ICS 35.240

CCS L70

团 体 标 准

T/SCBA 003—2023

区块链用户密钥管理规范

Specification for User Key Management of Blockchain

2023-07-01 发布 2023-07-20 实施

四川省区块链行业协会 发布

目　录

前　言

本标准按照 GB/T 1.1—2020 给出的规则起草。

本标准由四川省区块链行业协会标准化技术委员会提出并归口。

本标准起草单位：四川领链科技有限公司、豪符密码检测技术(成都)有限责任公司、嘉凯宇拓（成都）科技有限公司、四川省数字证书认证管理中心有限公司、成都壹石新科信息技术有限公司、四川省乡发数字科技有限公司、微众银行、四川长虹电子控股集团有限公司、云南南天电子信息产业股份有限公司。

本标准主要起草人：肖自信、徐顺斌、安红章、杨伟、邓力涵、吴华、尹才敏、支红杰、张晨曦、唐兴、张开翔、胡章一、左川民。

区块链用户密钥管理规范

1 范围

本文件规定了区块链服务平台的用户密钥管理规范，包括终端密钥管理、实名身份绑定和密钥托管服务三个方面的要求。

本规范适用于指导区块链用户端，以及区块链应用系统或第三方密钥托管服务的密钥管理方案的设计与实现。

2 规范性引用文件

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

GB/T 37092-2018 信息安全技术 密码模块安全技术要求；

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求；

GB/T 25069-2010 信息安全技术 术语；

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求；

GB/T 35273-2020 信息安全技术 个人信息安全规范；

GB/T 25058 信息安全技术信息系统安全等级保护实施指南；

GB/T 25070 信息安全技术信息系统等级保护安全设计技术要求；

GB/T 38561—2020 信息安全技术 网络安全管理支撑系统技术要求；

GM／T 0111-2021 区块链密码应用技术要求；

3 术语和定义

GM／T 0111-2021、GB/T 25069-2010、GB/T 39786-2021 界定的以及下术语和定义适用于本文件。

3.1

区块链 blockchain

一种采用分布式数据存储、点对点传输、共识机制、密码算法、智能合约等技术的新型应用模式和融合技术。

3.2

区块链服务平台 blockchain platform

在区块链上对外提供上链存证、查询验证等服务的信息系统或软件。

3.3

交易 transaction

数字资产的一次转账或者对智能合约的一次调用。

3.4

合规性 compliance

系统、产品或组件中采用的密码算法、密码技术、密码产品、密码服务及密钥管理符合法律法规和密码相关国家标准和行业标准的要求。

3.5

密钥 key

控制密码算法运算的关键信息或参数。

3.6

公钥 public key

非对称密钥对中可以公开的密钥。

3.7

私钥 private key

非对称密钥对中只能由用户使用的不公开密钥。

3.8

加密密钥 encryption key

对密钥进行加密保护的密钥。

3.9

数字资产 digital assets

以电子数据形式存在，持有者可以出售或者交换的有价资产。

3.10

智能合约 smart contract

一套以数字形式定义的约定。

3.11

密钥托管 key hosting

以签署协议的方式将密钥托管给第三方可信服务厂商管理，并授权密钥相关的操作权限。

4 缩写语

下列缩略语适用于本文件。

CA（Certificate Authority）

证书认证机构

5 密钥应用架构

区块链用户密钥应用架构如下图所示，主要包括用户终端密钥管理和密钥托管服务两种应用模式，以及实名身份绑定应用要求。

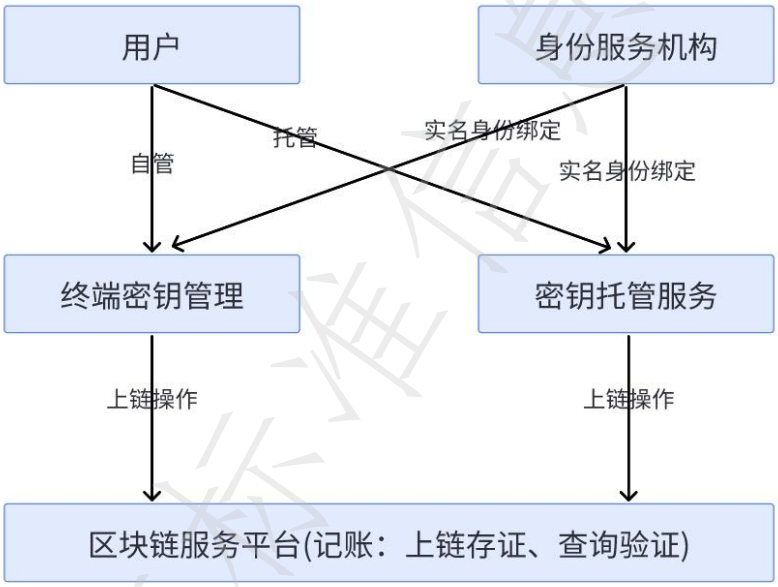

图 1 区块链用户密钥应用架构

a) 终端密钥管理：用户通过密码终端自行进行密钥管理，并为密钥管理承担全部责任。

b) 密钥托管服务：用户委托第三方进行密钥管理，通过协议方式将密钥管理的权利与责任委托给第三方，以获取统一的密钥管理服务。

c) 实名身份绑定：依托可信身份服务机构对用户进行实名身份鉴别，并通过数字证书等方式将用户公钥与实名身份进行绑定。

6 终端密钥管理

主要规范用户密码终端的密钥生成、存储、应用、生命终止等相关要求。

6.1 密码载体

a) 用户终端密钥管理须依托密码模块进行；

b) 密码模块须通过《GB/T 37092-2018 信息安全技术 密码模块安全技术要求》2 级以上测评。

6.2 密钥生成与存储

a) 用户公私钥对应在密码模块中生成及安全存储；

b) 用户私钥不得以任何明文或密文形式暴露于密码模块安全区域以外的任何地方。

6.3 密钥应用

a) 应实施密钥授权访问，调取使用密钥前应对用户进行身份鉴别；

b) 密钥应用所涉及密码协议应通过安全证明；

c) 对关键密钥应用操作应进行可靠记录，支持审计。

6.4 密钥生命终止

a) 应使用密码模块生命终止流程清理或销毁密码模块内的敏感信息（如敏感安全参数、用户数据等）；

b) 在密钥清理或销毁前，应确认由此密钥保护的数据信息不再需要。

7 实名身份绑定

主要规范身份服务机构为用户提供实名身份绑定服务，及区块链平台进行实名身份验证的相关要求。

7.1 身份服务机构

a) 应为国家授权的身份服务机构（如 CA 机构）；

b) 资质在有效期内；

c) 具有相应服务能力；

d) 应在区块链平台进行登记。

7.2 身份绑定方式

a) 通过签发数字证书的方式将用户实名身份与用户公钥进行绑定；

b) 绑定前应鉴别用户身份，鉴别方式应满足《GB/T 38561—2020 信息安全技术 网络安全管理支撑系统技术要求》有关要求；

c) 绑定后应将有关身份信息上链存储，上链信息应包括数字证书编号、发证机构、用户区块链公钥信息；

d) 使用身份绑定合约需要验证发证机构签名。若发证机构不能直接与区块链服务平台或智能合约进行交互，应提供签名后的消息转交用户或者托管机构代为上链。

7.3 实名身份验证

a) 区块链平台应支持通过提供标准智能合约查询用户身份绑定、记录、绑定日志等信息；

b) 区块链平台智能合约在接收交易申请时应确认用户是否拥有合法身份证书。

8 密钥托管服务

主要规范密钥托管服务在服务主体、服务内容、服务系统、服务安全及监管审计方面的要求。

8.1 服务主体

密钥托管服务可以为以下类型主体：

a) 专门的第三方托管服务机构；

b) 由应用系统厂商提供密钥托管服务。

8.2 服务内容

密钥托管服务应支持以下对象托管：

a) 用户密钥托管：用户密钥包括公钥、私钥等，代理用户进行密钥有关操作；

b) 用户数字资产托管：与用户密钥关联的数字资产，代理用户进行数字资产的保管、交易等操作。

8.3 服务系统

a) 密钥托管系统的密钥管理应遵从本标准第 6 部分终端密钥管理所有要求；

b) 密钥托管系统的密钥管理应遵从本标准第 7 部分实名身份绑定所有要求；

c) 密钥托管系统应通过信息安全等级保护 3 级测评和商用密码应用安全性评估；

d) 密钥托管系统应通过商用密码产品检测认证。

8.4 服务安全

a) 密钥托管机构应取得国家密码管理局要求的有关资质；

b) 应与用户签订服务协议，明确服务内容及相关安全责任界定；

c) 为用户提供服务时，应进行用户实名身份验证；

d) 应具有专职运维团队，确保服务 7*24 小时正常运作；

e) 应具有数据、系统备份等措施，确保用户资产安全性与可用性；

f) 应具有用户资产密钥更新等应急处理措施；

g) 应具有用户身份鉴别、自主访问控制、用户数据保护、恶意代码防范等技术能力。

8.5 监管审计要求

a) 应对用户所有操作进行详细日志记录；

b) 密钥托管系统涉及提供区块链信息服务的，应通过国家互联网信息办公室区块链信息服务备案。

参 考 文 献

[1] GMT 0028-2014 密码模块安全技术要求

[2] GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

[3] GB/T 38561—2020 信息安全技术 网络安全管理支撑系统技术要求

[4] GB/T 25069-2010 信息安全技术

[5] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[6] GB/T 25058信息安全技术信息系统安全等级保护实施指南；

[7] GB/T 25070信息安全技术信息系统等级保护安全设计技术要求

[8] GB/T 25069-2010 信息安全技术 术语

[9] GB/T 35273-2017 信息安全技术 个人信息安全规范

[10] GM／T 0111-2021 区块链密码应用技术要求

[11]中华人民共和国工业和信息化部. 中国区块链技术和应用发展白皮书，2016

[12]中共中央网络安全和信息化委员会办公室. 区块链信息服务管理规范，2018

[13]中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书，2018

[14]国家互联网信息办公室. 区块链信息服务管理规定，2019

[15] T/SCBA 001—2022 可信区块链应用服务评价规范

[16] T/SCBA 002—2022 可信区块链平台服务等级评价规范