

ICS 35.240.99

CCS L 67

SZSD

数 字 山 东 地 方 标 准

SZSD02 0013—2024

数字身份——基于区块链的去中心化标识 (DID) 技术要求

Digital Identity —— Blockchain-based Decentralized Identifiers Technical
Requirements

2024 - 04 - 15 发布

2024 - 06 - 01 实施

青岛市大数据发展管理局 发 布

目 次

前言 2

1 范围 3

2 规范性引用文件 3

3 术语和定义 3

4 缩略语 5

5 设计原则 5

 5.1 去中心化 5

 5.2 直接控制 5

 5.3 隐私安全 6

 5.4 加密交互 6

 5.5 互操作性 6

 5.6 可移植性 6

 5.7 简易性 6

6 DID 标识符..... 6

 6.1 基于区块链的 DID 标识符 5

 6.2 DID 主体..... 5

 6.3 DID 持有方..... 5

7 DID 方法..... 6

8 DID 数据模型..... 6

9 DID 生成..... 7

10 DID 验证..... 7

11 DID 解析..... 7

12 隐私安全 7

参 考 文 献 8

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这些专利的责任。

本文件由青岛市大数据发展管理局提出并归口。

本文件起草单位：北京泰尔英福科技有限公司、青岛科技大学

本文件主要起草人：艾崧溥、孙丽琚

数字身份——基于区块链的去中心化标识（DID）技术要求

1 范围

本文件规定了数字身份中基于区块链的去中心化标识的设计原则、DID 标识符、DID 方法、DID 数据模型、DID 生成、DID 验证、DID 解析，以及隐私安全的要求。

本文件适用于作为区块链服务的去中心化标识的设计、建设及应用活动。

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 15843.2-2017 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制
GB/T 15843.3-2016 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制
GB/T 15843.4-2008 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制
GB/T 15843.5-2005 信息技术 安全技术 实体鉴别 第5部分：采用零知识鉴别的机制
GB/T 25069-2022 信息安全技术 术语
GB/T 36651-2018 信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架
GB/T 39786-2021 信息安全技术信息系统密码应用基本要求

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

用户 user

使用基于区块链的去中心化标识符的主体。

注：申请方、声称方、持有方代表了用户在不同场景下的不同角色。

[来源：GB/T 25069—2022，3.733，有修改]

3.2

持有方 holder

已获得 DID 的用户。

3.3

申请方 applicant

请求成为持有方的主体，可对其进行身份核验。

3.4

声称方 claimant

被鉴别的 DID 持有方或者是代表持有方的主体。

注：声称方拥有其代表用户从事鉴别交换时所必须的功能和私有数据。

[来源：GB/T 25069—2022，3.535，有修改]

3.5

去中心化标识符 decentralized identifier, DID

一组与用户关联属性，全局唯一的标识符，通过分布式注册的方式，为实体社会中的用户身份提供数字空间的映射。DID 可以分为基础层和应用层两个层次。基础层是 DID 的规范，包括 DID 标识符号和 DID 文档；应用层主要是可验证凭证。

3.6

DID 文档 DID document

存储在区块链上，包含DID、公钥信息，以及DID持有者的其他属性的描述性文档。

[来源：W3C Decentralized Identifiers，2，有修改]

3.7

可验证凭证 verifiable credential

一种数字文档，文档以键值对的结构对某个实体的属性做出系列声明，并采用密码技术实现可验证。

[来源：W3C Verifiable Credentials Data Model，2，有修改]

3.8

可验证表达 verifiable presentation

由多个可验证凭证组合得到，其所有权可以通过密码技术验证。

[来源：W3C Verifiable Credentials Data Model，2，有修改]

3.9

声明 claim

不带证明的关于实体的数字断言。

[来源：ITU-T X.1252，6.19，有修改]

3.10

数字身份 digital identity

主体在线上交易场景中的表示，通常由标识符、可验证凭证、可验证表达共同标识其唯一性。

[来源：NIST SP 800-63，4.1，有修改]

3.11

依赖方 relay party

依赖数字身份验证结果以确定是否为用户建立信任关系的参与方。

3.12

基础级数字身份提供方 relay party

为用户颁发与其所持有的国家法定身份证件关联对应的数字身份的权威可信机构。

3.13

业务级数字身份提供方 relay party

为用户在各类业务活动中获得的属性提供数字化证明材料的机构。

3.14

数字钱包 digital wallet

装载在用户设备上的一种应用，以存储对应私钥的方式实现用户对数字身份标识符和凭证的控制权。

[来源：ITU-T X.1252, 6.98]

3.15

可信环境 trusted environment

用户设备上的安全区域，可保证加载到其内部数据的安全性，包括保密性、完整性和可用性等，如可信执行环境（TEE）、安全元件（SE）、可信密码模块（TCM）或其他具备安全边界的保护区域。

[来源：GB/T 36651-2018, 3.1]

4 缩略语

下列缩略语适用于本文件。

DID	数字身份标识符	Digital Identity Identifier
DID文档	数字身份标识符文档	Digital Identity Identifier Document
VC	可验证凭证	Verifiable Credential
VP	可验证表达	Verifiable Presentation

5 设计原则

5.1 去中心化

基于区块链的DID采取分布式管理原则，减少DID注册信息和服务的集中控制，避免对中心机构或单点故障的依赖性。

5.2 直接控制

持有方直接控制其DID，无需依赖外部机构的介入。

5.3 隐私安全

用户具备控制其信息隐私的能力，确保其他主体可依据DID文档与持有者获得所需的安全保证级别的交互。

5.4 加密交互

DID持有方在与其他主体交互时进行加密交互。

5.5 互操作性

DID基础设施可利用具备互操作性的软件工具和库

5.6 可移植性

DID独立于系统和网络，持有方能在任何支持DID和DID方法的系统中使用其DID。

5.7 简易性

DID设计支持简易操作组件功能，易于理解、实施和部署。

6 DID 标识符

6.1 基于区块链的 DID 标识符

DID标识符由DID申请方创建并由持有方控制，能够代表DID主体并解析为描述DID主体的DID文档。

区块链作为泛在数据注册中心，DID的申请方通过使用公钥在区块链上创建DID；DID声称方通过使用与该DID公钥对应的私钥证实其身份并使用区块链管理其DID文档，执行更新DID文档操作。

6.2 DID 主体

DID的主体由DID确定并由DID文件描述。DID主体的DID以DID文档中的ID属性表示，ID的值符合DID语法规则的字符串，且存在于DID文档的数据模型的根映射中。

6.3 DID 持有方

DID持有方具备通过区块链对DID文档更新的能力。DID方法规定DID持有方的具体授权过程。

持有方在DID文档中的值是一个字符串或一组符合DID语法规则的字符串。其DID文档包含明确允许为特定目的使用特定验证方法的验证关系。

7 DID 方法

DID方法符合以下技术要求：

- a) 规定授权及执行的操作过程及方法，包括加密过程；
- b) 规定 DID 控制器创建 DID 及其关联的 DID 文档的过程及方法；
- c) 规定 DID 解析器解析 DID 文档的过程及方法，包括 DID 解析器如何验证响应的真实性；
- d) 规定 DID 文档更新的条件以及 DID 控制人更新 DID 文档的方法，或声明无法进行更新的办法；
- e) 规定 DID 持有方声明 DID 停用条件及方法，或说明不可停用。

8 DID 数据模型

DID数据模型应提供DID文档和DID文档数据结构。DID文档应与DID标识符形成键值对，描述引导与标识实体进行加密验证交互所必需的公钥、身份验证协议和服务端点，如图1所示。

DID文档数据模型中的所有键值对应为序列化的字符串。

DID数据模型可定义其他的扩展机制，扩展机制支持无损转换到任何其他一致性表示。

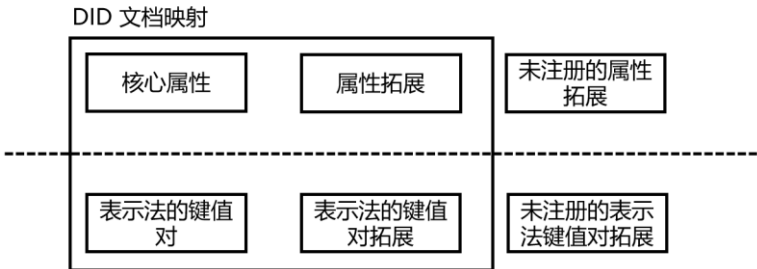


图 1 DID 数据模型图

9 DID 生成

DID标识符的生成由其对应的DID方法定义的创建过程。DID和DID文档宜通过将加密资料转化为符合要求而生成的序列表示。DID方法可使用基于区块链的可验证的数据注册表。

10 DID 验证

DID文档可定义验证方法，每个验证方法宜用一个映射来表示。

加密公钥可用于验证或授权与DID主体或关联方的交互，包括但不限于以下验证技术要求：

- a) 根据标识符在区块链中查询到该 DID 对应的 DID 文档；
- b) 从 DID 文档中选定一个或者多个身份验证方法，形成并发送身份验证消息；。
- c) 依据身份验证方法对用户开展身份验证的过程应符合相应验证协议的要求，包括但不限于 GB/T 15843.2-2017、GB/T 15843.3-2015、GB/T 15843.4-2008、GB/T 15843.5-2005、GB/T 36651-2018；
- d) 依据选定的身份验证方法对应的公私钥对、密码算法等，验证响应消息，并回复验证结果。

11 DID 解析

DID解析宜通过DID解析函数使用区块链将一个DID解析为一个DID文档。

DID解析应定义从DID解析到DID文档的输入和输出。定义一个通用解析器的功能：至少实现一个标准解析功能，并且必须能够以至少一个标准方式返回标准解析文档。使用DID方法中的“读取”操作，通过DID解析函数将一个DID解析为一个DID文档。

12 隐私安全

基于区块链的DID宜符合以下安全技术要求：

- a) 保证 DID 标识符的全局唯一性；
- b) 保证所管理的 DID 文档、数据注册表的完整性和不可篡改性；
- c) 通过访问控制保证只有持有方或经持有方授权方可以访问身份数据；

- d) 支持用户访问 DID 文档；
- e) DID 生成系统应符合等保及相关法律法规要求，应至少遵循 GB/T 39786-2021 中三级及以上密码应用要求；
- f) 支持 DID 文档的生命周期管理（产生、更新、失效等）；
- g) 采用密码技术保证交互过程数据来源的真实性、数据的完整性；
- h) 采用密码技术保证交互过程重要数据的机密性。

参 考 文 献

- [1] W3C 去中心化标识符（DID）v1.0（Decentralized Identifiers (DIDs) v1.0）
-