系统中根据签字的数据电文进行存储、识别、认证，保证系统可靠安全性。根据《中华人民共和国电子签名法》规定，数字签名与手写签名具有同等法律效力。

5 业务流程

5.1 业务流程图

业务流程示意图如图 1 所示。



标引序号说明：

1——普通用户；2——智能手机；3——身份生成机构；4——身份管理员；5——身份证明；6——生物信息：如指纹、面容；7——数字身份生成；8——数字身份管理；9——区块链系统。

图1 基于区块链的海运从业人员身份管理示意图

5.2 参与角色

基于区块链的海运从业人员身份管理具有以下四种参与角色：

a) 普通用户（图 1 中标注 1）

普通用户为海运从业人员，是基于区块链管理系统的主要业务操作者，如：卡车司机、仓库管理员等。普通用户需要从身份生成机构（图 1 标注 3）获取能在区块链使用的身份证书。普通用户在身份管理中是不可信的。若一个事务包括多个普通用户作为参与者，应互相验证对方电子身份的合法性；

b) 智能手机（图 1 标注 2）

- 智能手机所有权和使用权属于普通用户；
- 普通用户使用智能手机与区块链交互；
- 智能手机须有可信执行环境（TEE）对私密信息进行保护，并且保证存储在 TEE 里面的区块链相关信息不可篡改。

c) 身份生成机构（图 1 标注 3）

身份生成机构是一个可信机构，如：公安部门、公司身份管理部门等，其负责为普通用户创建区块链可用的电子身份；

d) 身份管理员（图 1 标注 4）

身份管理员是由一组区块链节点组成，它们共同维护与管理所有与海运区块链身份验证相关的事务。每一个节点单独都是不可信的，但它们整体可以作为区块链身份验证的可信管理员。

5.3 数字身份的生成与上链

5.3.1 普通用户准备可验证的身份证明：如身份证、驾驶证、公司工作证等，和具备生物信息检测的智能手机。

5.3.2 海运从业人员区块链身份生成流程：

a) 普通用户把身份证明发送给身份生成机构；

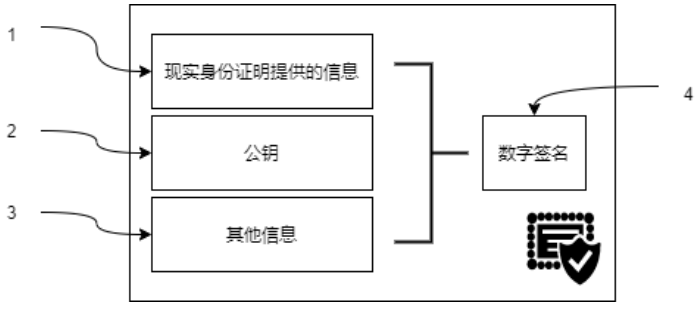
b) 身份生成机构检查：

1) cdt_1：身份证明的合法性；

2) cdt_2：身份证明和普通用户的匹配程度，确认是否本人。

c) 若 cdt_1 与 cdt_2均为真，普通用户把具备生物信息检测的智能手机提供给身份生成机构并用生物信息解锁智能手机，身份生成机构和智能手机使用 KEYGEN 算法产生公钥和私钥。私钥保存在智能手机的 TEE 环境里，不可篡改。身份生成机构从身份证明里获取与普通用户相关的身份信息:如性别、年龄、岗位等，从而创建包含公钥和身份信息的身份证书。

5.3.3 身份证书被提交并储存在区块链；身份证书的结构见图 2。



标引序号说明：

1——普通用户现实身份证明（如身份证、驾驶证、工作证等）提供的信息（如姓名、性别、岗位等；

2——KEYGEN算法产生的公钥pk；

3——其它信息，如使用的加密算法，ph及TEE的版本等；

4——普通用户创建身份证书的数字签名。

图2　身份证书（cert）的结构示意图

5.4　数字身份的使用

普通用户需要智能手机来使用其区块链身份。具体步骤如下：

a)　普通用户从区块链获取需要验证身份的事务；

b)　普通用户确认事务，并使用其区块链身份授权事务，普通用户使用生物信息解锁智能手机,并用私钥对事务进行电子签名；

c)　普通用户将签名后的事务提交到区块链；

d)　其它区块链用户收到签名后的事务，在区块链找到对应普通用户的身份证书，验证私钥和公钥是否匹配。根据共识算法，若成功匹配，签名后的事务将被添加到区块链。

5.5　数字身份管理

数字身份管理由一组区块链管理节点组成，数字身份管理操作包括增加和删除区块链身份。

a)　增加区块链身份

新生成的身份证书被提交的区块链，管理节点通过共识算法决定身份证书里的身份信息是否合法，合法的身份证书被储存在区块链中。

b)　删除区块链身份

普通用户丢失了其私钥，可以提交注销其身份证书的申请，该申请应由一个或多个管理节点背书，身份证书注销后，普通用户将不能使用旧的私钥来授权区块链事务，必须重新申请新的身份证书。

6　基本要求

6.1　架构标准要求

基于区块链的海运从业人员身份管理系统架构包括用户交互层、业务层、数据传输层、Web服务层、区块链层五个部分，如图3 所示。

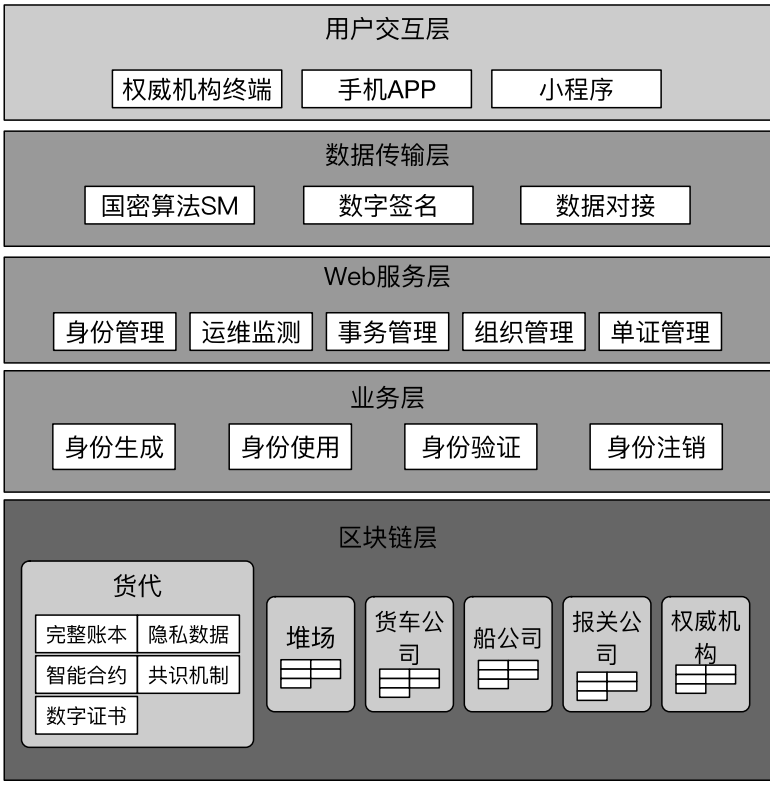


图3 基于区块链的海运从业人员身份管理系统架构

6.2 用户交互层

用户交互层为手机客户端（APP或者小程序）及权威机构的业务系统。权威机构的业务系统主要功能是生成机构背书的区块链身份数字证书。客户端或业务系统通过数据传输层与Web服务层提供的服务接口相连接。

6.2.1 交互层安全要求

由于区块链海运从业人员身份涉及到生物信息等隐私，交互层的客户端必须具备可信执行环境TEE，并符合中国人民银行金融行业标准《移动终端支付颗心环境技术规范》（JR/T 0156-2017）及相关规范要求。

6.3 数据传输层

信息传输应采用符合国家密码行业标准《SSL VPN 技术规范》（GM/T0024-2014）里定义的国密 SSL 协议进行 HTTPS 通信。签名算法使用 SM2（GM/T0003.2）。

6.4 Web 服务层

Web 服务层为用户交互层提供服务 API 接口，采用表述性状态转换机制（REST）。

6.4.1 接口要求

同步消息对接方式为标准RESTful网络服务接口，返回值应为JSON报文。同时传输过程应遵循6.3数据传输层涉及的国密SSL协议。异步消息对接可使用常用的消息队列协议，如Kafka等。须注意消息队列的当前容量，避免消息在中间件中产生堆积。

6.5 业务层

业务层由智能合约实现，智能合约包含身份数据交换规则和流程。这些规则和流程满足一定条件（如用户发起身份验证请求时），被计算机系统自动执行。业务层主要包括身份生成、使用、验证及注销四个功能模块。智能合约必须具备审核、部署、升级、日志分析、版本管理等功能。每一次对智能合约的更改都必须由区块链参与各方联合审核。

6.6 区块链层

区块链层应满足以下数据交换特性：

6.6.1 实用性

数据共享应科学合理，满足数据使用方的应用需求。

6.6.2 统一性

同一数据分享方式应统一，公共数据的代码应参考国家相关标准。

6.6.3 可扩展性

数据共享设计时应充分考虑数据范围扩充、时间增量等问题。

6.6.4 完整性

数据分享应充分保留数据原始信息，不做主观删减等特殊化处理。

6.7 硬件要求

区块链运行的硬件设备包括内存、硬盘等必须可扩展，避免因数据吞吐量增大而无法同步账本。

6.8 拓展性要求

考虑数据规模增长与大数据分析的需求，区块链建议采用云计算横向扩展的架构来实现。

6.9 性能要求

区块链的业务吞吐量需在极端条件下仍然能正常工作，所选用平台必须有不低于5000TPS的处理性能。

6.10 存储要求

应满足《中华人民共和国数据安全法》及相关国际数据法律法规等要求。

6.11 安全要求

6.11.1 系统安全应符合 GB/T 22239、GB/T 25058、GB/T 25070 的规定。
6.11.2 密码应用应符合 GB/T 39786 的规定。
6.11.3 数据交换安全应符合 GB/T 39477 的规定。
6.11.4 个人信息安全应符合 GB/T 35273 的规定。

参 考 文 献

[1] GB/T 5271.18 信息技术 词汇 第18部分:分布式数据处理
[2] GB/T 20520 信息安全技术 公钥基础设施 时间戳规范
[3] GA/T 756 法庭科学 电子数据收集提取技术规范
[4] DB52/T 1466-2019 区块链 应用指南
[5] DB43/T 1842-2020 区块链应用安全技术测评标准
[6] 《中华人民共和国网络安全法》