ICS 号 03.060
中国标准文献分类号 A11

团 体 标 准

T/HBPFS 001. 4-2022

雄安新区区块链支付平台
第 4 部分：安全与隐私规范

The Standard of Xiong'An New Area Blockchain Payment Platform

Part 4：Information Security and Privacy Specification

2022-12-27 发布　　2022-12-27 实施

河北省金融学会　　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。区块链支付信息服务是以区块链与智能合约技术为核心，通过业务流程触发形成支付指令，并对接银行支付网关实现资金支付的一种创新性区块链应用。前期，为解决工程建设资金管理场景中从业主体多、业务流程复杂、资金流向监管难等问题，雄安新区已基于上述区块链支付信息服务模式研发应用了工程建设资金管理区块链平台，实现了工程建设资金从业主到总、分包单位的及时、准确与高效拨付，具备按需支付、可信支付、穿透支付和无损支付等特点。根据区块链支付信息服务模式与特点，我们认为该模式亦可在政府资金监管、多级供应链等多个复杂企业支付场景进行应用，具备较好复制与推广应用前景。

为促进雄安新区区块链+支付模式应用，便于政府、银行和企业各方接入区块链支付平台并规范相关接入规范与接口要求，特制定《雄安新区区块链支付平台》。本标准由以下 6 部分构成：

——第 1 部分：参考模型及流程规范，总体阐述区块链支付定义、业务参考模型、技术架构和主要功能介绍；

——第 2 部分：银行接入规范，重点阐述银行接入区块链支付平台的接入方法与接口规范；

——第 3 部分：场景开发与接入规范，重点阐述客户通过开放场景接入区块链支付平台的方法与接口规范；

——第 4 部分：安全与隐私规范，重点阐述区块链支付基础安全规范、数据安全与隐私规范等内容；

——第 5 部分：数据服务规范，重点阐述区块链支付平台提供数据服务的方式、内容；

——第 6 部分：管理规范，重点阐述区块链支付平台基础管理、银行与客户准入、交易安全与管理等基础管理规范。

本文件为该标准的第 4 部分

本文件负责起草单位：中国人民银行雄安新区营业管理部、雄安新区区块链实验室、中国工商银行股份有限公司河北雄安分行、中国农业银行股份有限公司河北雄安分行、中国银行股份有限公司河北雄安分行、中国建设银行股份有限公司河北雄安分行、中信银行股份有限公司河北雄安分行、中国农业银行总行研发中心金融科技创新中心

本文件主要起草人：孟宏伟、赵天奕、高远、焦欣欣、王蒙、左爵希、宋正罡、穆文涛、唐上淳、李亚科、王桐、楚会永、耿浩杰、康宁、胡园园、杨耀华、刘兰真、王婷婷

引　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。区块链支付信息服务是以区块链与智能合约技术为核心，通过业务流程触发形成支付指令，并对接银行支付网关实现资金支付的一种创新性区块链应用。前期，为解决工程建设资金管理场景中从业主体多、业务流程复杂、资金流向监管难等问题，雄安新区已基于上述区块链支付信息服务模式研发应用了工程建设资金管理区块链平台，实现了工程建设资金从业主到总、分包单位的及时、准确与高效拨付，具备按需支付、可信支付、穿透支付和无损支付等特点。根据区块链支付信息服务模式与特点，我们认为该模式亦可在政府资金监管、多级供应链等多个复杂企业支付场景进行应用，具备较好复制与推广应用前景。

为促进雄安新区区块链+支付模式应用，便于政府、银行和企业各方接入区块链支付平台并规范相关接入规范与接口要求，特制定《第 4 部分：安全与隐私规范》。

本文件规定了雄安区块链支付信息服务安全与隐私规范包含的基本要求，包括术语与定义、平台基础安全规范、平台数据安全与隐私规范等内容，主要面向使用区块链支付信息服务信息服务平台的企业技术与管理人员和接入银行的技术与管理人员等。

雄安新区区块链支付平台
第 4 部分：安全与隐私规范

1 范围

本文件规定了雄安区块链支付信息服务安全与隐私规范包含的基本要求，包括术语与定义、平台基础安全规范（主要涵盖从客户端、通讯网络、服务端的基础安全要求和区块链安全性保障等内容）、平台数据安全与隐私规范等内容，主要面向使用区块链支付平台的企业技术人员、管理人员和接入银行的技术与管理人员等。

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 25069 信息安全技术术语

JR/T 0184-2020 金融分布式账本技术安全规范

JT/T 0068-2020 网上银行系统信息安全通用规范

3 术语和定义

3.1 区块链

区块链是一种不可篡改的分布式账本。

3.2 区块链支付信息服务

依托区块链技术，由业务流程触发的自动支付模式，是复杂场景下的有条件支付。满足对合规性、安全性、及时性、穿透性、协同性等有较高要求支付场景。

3.3 智能合约

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。[JR/T 0184-2020，定义 3.20]

3.4 区块链支付信息服务平台/系统

是以区块链支付信息服务和智能合约技术为基础，通过连接第三方银行的账户与支付系统，根据客户在复杂场景的支付需求，由业务流程自动触发支付的平台或信息管理系统。

3.5 访问控制

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。[GB/T 25069—2010，定义 2.2.1.42]

3.6 隐私保护

为保护隐私而采取的措施。例如：对个人数据的收集、处理和使用加以限制。[JR/T 0184-2020，定义 3.12]

3.7 隐私信息

特定自然人的标识信息及其在特定系统中的活动信息。[JR/T 0184-2020，定义 3.41]

3.8 区块链证书

全称为“区块链项目价值认证证书”，由中国区块链价值评价中心、区块链网电子标识发布平台推出的第三方网站真实身份认证服务，它通过对区块链项目的白皮书、域名、网站、备案信息、工商登记或组织机构信息进行严格交互审核来验证区块链项目的真实价值。

4 区块链支付信息服务平台客户端安全

4.1 客户端程序

本节所描述的客户端包括以独立程序形式存在的 PC、移动客户端，也包括借助浏览器或其他应用与区块链支付信息服务平台系统进行交互的插件、软件等形式。

- 客户端程序应对客户输入的敏感信息进行加密，例如采取随机键位软键盘等措施。
- 客户端程序应对输入字符的合法性进行判别并过滤非法字符。
- 客户端程序在一段时间内无任何操作，应自动断开连接。
- 客户端程序的临时文件中不应出现敏感信息，临时文件包括但不限于 Cookies、本地临时文件和移动数据库文件等。
- 客户端程序应防范键盘窃听敏感信息，例如防范采用挂钩 Windows 键盘消息等方式进行键盘窃听。

4.2 客户端环境

- 应提示客户安装杀毒软件等基本防护措施，提升客户端环境安全。
- 当发现客户端环境存在重大安全缺陷或安全威胁时，应通过短信、邮件等方式警示客户。

5 通信网络安全

5.1 通讯协议

本部分内容指数据在网络传输过程中采用的通讯协议和安全认证方式，不包括网络基础设施方面的内容。

- 应使用强壮的加密算法和安全协议保护客户端与服务器之间连接安全。
- 应使用安全加密算法，并使用安全的密钥长度。
- 根据数据传输的安全要求，使用安全的算法组合。
- 整个通讯期间，经过认证的通讯线路应一直保持安全连接状态。

5.2 通信链路

区块链支付信息服务平台应使用强壮的加密算法和安全协议保护客户端与服务器之间、外部机构与服务器之间所有连接，保证传输安全、报文完整性验证、数据加密传输、安全协议和算法以及不可抵赖性等。

- 区块链支付信息服务平台客户端和服务端之间的通讯，若通信数据中包含敏感信息则必须保证敏感信息被加密，禁止出现敏感信息明文。
- 客户端和服务端之间的通讯如经过第三方服务器时，应建立服务端和客户端之间的安全通道。

6 服务器端安全

服务器端安全主要包括网络安全、身份鉴别、访问控制、安全审计、入侵防范、Web应用安全、数据库安全与备份等通用服务器安全保障内容。本标准中涉及服务器端安全内容及与外部系统连接安全参照JT/T 0068-2020 6.2.4、6.2.5内容执行。

7 区块链安全性保障

区块链是一种基于密码学综合运用的去中心化信任解决工具，也是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。区块链系统构建的基本安全目标是通过密码学和网络安全等技术手段,保护区块链系统中的数据安全、共识安全、隐私保护、智能合约安全和内容安全。区块链安全性保障属于服务端安全保障的范围，鉴于区块链在系统中的特殊位置，除正常服务器端安全保障要求外，区块链安全性还有一些特殊要求。

- 区块链系统数据的安全性与隐私保障：块链系统应有访问控制能力，对访问用户进行身份认证与权限约束；区块链系统应能保证存储数据的完整性、不可抵赖性，能够识别或抵抗少数作恶节点对账本数据的篡改；区块链系统应保证用户敏感数据即使在账本节点服务器被攻破的情况下，也能在一定程度上保证获取者不能直接或完全获取用户敏感信息。
- 区块链系统的业务连续性：区块链系统应能在部分节点故障的情况下保持正常对外提供服务的能力；区块链系统应能支持故障节点回复后，重新接入系统并保持账本一致性。
- 区块链渠道接入安全：各银行应用与区块链节点的安全连接采用SSL（Security Socket Layer）协议，实行TLS双向认证；各应用接入方与对应区块链节点需要生成各自的tls证书，并通过安全渠道完成证书交换；接入方与区块链节点通讯时，需要通过双方证书验证，确定接入方身份，与区块链节点登录用户一致方可进行通讯。
- 区块链访问控制安全：区块链节点均有明确所属方，配有对应的用户。区块链CA节点维护与管理用户对于智能合约的读写权限，只有拥有权限的用户才能够执行智能合约的部署、读取和写入；智能合约内部对用户的业务权限也进行了控制，银行只能对与本行相关的支付指令进行查询与操作。
- 区块链数据存储安全：区块链中账本数据以密文方式存储；当区块链节点发送交易时，交易随共识在区块链网络的各个节点之间广播，共识完成后，各个记账节点执行该交易；在智能合约的执行过程中，通过交易用户中读出本次交易对通道的读写权限；合约内部调用插入和读取函数，入参中指定需要操作的通道，记账节点校验通道操作权限成功，则根据要操作的通道ID以ECDH算法与CA协商生成密钥，进行加密存取。

- 区块链账户信息安全：区块链账户信息（即公私钥信息）一般持有在用户或调用方手中，在需要序列化存储时，可以通过增加不同可选择的对称加密算法如DES、3DES、AES等，并通过用户提供的自定义密钥进行加密存储，为用户侧的序列化存储提供安全支持。
- 区块链智能合约安全：根据智能合约的整个生命周期运作流程,智能合约安全可以被划分为编写安全和运行安全两部分。编写安全：智能合约开发人员在编写智能合约之前,需要根据实际功能设计完善的合约文本,避免由合约文本错误导致智能合约执行异常甚至出现死锁等情况。运行安全：指智能合约在执行过程中一旦出现漏洞甚至被攻击,不会对节点本地系统设备造成影响,也不会使调用该合约的其他合约或程序执行异常。
- 区块链内容安全：内容安全是在数据安全的基础上衍生出来的应用层安全属性,要求区块链上传播和存储的数据内容符合道德规范和法律要求,防止不良或非法内容在区块链网络中传播,保证区块链网络中信息的纯净度。内容安全的保障重点是加强区块链中信息在传播和存储过程中的控制和管理。

8 区块链支付信息服务平台隐私规范

8.1 隐私保护策略

区块链支付信息服务平台在隐私保护原则、内容、策略、技术要求和监控与审计等方面的安全规范。本标准中所涉及的隐私信息是指在区块链支付信息服务平台系统中，单独或者与其他信息相结合能识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括但不限于各方的账户信息、鉴别信息、交易信息、合同信息、项目信息及支付附件信息等。

- 信息公开可验证：公开交易内容信息以及交易方信息；应对交易方身份信息进行标识和鉴别；应确保交易方无法被冒用；公开的信息应确保任何人能进行有效性和正确性的验证。
- 信息加密可验证：应对交易内容信息以及交易方信息至少其一进行加密；应确保参与方以及审计方拥有对加密信息解密验证的能力；应确保交易方无法被冒用；应确保除交易参与方外他人无法伪造加密信息。
- 信息由交易验证节点验证：应对交易内容信息以及交易方信息至少其一进行加密；应确保参与方、交易验证节点以及审计方拥有对加密信息解密验证的能力；应由交易验证节点负责对信息进行解密验证，以对其有效性和正确性进行验证。交易验证节点承担；他人应通过交易验证节点的验证信息对交易的有效性和正确性进行验证。

8.2 隐私保护技术要求

隐私保护技术和方法包括认证授权、局部广播、摘要存储、变更标识、混淆技术以及零知识证明、群签名、环签名、同态加密等算法组合，可根据业务场景组合解决方案，实现信息保密性和隐私保护的目的。隐私保护技术具体要求参照JR/T 0184-2020 14.4执行。