

# 《分布式数字身份 第1部分：技术框架》

## 编制说明

### 一、工作简况

#### （一）任务来源

本标准根据中国信息协会的通知立项，计划编号为 P2025-004。

本标准由中国信息协会提出并归口。

本标准由中国民航信息网络股份有限公司为牵头单位的起草小组组织起草，参与起草单位包括泉州晋江国际机场、成都航空有限公司、北京航空航天大学、北京工业大学、青岛国际机场集团有限公司、国网数字科技控股有限公司、中讯邮电咨询设计院有限公司、山东区块链研究院。

#### （二）研制背景

在数字经济快速发展的背景下，信息化行业作为数据密集型行业，传统数据管理模式凸显诸多弊端：各代理平台采用私有 ID 格式、私有协议存储使用用户数据，造成数据碎片化、用户体验不连贯，且数据易被篡改；用户作为数据归属主体，其身份信息和行为数据的自主控制权未得到充分尊重，无法按需存储、披露和使用相关数据，核心原因在于缺乏统一、可验证的数字身份标准及体系。

国家政策方面，《网络安全法》、《个人信息保护法》等法规为数字身份技术研究和应用奠定法律基础，《“十四五”数字经济发展规划》提出加快数字身份统一认证互信互认，《贯彻实施〈国家标准化发展纲要〉行动计划（2024—2025 年）》明确要求强化区块链技术标准体系建设、开展分布式数字身份分发核心标准研究，分布式数字身份标准化成为必然趋势。同时，W3C 成立 DID 工作组推动分布式标识符标准化，中国信通院加入该工作组参与相关标准研究，国际层面的技术和标准探索为国内发展提供了参考。

另外，民航、铁路、海运等信息化行业在业务办理中存在个人信息泄露风险，以民航为例，机票预定、安检、行李托运等环节均面临旅客隐私保护难题。分布式数字身份（DID）作为 Web3.0 时代的身份基石，具备去中心化、防篡改、用户自主可控、全局可解析等特性，能有效解决数据安全、可信、隐私保护和价值流通问题，为行业数字化转型提供基础支撑。目前国际航空运输协会（IATA）已

将 DID 纳入航空现代零售体系并推进相关国际标准制定，但国内信息化行业尤其是民航业尚未形成统一的分布式数字身份标准，行业发展缺乏规范指导，因此亟需制定适用于信息化行业的分布式数字身份技术框架标准。

### （三）主要工作过程

**前期调研阶段：**202X 年 XX 月 - 2024 年 XX 月，牵头单位中国民航信息网络股份有限公司联合各参编单位，开展分布式数字身份技术及行业应用调研，梳理 W3C DID v1.0、VC data model v2.0 等国际标准规范，研究 IATA TrulyMe、OneID 等国际行业应用案例，分析民航、铁路等信息化行业的数字身份需求和痛点，形成调研分析报告。

**立项筹备阶段：**202X 年 XX 月，完成《分布式数字身份》系列团体标准立项申请书编制，组织召开立项论证研讨会，确定标准体系框架（分为技术框架、可信机构通用服务规范、可验证凭证术语表、民航业分布式数字身份规范四部分），明确本部分（技术框架）为系列标准的核心基础部分，报中国信息协会完成立项申请。

**草案编制阶段：**202X 年 XX 月 - 202X 年 XX 月，成立由区块链、信息安全、密码学、民航业务等领域专家组成的起草小组，依据 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》，结合调研成果和国际标准，完成《分布式数字身份 第 1 部分：技术框架》大纲和草案编写，经起草小组内部多次审查、修改后，形成征求意见稿。

**意见征求阶段：**2026 年 3 月 - 2026 年 4 月，将征求意见稿面向行业内企事业单位、科研机构、高校等挂网征求意见，对反馈的意见和建议进行分类整理、分析研究，形成意见处理办法，根据意见对标准内容进行修改完善，组织专家审查会，经专家审议通过后形成送审稿。

**报批发布阶段：**202X 年 XX 月 - 202X 年 XX 月，根据专家审查会意见对送审稿进行最终修改，完成报批稿编制，报中国信息协会审批，审批通过后正式公开发布。

### （四）主要参加起草单位和工作组成员所做的工作

中国民航信息网络股份有限公司（主编单位）：牵头整体标准研制工作，负责项目统筹、调研组织、草案核心内容编制，梳理民航行业分布式数字身份应用需求，确定标准的总体架构和技术要求，组织召开各类研讨会和审查会，完成意见处理、报批稿编制等工作。

北京航空航天大学、北京工业大学（参编单位）：负责分布式数字身份相关技术研究，梳理国际前沿技术规范 and 标准，为标准的术语定义、技术框架设计提供理论支撑；刘懿中、杨震等专家牵头完成术语和定义、验证方法、数据模型等技术章节的编制，审核标准的技术严谨性和规范性。

泉州晋江国际机场、成都航空有限公司、青岛国际机场集团有限公司（参编单位）：结合民航一线业务场景，提供行业应用需求和实际案例，验证标准技术框架的可行性和实用性，提出针对民航行业的应用优化建议，确保标准符合行业实际应用需求。

国网数字科技控股有限公司、中讯邮电咨询设计院有限公司、山东区块链研究院（参编单位）：参与可信数据存储、分布式公钥基础设施（DPKI）等技术章节的编制，提供区块链、分布式存储等技术实践经验，对标准中的技术实施要求进行完善，保障标准的技术可落地性。

全体工作组成员均参与了标准草案的讨论、意见征求、修改完善等全过程工作，严格按照标准化工作要求，确保标准编制的科学性、规范性和适用性。

## 二、标准编制原则、主要内容及其确定依据

### （一）编写原则

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，同时遵循以下核心原则：

**合规性与国际接轨原则：**兼容国际通用的技术规范和数据模型，确保标准与国际发展同步，同时符合我国《网络安全法》《个人信息保护法》等法律法规要求。

**科学性与实用性原则：**基于分布式账本、区块链、IPFS 等成熟技术，结合民航等信息化行业的实际应用需求，构建可落地、可操作的技术框架，明确各层级

技术要求和实施规范，兼顾技术的先进性和行业的实用性。

**通用性与行业适配性原则：**本标准作为信息化行业的基础技术框架，兼顾民航、铁路、海运等多行业的通用需求，统一核心术语、总体架构和交互规则，同时预留行业扩展接口，为后续各行业专项规范制定奠定基础。

**用户自主与安全可控原则：**围绕分布式数字身份“用户自主可控”的核心特性，在标准中明确身份信息的管理、使用和验证规则，强化数据安全和隐私保护要求，确保身份数据在流通和使用过程中的安全性、可控性。

**开放性与互操作性原则：**明确标准中的数据格式、接口规范、交互流程，确保不同系统、不同机构、不同行业之间的分布式数字身份系统能够实现互联互通、互认互验，降低系统接入和数据交换成本。

## （二）主要内容及其确定依据

本标准规定了信息化行业分布式数字身份建设的术语和定义、缩略语、总体架构、建议实施技术等内容，适用于相关行业分布式数字身份系统建设、行业内及跨行业凭证数据交换和验证，其主要内容及确定依据如下：

术语和定义、缩略语部分，共定义分布式账本、分布式数字身份（DID）、可验证凭证等 30 项核心术语，明确 DID、DLT、VC 等 4 项关键缩略语，结合国内信息化行业的应用习惯进行界定，同时补充 DID 委托人、DID 方法注册中心等行业应用所需的术语，统一行业内的概念认知。

总体架构层，构建可信数据存储、分布式数字身份、可验证凭证生态三层技术架构，为分布式数字身份系统建设提供整体框架。确定依据为分布式数字身份的技术实现逻辑，结合民航行业航旅链平台的实践架构，三层架构既符合技术底层到应用层的层级划分，又适配行业实际应用中的数据存储、身份管理、凭证交互需求。

可信数据存储层，明确分布式账本、去中心化文件系统等存储设施的技术要求和作用，确定依据为区块链、IPFS 等分布式存储技术的特性，以及行业对身份数据安全、不可篡改、去中心化存储的需求。

分布式数字身份层，定义 DID 注册中心、DID 方法注册中心、VC 可信机构注册中心的核心功能和交互流程，结合行业内多机构参与的特点，明确各注册中心

的职责和服务要求，保障 DID 的全局可解析和统一管理。

可验证凭证生态层，规范可验证凭证的可信交换流程和生态参与方（发证方、持证方、验证方）的交互关系，结合行业凭证颁发、验证、流转的实际业务流程，明确凭证状态管理、转移方式等要求，实现凭证的安全可信交换。

建议实施技术，针对三层架构分别提出具体的实施技术要求，包括可信数据存储采用的区块链、IPFS 技术规范，分布式数字身份层的 DID 服务、VC 可信机构注册中心管理要求，可验证凭证生态的凭证定义、词汇表、模板、状态的标准化要求。确定依据为国内区块链、分布式数字身份技术的实践成果，结合民航等行业的技术应用能力，提出可落地的技术实施建议，同时明确行业统一的技术规范，确保不同机构的实施一致性。

附录部分包含 DID 标识符、DID URL、DID 文档、可验证凭证的详细技术规范和数据模型，结合行业应用需求补充数据模型的属性要求、序列化格式、示例等内容，为标准的实际实施提供详细的技术指导。

本标准的内容确定充分兼容国际标准规范、国内政策要求、信息化行业的实际需求和 技术实践，确保标准的科学性、规范性和可操作性，同时为《分布式数字身份》系列标准的后续部分（可信机构通用服务规范、可验证凭证术语表、民航业分布式数字身份规范）提供基础技术框架支撑。

### 三、国外相关法律、法规和标准情况的说明

国外目前尚未针对分布式数字身份制定专门的法律法规，但各国均通过数据保护、网络安全相关法律对数字身份的使用和数据安全进行规范，例如欧盟《通用数据保护条例（GDPR）》明确了个人数据的自主控制权和隐私保护要求，美国《加州消费者隐私法案（CCPA）》规定了消费者对个人信息的访问、删除等权利，此类法律法规为分布式数字身份的应用提供了法律边界，也是本标准编制中遵循的隐私保护和数据安全原则的重要依据。

在标准方面，国际上分布式数字身份的标准体系以 W3C（万维网联盟）制定的标准为核心，已发布多项成熟规范，成为全球行业遵循的基础。

另外，国际行业组织和企业也在推进分布式数字身份的行业应用标准和方案。如国际航空运输协会（IATA）提出的 TrulyMe 项目构想，将分布式数字身份的

可验证声明表示为智能旅行对象，推动 OneID 项目发展，制定航空行业的分布式数字身份应用规范，本标准在编制过程中参考了 IATA 的航空行业应用需求和方案设计，确保对民航业的适配性；微软、百度、华为等企业均推出各自的 DID 技术方案，在身份管理、可验证凭证应用等方面形成了实践经验，本标准在编制过程中梳理了各企业的技术实践，吸收了成熟的实施技术要求。

国外分布式数字身份的标准体系以 W3C 的基础技术标准为核心，行业应用标准由各行业组织逐步推进，本标准在编制过程中全面遵循国际通用的基础技术标准，同时结合国内信息化行业的需求进行优化和补充，确保与国际接轨的同时适配国内行业实际。

#### 四、与国内有关现行法律、法规及相关标准的关系

本标准的编制严格符合我国现行的网络安全、数据保护、个人信息保护相关法律法规，包括《网络安全法》《数据安全法》《个人信息保护法》等：

符合《个人信息保护法》中“个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理”的规定，本标准围绕分布式数字身份“用户自主可控”的核心特性，明确用户对其数字身份信息的管理和控制权，规范身份信息的使用和验证流程。

符合《网络安全法》《数据安全法》中关于数据安全保护、防篡改、可追溯的要求，本标准采用分布式账本、区块链等技术实现身份数据和可验证凭证的安全存储，明确数据传输和交换的安全要求，确保数据的完整性和安全性。

符合法律法规中关于电子证照、电子认证的相关规定，本标准中的可验证凭证规范与电子证照的互认互验要求相衔接，为电子证照的分布式管理和跨行业使用提供技术框架。

本标准与国内现行法律、法规无冲突，是对法律法规中数字身份、数据安全相关要求的落地和规范细化，为法律法规在信息化行业的实施提供技术支撑。

目前国内尚未发布分布式数字身份的国家标准和行业标准，相关标准研究主要以团体标准和地方标准为主，且多聚焦于区块链技术基础，本标准与国内现有相关标准的关系如下：

本标准中可信数据存储层采用的区块链技术要求，与《区块链 分布式账本

技术要求》(GB/T 42752-2023)等国家标准相衔接,遵循区块链的基础技术规范,确保分布式数字身份系统与区块链基础设施的兼容性。

本标准作为信息化行业的基础技术框架,与民航、铁路等行业的现有信息化标准相衔接,例如民航行业的旅客信息管理、电子客票等标准,预留行业接口,确保分布式数字身份系统能够融入行业现有信息化体系。

## 五、重大意见分歧的处理经过和依据

本标准在标准起草过程中,对标准中的技术内容没有发生重大分歧。

在标准编制的意见征求和专家审查阶段,行业内专家和参编单位主要提出了部分技术细节的优化建议,例如对可验证凭证状态的分类、DID解析流程的简化、行业扩展接口的设计等,起草小组对所有建议进行了认真研究和讨论,对合理的建议予以采纳并对标准内容进行修改完善,对暂不具备实施条件的建议,结合行业技术发展现状进行了说明并保留后续优化空间。所有意见均得到妥善处理,未形成重大分歧,确保了标准编制的顺利推进。

## 六、涉及专利的有关说明

本标准的编制过程中,参考和采用的技术内容主要基于国际组织发布的开源标准和通用技术,同时融合了起草单位在区块链、分布式数字身份领域的技术实践成果。其中,牵头单位中国民航信息网络股份有限公司在航旅链平台、DID基础设施建设方面拥有多项区块链相关的发明专利和实用新型专利,相关专利技术已应用于标准的技术实施建议中,为标准的可落地性提供了技术支撑。

本标准发布机构不承担识别专利的责任,标准中涉及的专利技术均由相关持有单位提供,且相关单位承诺在标准实施过程中,为行业内单位提供合理、非歧视性的专利许可,确保标准的顺利推广和实施。本标准的编制和实施不存在专利壁垒问题。

## 七、预期的社会效益

### (一) 社会效益

1. **完善数字身份标准体系,推动数字经济规范化发展:** 本标准填补了国内

信息化行业分布式数字身份技术框架的标准空白，构建了统一、规范的技术体系，为后续各行业专项规范和国家标准的制定奠定基础，推动我国数字身份领域的标准化、规范化发展，助力《“十四五” 数字经济发展规划》相关要求的落地。

**2. 强化个人信息保护，保障用户数字身份自主权：**标准以“用户自主可控”为核心，规范分布式数字身份的管理和使用流程，有效解决传统身份管理模式中用户信息泄露、控制权缺失等问题，切实保障用户的个人信息安全和数字身份自主权，符合《个人信息保护法》的立法精神。

**3. 促进跨行业互联互通，推动数字生态建设：**标准统一了信息化行业分布式数字身份的核心术语、技术框架和交互规范，打破各行业、各机构之间的身份壁垒，实现数字身份和可验证凭证的跨行业互认互验，推动形成开放、互联、可信的数字生态。

**4. 助力行业数字化转型，提升公共服务能力：**以民航行业为代表，标准为行业打造“无证通行”等便捷服务提供技术支撑，简化业务办理流程，提升旅客出行体验，同时为铁路、海运等其他信息化行业的数字化转型提供基础技术框架，提升行业公共服务的智能化、便捷化水平。

## （二）经济效益

**1. 降低行业系统接入和运营成本：**标准统一了分布式数字身份系统的技术框架和接口规范，降低了第三方服务商的系统理解难度和接入复杂度，减少了各机构重复开发和系统对接的成本，提升行业整体运营效率。

**2. 减少信息泄露带来的经济损失：**标准通过分布式存储、加密验证等技术手段，强化身份数据和业务数据的安全保护，有效降低民航、铁路等行业因个人信息泄露带来的经济损失和品牌风险，减少行业监管和风险处置成本。

**3. 推动数字身份相关产业发展：**标准的发布和实施将带动区块链、分布式存储、数字认证等相关技术产业的发展，培育分布式数字身份的应用服务市场，为数字经济发展注入新的增长点。

**4. 提升行业数字化服务的商业价值：**以民航行业为例，基于标准的分布式数字身份系统可实现旅客信息的精准、安全管理，推动航空旅游服务的个性化、智能化升级，提升行业数字化服务的商业价值和市场竞争力。

八、推广实施团体标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等。

#### （一）推广实施要求

民航、铁路、海运等信息化行业的企事业单位、科研机构、服务商在建设分布式数字身份系统时，应统一遵循本标准的技术框架、术语定义和实施规范，确保系统的兼容性和互操作性。

先在民航行业开展标准试点应用，依托中国民航信息网络股份有限公司的航旅链平台，在航空公司、机场等单位落地分布式数字身份系统，总结试点经验后，逐步推广至铁路、海运等其他信息化行业。

各单位在实施标准时，应做好与现有信息化系统、电子认证体系、数据管理系统的衔接，充分利用现有技术资源，避免重复建设，实现分布式数字身份系统与现有系统的平滑融合。

在遵循本标准核心技术要求的基础上，鼓励行业内单位开展分布式数字身份技术的创新研究和应用探索，推动标准的持续优化和升级，实现技术创新与标准落地的良性互动。

#### （二）组织措施

由中国信息协会牵头，联合中国民航信息网络股份有限公司等主编单位、各参编单位，成立标准推广实施工作组，负责标准的宣贯、培训、试点指导和实施效果评估，统筹推进标准在行业内的推广实施工作。

组织编写标准宣贯材料和培训教材，面向行业内企事业单位、服务商开展线上线下相结合的宣贯和培训活动，普及标准的核心内容和实施要求，培养一批掌握标准的技术和管理人才。

工作组定期对行业内标准实施情况进行监督和评估，收集实施过程中的问题和建议，及时对标准进行修订和完善，确保标准的适用性和有效性。

组织开展分布式数字身份标准实施的行业交流研讨会，分享实施经验和科技成果，推动行业内单位之间的合作，共同完善分布式数字身份生态体系。

### （三）技术措施

由起草小组编制《分布式数字身份 第 1 部分：技术框架》实施技术指南，对标准中的核心技术内容、实施步骤、数据模型、接口规范等进行详细解读，为各单位的实际实施提供技术指导。

主编单位和参编单位的技术专家为行业内单位提供标准实施的技术咨询和技术支持，解决实施过程中的技术难题，保障标准的顺利落地。

鼓励区块链、分布式存储、数字认证等领域的技术企业，按照本标准的要求开发相关技术产品和解决方案，推动行业内技术产品的标准化，提升产品的兼容性和可操作性。

### （四）过渡期建议

建议本标准发布后设置 12 个月的过渡期（自标准实施之日起计算），过渡期内为行业内单位的标准实施提供缓冲时间：

过渡期内，各单位可结合自身实际情况，开展现有系统的改造和分布式数字身份系统的规划、设计工作，组织技术人员参加标准培训，完成技术储备和人员储备。

过渡期后，民航行业的核心企事业单位（航空公司、大型机场、民航信息服务商）应全面实施本标准，建成符合标准要求的分布式数字身份系统；铁路、海运等其他信息化行业应启动标准实施工作，逐步完成系统建设和改造。

### （五）实施日期建议

建议本标准的正式实施日期为 2026 年 XX 月 XX 日（自标准公开发布之日起 3 个月后），预留足够的时间供行业内单位开展标准宣贯、培训和实施准备工作。

## 九、其他应当说明的事项。

本标准为《分布式数字身份》系列团体标准的第 1 部分（技术框架），是系列标准的核心基础部分，后续将陆续发布第 2 部分《可信机构通用服务规范》、第 3 部分《可验证凭证术语表》、第 4 部分《民航业分布式数字身份规范》，各部分标准将紧密衔接，形成完整的信息化行业分布式数字身份标准体系。

本标准的编制充分考虑了技术的发展趋势，预留了技术扩展接口和行业扩展接口，对于新兴的分布式存储技术、密码学技术、身份验证技术，以及其他信息化行业的特殊需求，可在后续标准修订和专项规范中进行补充和完善。

本标准的实施过程中，及时跟踪国际标准的更新动态，确保本标准与国际标准的持续接轨，同时推动我国分布式数字身份标准的国际化输出。

本标准的起草团队由区块链、信息安全、密码学、民航业务、铁路业务等多领域的专家组成，具备扎实的理论基础和丰富的实践经验，为标准的科学性、规范性和可操作性提供了有力的人才保障。