ICS 35.240
CCS L 67

团　　体　　标　　准

T/ABI 0003-2025

分布式标识技术要求

Decentralized identifiers technical requirements

（发布稿）

2025-12-12 发布　　2025-12-12 实施

中关村区块链产业联盟　　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这些专利的责任。

本文件由中关村区块链产业联盟提出并归口。

本文件起草单位：中国信息通信研究院、杭州溪塔科技有限公司、天津市气象信息中心、杭州向量共识科技有限公司、北京泰尔英福科技有限公司、布比(北京)网络技术有限公司、心物一同数字科技上海有限公司、理工比特林克(苏州)软件信息技术服务有限公司。

本文件主要起草人：金键、谢家贵、李志平、聂凡杰、蔡啸、徐晓晨、张波、许金良、于明、朱涛、赵玉娟、常高伟、张发振、高琰飙、王鹏理、马一骉。

引　言

分布式数字身份是实现人、机、物、系统等的全面连接与数据互通的新型数字信任体系。广泛连接、异构融合、跨域协作的现代互联网应用场景中，存在着海量设备、智能体、各类应用系统、业务流程以及众多参与方（企业、平台、用户），需分布式标识技术标准作为基础支撑，以实现实体的全域唯一标识、分布式身份认证及跨系统跨域的安全互联与可信协作。

本文件在万维网联盟（W3C）分布式标识系列规范的基础上，规定了分布式标识的核心技术要求，包括分布式标识方法的编码、语法规则要求，同时对分布式标识的文档属性与解析结果数据进行了规范。本文件旨在通过对分布式标识核心数据结构、解析结果数据要求等标准定义，来促进分布式标识方法的互联互通，实现实体在互联网下全域可识别、可验证、可解析的分布式标识解析设施的建立，规范分布式标识应用系统的建设和实施，促进数字实体的安全互联互通与可信协作，为构建自主可控、稳定可靠的互联网数字信任底座提供关键支撑。

分布式标识技术要求

1 范围

本文件规定了分布式标识（DID）的编码、语法、文档属性和解析数据。
本文件适用于分布式标识系统的建设或应用。

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/T25069 信息安全技术术语
IETF RFC 3986 Uniform Resource Identifier (URI): Generic Syntax
IETF RFC 5234 Augmented BNF for Syntax Specifications: ABNF

3 术语和定义

下列术语和定义适用于本文件。

3.1
分布式数字身份标识符 decentralized identifiers;DID
一种全球唯一的持久标识符，不需要集中注册机构，通常通过加密方式生成。
注：DID由三部分组成的统一资源标识符来表示，包括DID方案标识符（固定取值为‘did’）、DID方法标识符和由DID方法指定的唯一特定标识符。DID可解析为DID文档。

3.2
DID **主体** DID subject
由DID标识的实体。
注：DID主体可包括：人、组织、事物或概念。DID主体也可能是DID控制者。

3.3
DID **文档** DID document
描述DID主体的一组数据，包括机制，如加密公钥，DID主体或DID代理可以使用这些机制来验证自身身份并证明其与DID的关联。

3.4
DID **方法** DID method
基于特定方案的DID实现定义。

3.5
DID **解析** DID resolution
以DID作为输入，返回对应的DID文档及附加元数据的过程。

3.6
扩展的巴科斯范式 Augmented Backus–Naur Form
定义形式语言的语法规则，应用于定义各种语言、协议和格式。

4 缩略语

JSON：Javascript对象标记（JavaScript Object Notation）
JSON-LD：互联数据的Javascript对象标记（JavaScript Object Notation for Linked Data）
JWK：JSON Web密钥（JSON Web Key）

URI：统一资源标识符（Uniform Resource Identifier）
URL：统一资源定位符（Uniform Resource Locator）
UTF-8：8比特位的Unicode转换格式（8-bit Unicode Transformation Format）
ABNF：扩展的巴科斯范式（Augmented Backus–Naur Form）

5 分布式标识编码要求

DID应符合IETF[RFC3986]的URI方案。DID编码规则应符合表1要求，字符编码应符合通用字符编码方法UTF-8。

表 1 DID 编码规则

Scheme	DIDMethod	DIDMethodSpecificIdentifier
URI方案标识符	DID方法标识符	DID方法特定的标识符

注：完整的DID标识例如did:example:123456789abcdefghi

6 分布式标识语法要求

DID语法规范应符合IETF [RFC5234]和表2中ABNF规则。

表 2 DID 语法 ABNF 规则

规则	定义
did	="did:"method-name":"method-specific-id（包含小写字母序列 did:、单个冒号、非空的 method-name、单个冒号、非空的 method-specific-id）
method-name	=1*method-char（一个或多个连续的method-char字符）
method-char	=%x61-7A/DIGIT（所有小写字母（a-z）和所有数字（0-9））
method-specific-id	=*(*idchar":")1*idchar（可包含多个以冒号分隔的子段（如 a:b:c），且最后一个子段不能以冒号结尾）
idchar	=ALPHA/DIGIT/"."/"-"/"_"/pct-encoded（可包括所有小写字母（a-z）和所有数字（0-9）、点号(.)、连字符(-)、下划线(_)以及百分号编码）
pct-encoded	="%"HEXDIGHEXDIG（以 % 开头、后跟两个大写十六进制数字字符（0-9 或 A-F）的固定三字节转义序列，用于在文本流中编码保留字符或非ASCII字符）

7 分布式标识方法要求

7.1 方法语法要求

7.1.1 DID 方法规范应定义一个且仅有一个特定的 DID 方法标识符。该标识由第 6 章 DID 语法规范中 method-name 规则指定的唯一方法名称标识。
7.1.2 DID 方法规范应说明如何生成 DID 的 method-specific-id 部分，并定义 method-specific-id 值的敏感性和规范化。method-specific-id 值应在一个 DID 方法中唯一。
7.1.3 任何由 DID 方法生成的 DID 应是全局唯一的。

7.2 方法操作要求

7.2.1 DID 方法规范应定义如何执行所有操作的授权，包括任何必要的加密过程。
7.2.2 DID 方法规范应说明 DID 控制者如何创建 DID 及其关联的 DID 文档。
7.2.3 DID 方法规范应说明如何解析 DID 文档，包括如何验证解析响应的真实性。
7.2.4 DID 方法规范应说明如何更新 DID 文档。
7.2.5 DID 方法规范应说明 DID 控制者如何停用 DID。

8 分布式标识文档及其属性

8.1 DID 文档

8.1.1 DID 文档构成

DID文档应包括DID主体、DID控制者标识符的机制等信息。DID文档中的属性应符合8.2中的要求。

8.1.2 DID 文档的序列化

DID文档可以序列化为字节流。DID文档序列化后的结果应为JSON-LD结构，该结构可作为DID解析的输出结果。附录A给出了DID文档示例。

8.2 DID 文档属性信息

8.2.1 DID 主体

id

```
{
"id":"did:example:123456789abcdefghi"
}
```

标识属性用于表明DID文档对应的主体，其值应是符合5中的编码与语法规则的字符串。标识属性为必选项。

8.2.2 别名

alsoKnownAs

```
{
"alsoKnownAs":["https://Example.com/","did:example:12345qwer"]
}
```

别名属性声明该DID主体控制的一个或多个其他标识符，别名属性为可选项。

别名属性的值应是一个集合，集合内的每项都应是符合IETF[RFC3986]的URI。

8.2.3 控制者

controller

```
{
"controller":"did:example:7643ytgr"
}
```

DID控制者是被授权对DID文档进行更改的实体。该字段的值应为被授权主体的DID。授权DID控制者的过程由DID方法定义。

控制者属性为必选项。

8.2.4 验证方法

verificationMethod

```
{
"verificationMethod":[{
      "id":"did:example:123456789abcdefghi#keys-1",
      "type":"JsonWebKey2020",
      "controller":"did:example:123",
"publicKeyJwk":{
"crv":"Ed25519",
"x":"VCpo2LMLhn6iWku8MKvSLg2ZAoC-nlOyPVQaO3FxVeQ",
"kty":"OKP",//external(propertyname)
"kid":"_Qq0UL2Fq651Q0Fjd6TvnYE-faHiOpRlPVQcY_-tA4A"
}
},{
      "id":"did:example:123456789abcdefghi#keys-2",
      "type":"Ed25519VerificationKey2020",
      "controller":"did:example:pqrstuvwxyz0987654321",
      "publicKeyMultibase":"zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
}]
```

}

验证方法属性为必选项。它可以用来验证或授权与DID主体或关联方的交互。例如，可将公钥用作数字签名的验证。验证方法可包括如下参数：

——id

验证方法的标识符，应定义为DID标识符连接片段（fragment）的方式。

——type

type属性的值为引用一个加密验证方法类型的字符串。验证方法类型应使用公认的标识符。本标准鼓励支持符合国家密码管理政策的验证方法类型，如SM2VerificationKey2022等。

——controller

控制者属性的值为一个符合第5章要求的DID标识符，表明当前验证方法的控制者。

——publicKeyJwk

publicKeyJwk属性是可选项。其值为一个JWK结构，应是一个符合IETF[RFC7517]的JSONWebKey的映射。

——publicKeyMultibase

publicKeyMultibase属性是可选项。该值应是一个编码公钥的字符串表示。

8.2.5 认证

authentication

```
{
"authentication":[
"did:example:123456789abcdefghi#keys-1",
{
    "id":"did:example:123456789abcdefghi#keys-2",
    "type":"Ed25519VerificationKey2020",
    "controller":"did:example:123456789abcdefghi",
    "publicKeyMultibase":"zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
}
]
}
```

认证属性为可选项。其用于指定如何对DID主体进行身份验证，例如用于登录网站或参与任何类型的挑战-响应协议等目的。

认证属性的属性值应为一组验证方法。

8.2.6 断言

assertionMethod

```
{
"id":"did:example:123456789abcdefghi",
"assertionMethod":[
"did:example:123456789abcdefghi#keys-1",
{
    "id":"did:example:123456789abcdefghi#keys-2",
    "type":"Ed25519VerificationKey2020",
    "controller":"did:example:123456789abcdefghi",
    "publicKeyMultibase":"zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
}
],
}
```

断言属性为可选项。其用于指定DID主体预期如何表达声明，例如用于颁发可验证凭证。

断言属性的属性值应为一组验证方法。

8.2.7 服务

service

```
{
```

"service":[{
"id":"did:example:123#linked-domain",
"type":"LinkedDomains",
"serviceEndpoint":"https://bar.example.com"
}]
}

服务属性为可选项。可以是DID主体想要发布的任何类型的服务，例如用于进一步发现、身份验证、授权或交互的身份管理服务。服务应包括如下参数：

——id

id属性的值应符合IETF[RFC3986]的URI。

——type

type属性的值应为一个或一组字符串。

——serviceEndpoint

serviceEndpoint属性的值应是符合[RFC3986]的有效URI。

9 分布式标识解析结果

9.1 DID 解析结果

DID解析应能够通过查询DID标识，以符合规范的格式返回一个DID文档。DID解析结果为JSON结构，由3部分组成：DID解析元数据didResolutionMetadata、DID文档元数据didDocumentMetadata和DID文档流didDocumentStream。附录B给出了DID解析结果示例。

其中，解析元数据didResolutionMetadata的属性定义应符合9.2的要求，DID文档元数据didDocumentMetadata的属性定义应符合9.3的要求，DID文档流didDocumentStream为DID文档的字节流，结构和属性定义应符合第8章的要求。

9.2 DID 解析元数据

9.2.1 内容类型

contentType
{
"contentType":"application/did+ld+json"
}

内容类型属性描述了didDocumentStream的数据结构。

9.2.2 错误

error
{
"error":"notFound"
}

错误属性表示解析错误信息，无错误时不展示。解析元数据中的错误编码应符合表3要求。

表 3 解析元数据中的错误编码

编号	错误值	含义
1	InvalidDid	提供的DID不符合有效语法
2	notFound	找不到对应的DID文档
3	representationNotSupported	不支持此DID方法解析

9.3 DID 文档元数据

9.3.1 创建时间

created
{

"created":"2019-03-23T06:35:22Z"
}

创建时间属性表示DID文档的创建时间。该属性的值应是一个字符串，格式为标准化到UTC00:00:00的XML日期时间，且不包含亚秒小数精度。

9.3.2 更新时间

updated
{
"updated":"2023-08-10T13:40:06Z"
}

更新时间属性表示DID文档的最后更新时间。该属性的值应是一个字符串，格式为标准化到UTC00:00:00的XML日期时间，且不包含亚秒小数精度。

9.3.3 是否停用

deactivated
{
"deactivated":true
}

是否停用属性为Boolean值，表示返回的DID文档是否为停用状态。如果当前DID文档已停用则该属性的值为true，否则为false。

9.3.4 版本号

versionId
"versionId":"bafyreifederejlobaec6kwpl2mc3tw7qk3j3ey4uytkbiw2qw7dzylud6i"
}

版本号属性为字符串类型，用来表示DID文档的版本号。该属性的值应是ASCII字符串。

附 录 A
（资料性）
DID 文档示例

以某生产制造企业主体为例的DID文档结构如下：


```
{
"@context":"https://www.w3.org/ns/did/v1",
"id":"did:example:7hjkb121",
"alsoKnownAs":"https://www.example.cn",
"controller":"did:example:7hjkb121",
"verificationMethod":
{
      "id":"did:example:7hjkb121#keys-1",
      "type":"SM2VerificationKey2022",
      "controller":"did:example:7hjkb121",
      "publicKeyJwk":{
      "kty":"EC",
      "crv":"SM2",
      "x":"dWCvM4fTdeM0KmloF57zxtBPXTOythHPMm1HCLrdd3A",
      "y":"36uMVGM7hnw-N6GnjFcihWE3SkrhMLzzLCdPMXPEXlA"}
},
"assertionMethod":
{
      "id":"did:example:7hjkb121#keys-1"
},
"service":
{
      "id":"did:example:7hjkb121#linkedDomains",
      "type":"LinkedDomains",
      "serviceEndpoint":"https://www.example.cn//linkedDomain"
}
}
```

附 录 B
（资料性）
DID 解析结果示例

以某生产制造企业主体为例的 DID 解析结果如下：


```
{
"didResolutionMetadata":{
"contentType":"application/did+ld+json"},
"didDocumentMetadata":{
"created":"2024-03-23T06:35:22Z",
"updated":"2025-03-10T13:40:06Z",
"deactivated":false,
"versionId":"bafyreifederejlobaec6kwpl2mc3tw7qk3j3ey4uytkbiw2qw7dzylud6i"
},
"didDocument":{
    "@context":"https://www.w3.org/ns/did/v1",
    "id":"did:example:7hjkb121",
    "alsoKnownAs":"https://www.example.cn",
    "controller":"did:example:7hjkb121",
    "verificationMethod":
{
    "id":"did:example:7hjkb121#keys-1",
    "type":"SM2VerificationKey2022",
    "controller":"did:example:7hjkb121",
    "publicKeyJwk":{
    "kty":"EC",
    "crv":"SM2",
    "x":"dWCvM4fTdeM0KmloF57zxtBPXTOythHPMm1HCLrdd3A",
    "y":"36uMVGM7hnw-N6GnjFcihWE3SkrhMLzzLCdPMXPEXlA"}
},
"assertionMethod":
{
    "id":"did:example:7hjkb121#keys-1"
},
"service":
{
    "id":"did:example:7hjkb121#linkedDomains",
    "type":"LinkedDomains",
    "serviceEndpoint":"https://www.example.cn//linkedDomain"
}
},
"assertionMethod":
{
    "id":"did:rem:shanghai:SH000001F.S2101#keys-1"
},
"service":
{
    "id":"did:rem:shanghai:SH000001F.S2101#linkedDomains",
    "type":"LinkedDomains",
    "serviceEndpoint":"https://www.agency.sh.com.cn/linkedDomain"
}
}
}
```

参 考 文 献

［1］GB/T 17902.2-2005　信息技术 安全技术 带附录的数字签名 第 2 部分:基于身份的机制
［2］GB/T 31504—2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范
［3］GB/T 42021—2022 工业互联网 总体网络架构
［4］JR/T 0325—2024 区域性股权市场分布式数字身份技术规范
［5］万维网联盟 互联数据的 JSON 1.1（W3C JSON-LD 1.1）
［6］万维网联盟 XML 模式定义语言 1.1 第 2 部分：数据类型（W3C XML Schema Definition Language
［7］万维网联盟 W3C Decentralized Identifiers Core architecture,datamodel,and representations