

引用格式: 李海晏.可信数字身份标准化现状与对策研究[J].标准科学,2025(2):36-46.

LI Hai-yan.Current Status and Countermeasures of Standardization for Trusted Digital Identity[J]. Standard Science,2025(2):36-46.

可信数字身份标准化现状与对策研究

李海晏

(福建省标准化研究院)

摘 要:【目的】通过提出可信数字身份标准化对策建议,促进可信数字身份战略实施。【方法】基于对可信数字身份概念及内涵、标准化研究进展、标准化现状、存在问题进行分析,提出标准制修订建议目录和标准化对策建议。【结果】可信数字身份标准化研究蓬勃发展,众多国际、区域及我国标准化组织都致力于统一可信数字身份认证研究。存在可信数字身份互联互通,跨行业、跨领域应用标准不足等问题。【结论】从完善可信数字身份标准化政策措施和工作机制、建立健全标准体系、开展标准化研究和标准研制、加强标准实施应用、加强国际标准化工作等方面提出了对策建议。

关键词: 可信数字身份; 生物特征识别; 认证; 标准; 标准化; 标准体系

DOI编码: 10.3969/j.issn.1674-5698.2025.02.006

Current Status and Countermeasures of Standardization for Trusted Digital Identity

LI Hai-yan

(Fujian Institute of Standardization)

Abstract: [Objective] This paper aims to facilitate the implementation of the trusted digital identity strategy by proposing standardization countermeasures and recommendations for trusted digital identity. [Methods] Based on the analysis of the concept and connotation of trusted digital identity, the progress in standardization research, the current status of standardization, and existing issues, a list of recommendations for the revision of standards and standardization countermeasures is proposed. [Results] The research on the standardization of trusted digital identity is flourishing, with numerous international, regional, and national standardization organizations dedicated to the study on unified trusted digital identity authentication. Issues such as insufficient standards for interoperability, cross-industry, and cross-domain applications of trusted digital identity persist. [Conclusion] Some countermeasures and suggestions for the standardization of trusted digital identity have been put forward such as improving the policy measures and working mechanism of trusted digital identity standardization, establishing and improving the standards system, carrying out research on trusted digital identity standardization, conducting standardization research and developing standards, strengthening the application of standards, and strengthening international standardization efforts.

Keywords: trusted digital identity, biometric identification, authentication, standard, standardization, standards system

基金项目: 本文受福建省公益类科研院所专项项目“可信数字身份及其数据价值挖掘标准化研究”(项目编号: 2022R1017004)资助。

作者简介: 李海晏, 博士, 高级工程师, 研究方向为数字化、生态文明、知识产权标准化。

可信数字身份是保障网络信息安全与合规,提高交流效率与互信的基础。在政务服务、数字经济、社会治理等各类应用场景中,大量的企业法人、自然人、物品有身份识别认证需求。可信数字身份和电子认证是满足这些需求的有效数字化解决方案。标准化水平已成为影响可信数字身份行业核心竞争力的基本要素。开展可信数字身份标准化工作对促进互联、互通、互认和自主可控的可信数字身份认证技术发展,促进可信数字身份战略实施,助力数字经济发展和经济社会数字化转型具有重要意义。

1 可信数字身份相关概念及内涵

ISO/IEC 24760-1将“身份(identity)”定义为:“一组与实体(entity)相关的属性(attributes)”^[1]。这里所说的实体为“操作某个特定域的相关项,具有物理或逻辑形态,包括自然人、组织、设备、SIM卡、护照、网卡、应用软件、服务或网站等”^[1]。YD/T 2592—2013将“身份(identity)”定义为:“实体的表现形式,由一种或多种属性构成,这些属性使某个实体或多个实体能够在环境中被充分区分”^[2]。上述两项标准都强调“身份”是由实体相关的属性构成的。

在数字经济时代,人类的经济和数据活动转移到了网络空间,传统身份认证体系难以适应数字经济的发展需求。数字身份的出现是对传统身份认证体系的突破和超越^[3]。GB/T 31504—2015将“数字身份(digital identity)”定义为“主体在互联网中的虚拟身份表示,关联了与该主体相关的属性信息,通常由一个账户标识其唯一性”^[4]。数字身份不仅包括人,还包括网络及计算设备、系统及应用软件、数据或其他信息资产等其他主体^[3]。数字身份可以采用实物凭证,如电子证卡、数字证书、智能卡等,也可以是虚拟标识符或数据。对于自然人来说,数字身份包含了个人标识及与标识所绑定的个人信息,并以可验证身份凭证的方式为自然人在数字空间提供真实身份及属性证明^[5]。

可信数字身份是基于法定身份信息,由权威

机构签发,有政策法规保障支撑的数字身份,是数字空间自然人身份的信任根本^[6]。其更加强调可信性、安全性和便捷性,在增强互信、确保信息安全等方面强化了数字身份的价值。其内涵以法律法规和标准规范为基础,由权威机构认证,通过技术手段和治理机制,解决各类应用场景中“人机物”的身份认证与验证、身份数据保护与管理、身份权力与责任界定等关键问题,具有主体可验证、操作可追溯、管理可控制、监管可触达等特征,最终保证数字身份可信、安全、便捷、高效和低成本,广泛应用于生产、生活、治理等各个领域,助力提升生产效率,改善生产关系。其核心在于加强人与人之间、人机之间、万物之间的身份信任,实现各主体身份的互认、互联和互通,最终推动数字身份广泛应用,实现价值最大化^[7]。可信数字身份不仅具有唯一性、虚构性与多态性、稳定性、超域性、可追溯性等特征,还具有防止合法用户超越权限的操作,防止非法用户入侵的功能。

2 可信数字身份标准化研究进展

可信数字身份标准化研究主要集中于分布式数字身份、与移动通信网络协同发展、生物特征识别、数据挖掘应用等方面。

分布式数字身份标准化工作日益受到重视。围绕分布式数字身份,多个标准组织、开源社区、分布式数字身份联盟共同努力,推进了一系列分布式数字身份相关技术标准和协议的制定,主要包括W3C(万维网联盟)推动的DID和可验证凭证规范,重启可信网络(RWOT)工作组的DID Auth规范,OASIS(结构化信息标准促进组织)的分布式密钥管理(DKMS)规范和DIF(去中心化身份基金会)推动的DID Comm协议等^[8]。其中W3C于2019年成立DID专项工作组,致力于解决身份标识、权威认证、可信验证、高效互通、隐私保护等核心问题,并制定DID URL方案标识符、数据模型、DID文件语法等相关标准^[8]。W3C发布《DID——核心架构、数据模型及表示》标准^[5],对去中心化身份标识符的使用进行了规范,增强了互操作性和用

户控制^[9]；更新Web Authn标准，支持更多的身份验证设备和生物识别技术，提升Web上的身份验证安全性^[9]。ETSI（欧洲电信标准化协会）下属的电子签名和基础设施委员会专门负责电子签名和数字身份相关标准的制定，已建立了涵盖签名设备、签名生成与验证、证书策略等内容的较为完善的电子签名技术标准体系^[3]。

标准化支撑引领数字身份与移动通信网络协同发展。移动通信网络为数字身份的安全、可靠和互操作性提供保障，数字身份为移动通信业务场景应用赋能。ITU-T（国际电信联盟电信标准分局）率先开启移动通信分布式数字身份相关标准研制。ITU-T所属的SG2 Operational aspects（运营方面）对基于数字身份的移动通信网络资源访问控制策略进行了研究。ITU-T所属的SG17 Security（安全），一方面，推动修订X.1250等身份管理基础技术标准，并引入分布式数字身份和数字钱包、区块链等新型数字身份管理概念；另一方面，积极推动移动通信网络数字身份基础定义、技术框架及安全隐私相关标准研制^[9]。SG13 Future networks（未来网络）从下一代通信网络（NGN）角度出发，制定了身份管理在电信行业的应用框架，同时，关注分布式数字身份对用户身份和网络标识管理的赋能，将分布式身份/自主身份等理念与未来网络和IMT-2030网络相结合。SG16 Multimedia and digital technologies（多媒体与数字技术）关注分布式账本技术在移动通信网络中标识跨域互信的应用。NGMN（下一代移动网络联盟）发布了关于5G网络中隐私保护和安全性报告，提供了详细的实施指南和最佳实践^[9]。3GPP（第三代合作伙伴计划）通过其所属的SA2（系统架构组）和SA3（安全组），专注于研制与数字身份相关的身份分发、身份识别与认证、隐私保护、用户身份与权限管理、身份相关能力开放等方面的标准，旨在确保用户通过数字身份接入网络，享受高速移动网络服务，5G release19阶段中有部分标准正在构筑全新userID身份管理机制。GSMA（全球移动通信系统协会）提出了Mobile Connect 2.0，提供多因素认证和用户控制选项，支持面部识别和指纹识别等生物特征识别

技术；推出跨国身份互操作性框架，简化国际用户在不同国家和地区之间的身份验证过程。2021年，IEEE（电气与电子工程师协会）成立了致力于物联网应用与DID技术相结合的专项工作组，以实现基于DID的智能设备可信接入和设备间的点到点直接通信^[5]。

可信数字身份识别，尤其是生物特征识别标准化相关研究是重点。岳林指出，身份识别标准被各国隐私法和个人信息法普遍采纳，是人们界定信息相关权利利益的主要标签^[10]。苏宇等指出，应确定个人信息的识别标准与保护范围，并且单一的身份识别标准应发展成具有差异化、可动态调整的标准体系^[11]。谢宗晓等介绍了身份和访问管理相关标准，包括关于身份管理的ISO/IEC 24760，关于访问管理的ISO/IEC 29146，关于鉴别保证的ISO/IEC 29115，关于鉴别模式的ISO/IEC 9798系列标准^[12]。李俊等建议制定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》的配套验证评估标准^[13]。林冠辰等建议基于GB/T 38542—2020《信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架》，进一步细化深入提出智能终端侧基于生物特征识别身份鉴别的技术要求和实践指南，完善智能终端侧网络安全标准体系^[14]。孙曦等阐述了由我国专家在ISO/IEC JTC 1/SC 27/WG 5牵头的国际标准研究项目《移动设备生物特征识别身份认证安全框架》的编制背景、相关标准、技术内容以及对国内产业的影响^[15]。中国电子技术标准化研究院等发布《人脸识别数据安全标准化研究报告（2021版）》，阐述了人脸识别数据安全政策法规和标准现状^[16]。

为推动数字身份数据的开发应用，数据挖掘技术得到广泛应用。宋宇航基于SPARK技术开展了虚拟身份数据的采集、存储、预处理以及数据分析研究，指出可以根据用户网络行为提供个性化信息，减少信息提供者的信息推送成本^[17]。周瑞等开展了“基于情景感知与数据挖掘的互联网身份认证机制与关键技术研究”，指出该身份认证机制可以应用在智能移动设备上，既可以作为开机时的解锁认证，也可以作为手机银行、手机支付前的二级认

证,增加对个人财产和隐私信息的保护^[18]。黄润飞等指出港澳地区以统一社会信用代码数据为基础,在金融、海关、电商等领域不断推进可信数字身份的创新应用^[19]。黄炜将数据挖掘技术中的分类、聚类、关联三种算法结合,提出了基于数据挖掘的学习者身份识别技术^[20]。

3 可信数字身份标准化现状

3.1 政策要求

我国多项法规、政策要求推动可信数字身份标准化工作,要求完善隐私保护、网络身份认证服务等安全可信标准。2021年11月起施行的《中华人民共和国个人信息保护法》要求,制定个人信息保护具体规则、标准,积极参与个人信息保护国际规则的制定,推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认,针对人脸识别制定专门的个人信息保护规则、标准^[21]。2021年12月,国家标准化管理委员会等十部门印发《“十四五”推动高质量发展的国家标准体系建设规划》,要求推动网络空间可信身份等重点领域国家标准研制,完善网络安全标准体系,支撑网络强国建设^[22]。2024年3月,由市场监管总局、中央网信办等多部门联合印发的《贯彻实施〈国家标准化发展纲要〉行动计划(2024—2025年)》提出,推动分布式数字身份分发等关键技术领域的标准化工作,以确保数字身份的安全和隐私保护,同时促进相关技术的规范化发展和应用。2024年5月,国家标准化管理委员会等十一部门联合发布《关于实施公共安全标准化筑底工程的指导意见》,要求推进国家网络身份认证公共服务标准化建设,加强人体生物特征识别应用相关标准制修订,推动公共安全视频图像信息智能分析与深度挖掘应用标准制修订^[23]。2024年6月,工业和信息化部等四部门联合发布《国家人工智能产业综合标准化体系建设指南(2024版)》,将生物特征识别标准纳入关键技术标准范畴。生物特征识别标准内容涉及规范生物特征样本处理、生物特征数据协议、设备或系统等技术要求,包括生物特征数据交换格式、接口协议等标准^[24]。

3.2 标准化组织

ISO、ITU-T、3GPP、ETSI、IEEE、OASIS、W3C、IETF(国际互联网工程任务组)、Liberty Alliance(自由联盟)等众多国际或区域标准化组织都致力于统一可信数字身份认证研究^[25]。ISO/IEC JTC 1/SC 27(信息安全、网络安全和隐私保护分技术委员会)以及ISO/IEC JTC 1/SC 37(生物特征识别标准化分技术委员会)在积极开展生物特征识别身份认证安全相关标准化工作^[15]。此外,ITU-TSG 17(安全标准研究组)、ICAO(国际民用航空组织)和ILO(国际劳工组织)也从事着与生物特征相关的国际标准化工作^[26]。

ISO/IEC JTC 1/SC 27负责网络安全国际标准制定,在人脸识别数据安全等生物特征数据安全标准化方面,推动了通用框架、安全技术、安全管理、应用实施等相关标准的研制。通用框架类标准从生物特征数据安全保护与系统安全等方面给出了参考架构。安全技术类标准从生物特征数据安全和隐私保护技术等角度给出了去标识化、匿名化等技术规范。安全管理类标准从组织机构运营管理角度,以信息安全管理体系为基础,重点面向个人可识别信息提出安全管理与保障措施。应用实施类标准重点从隐私保护能力建立与工程实施的角度给出了安全实践参考^[16]。

ISO/IEC JTC 1/SC 37负责生物特征识别标准化工作,其主要任务是在不同的生物特征识别应用和系统之间实现互操作和数据交换,从而对生物特征识别相关技术进行标准化。其工作范围为:对与人体相关、支持在不同生物特征识别应用和系统间实现互操作和数据交换的通用生物特征识别技术进行标准化。通用人体生物特征识别标准包括:通用文档框架、生物特征识别应用编程接口、生物特征识别数据交换格式、相关生物特征识别轮廓、生物特征识别技术评估标准的应用、性能测试与报告的相关方法以及司法与社会相关问题^[26]。其工作组设置情况见表1。

ITU-T SG17安全标准工作组下设Q9(远程生物特征识别问题组)和Q10(身份管理架构和机制问题组)。其中,Q9主要关注生物特征识别在电信

系统中的应用标准, Q10主要关注身份管理架构和机制^[16]。

表1 ISO/IEC JTC 1/SC 37工作组设置情况

工作组	名称	负责专业范围
WG 1	生物特征识别术语	负责生物特征识别术语和指南的标准制修订工作
WG 2	生物特征识别技术接口	负责生物特征识别应用程序接口标准的制修订工作
WG 3	生物特征识别数据交换格式	负责生物特征数据交换格式标准的制修订工作。其大力推进可扩展的生物特征数据交换格式标准、呈现攻击检测标准、样本质量相关标准
WG 4	生物特征识别技术实现	负责生物特征识别系统技术实现的标准制修订工作
WG 5	生物特征识别测试和报告	负责生物特征识别测试和应用标准的制修订工作
WG 6	生物特征识别司法和社会活动相关管理	负责生物特征识别与社会司法相关标准的制修订工作

我国可信数字身份相关主要标准化组织见表2。SAC/TC 28/SC 37(全国信息技术标准化技术委员会生物特征识别分技术委员会)负责生物特征识别通用文档框架、应用编程接口、数据交换格式、生物特征识别轮廓、技术评估、性能测试与报告方法等领域的国家标准制修订工作,成立了人脸识别、移动设备生物特征识别等多个工作组,发布了人脸样本质量、人脸图像数据交换格式、移动设备人脸识别等标准。SAC/TC 100/SC 2(全国安全防范报警系统标准化技术委员会人体生物特征识别应用分技术委员会)结合证卡、视频监控、出入口控制、入侵报警等场景下的人脸识别需求,开展相关产品标准、系统标准、测试检验标准和管理标准研究。

此外,中国通信标准化协会(CCSA)所属TC 1互联网与应用工作组重点推进大数据、区块链等新一代信息技术对数字身份技术发展进行赋能,TC 8重点推进移动通信网络与数据安全、融合新兴技术和业务安全,研制了多项身份管理框架、身

份认证、身份安全等方面的标准^[9]。

3.3 标准研制

ISO、ISO/IEC JTC1、ITU发布了涵盖生物特征数据格式、采集、处理、流通、保护、身份识别、身份验证、数字签名、数字身份基础设施建设,以及数字身份在医疗、社会治理等领域应用可信数字身份相关国际标准,推动了可信数字身份跨境或跨境互联、互通、互认。此外,IEEE等标准化组织为满足数字身份产业发展需要,也发布了部分数字身份相关标准。如IEEE P2859《生物特征识别多模态融合标准》、IEEE P7013《人脸自动分析技术的收录与应用标准》等。

美国、欧盟高度重视数字身份标准制定工作。2017年美国国家标准与技术研究院(NIST)发布了《数字身份指南》(SP 800-63-3)系列标准,增加了网络可信数字身份的互操作性^[6]。2024年,NIST发布了新版《数字身份指南》(SP 800-63-4)系列标准,定义了身份验证、注册、身份验证器、管理流程、身份验证协议等各个领域的技术要求,适用于用户通过网络进行身份证明和身份验证^[27-28]。欧盟重视网络应用的可信性和跨境互操作性,制定了可信服务标准,包括支持电子签名的时间戳服务、证书服务、签名生成和验证服务标准等;可信应用服务标准包括应用电子签名注册电子邮件、数据存储、电子发票标准等;可信服务状态列表标准包括可信服务状态、可信服务提供商状态列表等^[3]。

我国已立项在研的可信数字身份相关国家标准主要包括公民身份号码编制、身份信息核验、网络身份认证、标识密码认证、生物特征识别等方面的标准。可信数字身份现行相关国家标准主要包括用户可信身份鉴别、可信计算密码、统一身份认证、个人身份识别、网络用户身份鉴别、公民网络电子身份、数字身份信息服务、个人基本信息分类与代码、生物特征识别应用编程接口、数据交换格式等方面的标准。可信数字身份现行相关行业标准主要包括居民身份网络认证、网络身份服务密码应用、居民身份网络认证、网络电子身份标识eID、网络虚拟身份数据存储与交换、生物特征识别、可信数据服务、隐私计算等方面的标准。与可信数字身

表2 我国可信数字身份相关主要标准化组织

序号	标准化（分）技术委员会编号	标准化（分）技术委员会名称	秘书处所在单位	负责专业范围
1	TC 28	全国信息技术标准化技术委员会	中国电子技术标准化研究院	负责全国信息采集、表示、处理、传输、交换、表述、管理、组织、存储和检索的系统和工具的规范、设计和研制等专业领域标准化工作
2	TC 28/SC 17	卡及身份识别安全设备分技术委员会	中国电子技术标准化研究院	主要负责身份识别和相关文件、卡、安全设备和令牌，以及其在行业间应用和国际交换中使用的相关接口等领域国家标准制修订工作
3	TC 28/SC 37	生物特征识别分技术委员会	中国电子技术标准化研究院	生物特征识别，包括生物特征识别的公共文档框架、应用程序接口、数据交换格式、轮廓、评估准则的应用、性能测试等
4	TC 100	全国安全防范报警系统标准化技术委员会	公安部第一研究所	负责全国安全防范报警系统、产品等专业领域标准化工作
5	TC 100/SC 2	人体生物特征识别应用分技术委员会	公安部第一研究所	负责安全防范报警系统中以人体生物特征识别应用为主要内容的产品、应用系统以及测试检验等领域标准化工作
6	TC 218	全国防伪标准化技术委员会	中国防伪行业协会	负责全国防伪等专业领域标准化工作
7	TC 260	全国网络安全标准化技术委员会	中国电子技术标准化研究院	负责网络安全技术、机制、服务、管理、评估等领域国家标准制修订工作
8	TC 470/SC 3	组织机构代码统一社会信用代码分技术委员会	全国组织机构代码统一社会信用代码数据服务中心	负责统一社会信用代码基础、数据规范、应用服务等领域国家标准的制修订工作
9	TC 485	全国通信标准化技术委员会	中国通信标准化协会	负责专业范围为通信网络、系统和设备的性能要求、通信基本协议和相关测试方法等
10	TC 590	全国区块链和分布式记账技术标准化技术委员会	中国电子技术标准化研究院	区块链和分布式记账技术领域基础标准、业务和应用标准、过程和方法标准、可信和互操作标准、信息安全标准等
11	TC 609	全国数据标准化技术委员会	中国电子技术标准化研究院	主要负责数据资源、数据技术、数据流通、智慧城市、数字化转型等基础通用标准，支撑数据流通利用的数据基础设施标准，以及保障数据流通利用的安全标准等
12	—	密码行业标准化技术委员会	中国密码学会	主要从事密码技术、产品、系统和管理等方面的标准化工作。下设秘书处和总体、基础、应用、测评四个工作组
13	GATC 4	公安部社会公共安全应用基础标准化技术委员会	公安部第一研究所	社会公共安全行业内新技术、新标准领域及跨技术领域、跨部门、跨警种的公用性国家标准和公安行业标准

份直接相关的地方标准主要集中在身份认证平台接入、身份核验系统一卡通、身份识别电子标签、跨境贸易电子认证服务、生物特征识别应用等方面。已发布可信数字身份相关团体标准涉及内容主要

要包括可信计算技术、可信数字身份服务、身份数据治理、跨境身份认证、个人身份认证服务、企业身份识别编码、艺术品数字身份编码、跨平台接入与身份验证技术、声纹识别、区块链数字身份框

架、基于区块链的元宇宙身份认证、认证签名等。

梳理已发布和已经立项正在研制的可信数字身份相关标准明细表,分析标准体系中存在的空白领域,结合我国可信数字身份发展实践经验、特色亮点和发展需求,提出可信数字身份制修订建议目录,见表3。

3.4 平台建设

暂未见专门的可信数字身份标准信息平台建设报道。我国建设了“公民网络身份识别系统”和“互联网+”可信身份认证平台(CTID平台),并针对上述系统、平台分别制定了标准规范。

“十二五”规划期间,公安部第三研究所承担国家“863”计划中的信息安全重大专项,开展数字身份eID技术研究。2010年,建成了全国“公民网络身份识别系统”,已于2011年投入正式运行。2014年,公安部第三研究所正式开启eID实施战略框架,与eID登记/发行机构、eID运营/服务机构开展合作,推进eID的产业化^[3]。eID载体可使用通用eID,嵌入银行IC智能卡、社保卡、市民卡等中,或者USB Key中。载体还可扩展到可穿戴智能设备,如智能手表、智能手环等。2018年,eID载体进一步扩大到具有安全元件的手机SIM卡,或者手机贴膜卡SIMeID^[3]。

2018年10月,公安部第三研究所针对网络电子身份标识eID的推广应用需求牵头制定国家标准GB/T 36629—2018《信息安全技术 公民网络电子身份标识安全技术要求》和GB/T 36632—2018《信息安全技术 公民网络电子身份标识格式规范》。这些标准已于2019年5月1日正式实施。此外,公安部第三研究所还牵头制定了一系列eID通信行业标准,见表4。

为推进并规范国家网络身份认证公共服务建设应用,加快实施网络可信身份战略,在中央网信办、国家发改委和科技部的支持指导下,在公安部领导下组织建设“互联网+”可信身份认证平台(CTID平台),为各行业提供安全、可信、便捷、权威的网络身份认证服务。CTID平台采用高性能、高并发的系统架构,统筹兼顾系统的先进性、安全性、稳定性、高效性和可扩展性,实现了海量身份

表3 可信数字身份相关标准制修订建议目录

序号	标准名称
1	智能终端生物特征识别身份鉴别 技术要求
2	智能终端生物特征识别身份鉴别 应用指南
3	智能终端生物特征识别身份鉴别 安全评估
4	智能终端生物特征识别身份鉴别 风险防控指南
5	数字身份体系“端-网-云-平台”一体化综合纵深防御指南
6	数字身份认证追溯指南
7	可信数字身份跨域无缝认证与接入技术规范
8	可信数字身份泛在验证技术要求
9	数字钱包身份验证技术规范
10	数字身份协议技术要求
11	数字身份电子凭证互操作性技术要求
12	数字身份数据分级分类指南
13	数字身份全生命周期管理指南
14	数字身份数据授权运营指南
15	数字身份大数据算法应用指南
16	数字身份多信任级认证服务指南
17	Web3.0数字身份应用指南
18	智能体通信网络数字身份应用指南

证数据的分域存储和脱敏应用^[29]。官方客户端“网络身份认证App(试点版)”已于2023年7月初在国内各大手机应用商店上架。通过该App,用户可以使用网络身份认证公共服务,可在不暴露公民身份信息的前提下核实、验证公民真实身份,登记公民身份。

针对CTID平台建设运营,公安部第一研究所等单位提出了网络可信身份认证标准体系^[29],并牵头制定了CTID相关标准。2020年7月,公安部发布了由公安部第一研究所牵头制定的《居民身份网络认证》系列公安行业推荐标准,内容涵盖了术语、整体技术框架、网络可信凭证和网络标识格式要求、认证服务、信息采集设备等^[3],见表5。公安部第一研究所牵头制定的国家标准《信息安全技术 居民身份网络认证服务接口要求》正在审查过程中。

统一的标准规范对于构建安全、便捷的居民身份网络认证技术体系十分重要。但我国当前同时存

表4 网络电子身份标识相关国家标准和行业标准

序号	标准号/计划号	标准名称
1	GB/T 36629.1—2018	信息安全技术 公民网络电子身份标识安全技术要求 第1部分：读写机具安全技术要求
2	GB/T 36629.2—2018	信息安全技术 公民网络电子身份标识安全技术要求 第2部分：载体安全技术要求
3	GB/T 36629.3—2018	信息安全技术 公民网络电子身份标识安全技术要求 第3部分：验证服务消息及其处理规则
4	GB/T 36632—2018	信息安全技术 公民网络电子身份标识格式规范
5	YD/T 3150—2016	网络电子身份标识eID验证服务接口技术要求
6	YD/T 3151—2016	网络电子身份标识eID桌面应用接口技术要求
7	YD/T 3152—2016	网络电子身份标识eID移动应用接口技术要求
8	YD/T 3154—2016	网络电子身份标识eID验证服务接口测试方法
9	YD/T 3155—2016	网络电子身份标识eID移动应用接口测试方法
10	YD/T 3156—2016	网络电子身份标识eID桌面应用接口测试方法
11	YD/T 3203—2016	网络电子身份标识eID术语和定义
12	YD/T 3204—2016	网络电子身份标识eID体系架构
13	YD/T 3205—2016	网络电子身份标识eID的审计追溯技术框架
14	YD/T 3206—2016	网络电子身份标识eID的审计追溯接口技术要求
15	YD/T 3453—2019	基于eID的多级数字身份管理技术参考框架
16	YD/T 3454—2019	加载eID的多应用智能卡安全技术要求
17	YD/T 3455—2019	基于eID的属性证明规范
18	YD/T 3456—2019	网络电子身份标识eID载体安全技术要求

表5 可信身份认证平台（CTID平台）相关国家标准和行业标准

序号	标准号/计划号	标准名称
1	GA/T 1721—2020	居民身份网络认证 通用术语
2	GA/T 1722—2020	居民身份网络认证 整体技术框架
3	GA/T 1723.1—2020	居民身份网络认证 认证服务 第1部分：认证分级
4	GA/T 1723.2—2020	居民身份网络认证 认证服务 第2部分：服务接口要求
5	GA/T 1723.3—2020	居民身份网络认证 认证服务 第3部分：信息获取控件接口要求
6	GA/T 1723.4—2020	居民身份网络认证 认证服务 第4部分：人脸图像采集控件技术要求
7	GA/T 1723.5—2020	居民身份网络认证 认证服务 第5部分：人脸比对引擎接口要求
8	GA/T 1724—2020	居民身份网络认证 网络可信凭证和网络标识格式要求
9	GA/T 1725.1—2020	居民身份网络认证 信息采集设备 第1部分：居民身份证开通网证读卡器
10	GA/T 1725.2—2020	居民身份网络认证 信息采集设备 第2部分：自助开通网证设备
11	GA/T 1725.3—2020	居民身份网络认证 信息采集设备 第3部分：批量开通网证设备
12	GA/T 1725.4—2020	居民身份网络认证 信息采集设备 第4部分：移动终端安全技术要求
13	20213515-T-312	信息安全技术 居民身份网络认证服务接口要求

在上述两套不同的身份认证体系(平台),上述标准都由特定方案研发者围绕上述两套不同身份认证体系各自的技术方案制定,不利于数字身份的推广与普及。要提高认证及管理能力,推进我国数字身份普及应用,需要研制一套能够整合打通两种方案的标准规范。

4 可信数字身份标准化存在的问题

可信数字身份标准化工作取得了丰硕成果,但也面临着一些问题。一是数字身份互联互通标准化工作有待加强。各数字身份协议在数据结构、接口设计、交互流程上不统一,在通信协议、数据存储、交互步骤、安全控制等环节的互通、互认、互验有待强化。二是数字身份在行业和领域,尤其是跨行业、跨领域的应用标准化工作有待加强。公共服务、社会治理、金融、医疗等各行业在应用数字身份时,对参与角色的权利、安全等级、可用性、技术指标要求不同,针对行业特定需求标准有待研制。

5 可信数字身份标准化对策建议

5.1 完善可信数字身份标准化政策措施和工作机制

一是完善可信数字身份标准化政策体系。根据需出台可信数字身份创新发展指导意见、促进可信数字身份发展规划、可信数字身份标准化工作实施方案等政策文件或促进可信数字身份标准化工作写入相关综合性标准化政策文件。在这些政策文件中突出标准引领和标准化工作对可信数字身份发展的促进作用,注重政策与标准的有效衔接。二是建立可信数字身份标准化工作机制。可根据需要成立相应层级的可信数字身份标准化工作领导小组,协调推进可信数字身份标准化工作。鼓励可信数字身份相关企事业单位工作人员积极加入ISO/IEC JTC 1/SC 27、ISO/IEC JTC 1/SC 37、ITU-T SG 17下属的Q 9和Q 10、SAC/TC 28/SC 37、SAC/TC100/SC 2、TC 590、TC 609、GATC 4等可信数字身份相关标准化组织,参与其标准化活动。鼓励各地、各行业根据需要成立特定领域的可信数字身份标准化工作组织,以开展相关标准化活动和制

修订相关缺失标准。鼓励引导数字身份、生物特征识别等相关标准化组织、社会团体、企业、科研机构协同开展可信数字身份标准化工作。

5.2 建立健全可信数字身份标准体系

加强可信数字身份标准体系建设工作,做好标准化顶层规划。根据可信数字身份发展政策导向和实际需求,依托相关标准化组织、研究机构和企业,结合可信数字身份发展现状、特点和趋势做好标准化顶层设计。在充分吸取国际经验的基础上,利用我国以居民身份证为代表的国家法定基础身份证件和国际标准的机读旅行证件等重要资源,创新应用人工智能、网络安全、数据保护等新一代信息技术,建立完善可信数字身份标准体系。为可信数字身份标准化工作奠定基础,规划蓝图,确定主要范围和重点领域,为标准制修订计划提供依据。征集可信数字身份标准制修订项目,形成标准制修订建议目录并动态更新。为构建身份可信、安全友好、行为可溯、监管可达的可信数字身份体系和满足市场需求的可信数字身份技术解决方案提供标准化技术支撑。

5.3 开展可信数字身份标准化研究和标准研制

加强可信数字身份标准化研究,及时将研究成果转化为技术标准。一是制定更加完善的数字身份隐私保护、互操作性、互联互通、全生命周期管理标准,推动可信数字身份跨域或跨境互联、互通、互认。开展隐私计算、联盟链、分布式账本等可信存证技术标准化研究,提高用户可信数字身份凭证的通用性和扩展性。建立数字身份协议技术要求标准,规范数字身份协议数据结构、接口设计、交互流程、数据存储、交互步骤、安全控制等事项,促进数字身份协议之间互通、互认、互验。二是健全可信数字身份认证标准。研制多信任级数字身份认证服务标准,研制满足不同层次、不同安全等级需求的身份认证标准。加强对不同类型实体的电子凭证标准化研究,研制电子凭证互操作性、基于可信环境或安全芯片的电子凭证相关标准。开展数字钱包身份验证标准化工作,形成共识标准。三是加强可信数字身份数据安全相关标准研制。开展可信数字身份相关数据安全技术研发、

安全产品开发、安全测试、安全风险评估、安全能力成熟度评估、应用安全性评估等标准化研究和标准研制工作。面向金融、安防、医疗、交通等重点行业,提出各行业生物特征识别等数字身份识别数据采集精度、数据存储周期、身份认证模式等方面的安全标准要求。四是加强可信数字身份测试类标准研发,完善公共测试平台。推动建立可信数字身份产品的功能性能、可靠性和兼容性测试平台,以及产品的标准符合性测试平台、标准验证点。五是开展可信数字身份技术创新应用安全风险分析与标准化前瞻研究。基于新一代移动通信网络、人工智能技术,开展可信数字身份跨域无缝认证与接入标准化研究。开展Web3.0、智能体通信网络等数字身份新兴应用场景标准化研究,以满足日益增长的数据流通和信息通信需求。研制智能终端生物特征识别身份鉴别技术要求、应用、安全评估、风险防控等方面的标准。六是加强可信数字身份数据应用标准化研究。研制可信数字身份数据挖掘相关算法、平台和框架标准,数据转换和清洗标准,数据分级、分类和授权运营管理标准。

5.4 加强可信数字身份标准实施应用

结合数字中国建设、数字化转型工作,积极开展可信数字身份标准化试点示范,加大可信数字身份相关标准的宣贯、培训、实施力度。聚焦公共服务、社会治理、金融、医疗、安防、交通等重要行

业、重点领域典型场景,拓展可信数字身份应用场景,促进可信数字身份应用落地。激发经营主体标准、用标准的活力,发挥市场机制和企业主体作用,推动可信数字身份标准研究、编制、优化、验证、检测、评估、认证、溯源一体化发展。鼓励可信数字身份相关企业制定实施严于国家标准、行业标准、地方标准的可信数字身份相关团体标准、企业标准。编制可信数字身份标准应用示范案例及标准化白皮书,跟踪国内外可信数字身份应用发展趋势和标准化发展趋势,及时修订白皮书主要内容。

5.5 加强可信数字身份国际标准化工作

加强可信数字身份国际标准化工作,提升我国相关企业在国际上的竞争力和话语权。基于我国可信数字身份领域的技术优势和丰富的应用场景,总结形成具有我国特色的可信数字身份标准化成果,深度参与相关国际标准化工作。一是跟踪研究国际国外数字身份相关政策法规和标准研制进展,引进实施国际先进的可信数字身份标准化成果,根据需要有选择有步骤地将相关国际标准转化为国家标准,补充完善我国可信数字身份标准体系;二是发挥我国参与国际标准化工作的交流机制,鼓励可信数字身份相关企业积极向ISO、ISO/IEC JTC1、ITU-T等重要标准化组织贡献国际标准提案,促进我国可信数字身份相关标准与国际标准互联互通,共同构建安全、开放、互信的技术生态。

参考文献

- [1] TECHNIQUES T S. It security and privacy : a framework for identity management part 1: terminology and concepts: ISO/IEC 24760-1:2019[S/OL], 2019: 1.
- [2] 中国通信技术标准协会.身份管理(IdM)术语: YD/T 2592-2013[S].北京:人民邮电出版社,2013:6.
- [3] 冀俊峰.数字身份:元宇宙时代的智能通行证[M].北京:中国人民大学出版社,2023:102.
- [4] 全国信息安全标准化技术委员会.信息安全技术 鉴别与授权 数字身份信息服务框架规范:GB/T 31504—2015[S].北京:中国标准出版社,2019:1.
- [5] 王妮娜,杨帆,桑杰,等.国内外分布式数字身份建设研究[J].信息安全研究,2023(10):993-1000.
- [6] 于锐.各国数字身份建设情况及我国可信数字身份发展路径[J].信息安全研究,2022(9):858-862.
- [7] 中国移动通信研究院(中移智库),中国移动金融科技有限公司,中国信息通信研究院,等.构建可信数字身份体系筑牢数字文明基石白皮书(2024年)[EB/OL].搜狐.(2024-06-24)[2024-10-30].https://www.sohu.com/a/788115207_120359514.
- [8] 张亚宁,卢细梅,平庆瑞,等.DIDA白皮书[EB/OL].分布式数字身份产业联盟官网. (2024-08-01)[2024-10-02]. <https://dl.brop.cn/wechat/DIDA/DIDA%E7%99%BD%E7%9A%AE%E4%B9%A6.pdf>.
- [9] CCSATC603数字信任技术标准推进委员会.未来网络支

- 撑下的数字身份体系:产业和技术发展趋势(2024年)[EB/OL].(2024-09-14)[2024-10-12].https://mp.weixin.qq.com/s?__biz=MzU1Mzc4NTE1Nw==&mid=2247497228&idx=1&sn=d0f942cbc3ee63c5f371f901e9cc05d1&chksm=fab0c4e217838f42cf227096407fefba4b5df02a0b2527a6e9e309c03252c7ef1d2405e4f605&scene=27.
- [10] 岳林.个人信息的身分识别标准[J].上海大学学报(社会科学版).2017,34(6):28-41.
- [11] 苏宇,高文英.个人信息的身分识别标准:源流、实践与反思[J].交大法学,2019(4):54-71.
- [12] 谢宗晓,龚喜杰.身份与访问管理(IAM)及其国际标准简析[J].中国质量与标准导报,2019(10):14-17.
- [13] 李俊,柴海新,沈明峰,等.可信生物特征识别身份鉴别协议框架标准实践[J].信息技术与标准化,2021(3):38-40.
- [14] 林冠辰,张楚,彭晋,等.移动智能终端生物特征识别可信身份鉴别标准应用[J].信息技术与标准化,2022(5):41-44.
- [15] 孙曦,冯春培,落红卫.移动设备生物特征识别身份认证安全框架国际标准提案研究[J].信息技术与标准化,2018(5):24-27.
- [16] 姚相振,上官晓丽,郝春亮,等.人脸识别数据安全标准化研究报告(2021版)[EB/OL].(2024-11-02). <http://www.cesi.cn/images/editor/20211227/20211227165553392.pdf>.
- [17] 宋宇航.基于SPARK技术的网络虚拟身份数据挖掘[D].北京:北京邮电大学,2017.
- [18] 周瑞,鲁翔,赵浩森,等.基于情景感知与数据挖掘的互联网身份认证机制与关键技术研究[EB/OL].(2024-11-01). https://kns.cnki.net/kcms2/article/abstract?v=SQNd6s98mAyNpuChC-Dc_ceomItLTveYmr7uwCh3iyeMD8wk1LKpbc3uuWeUYggIxhOluOFAPoccoD33YUAmjkWZYfYufIFjXb4FwjT2eE72h8MlSaB_t0cz3NzY1lWuMqh2oXyYCOTi_nWfoAlHNsJJJo6nI4tEm11DuqRenlFncLLenn0dQo2u-ChIa20R&uniplatform=NZKP.
- [19] 黄润飞,陈贤明,黄燕玲,等.基于身份标识和区块链技术的粤港澳大湾区法人及其他组织跨境身份认证应用研究[J].标准科学,2023(8):53-57.
- [20] 黄炜.基于数据挖掘的学习者身份识别[D].杭州:杭州电子科技大学,2011.
- [21] 全国人民代表大会及其常务委员会.中华人民共和国个人信息保护法[EB/OL].(2021-08-20)[2024-11-04].https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.
- [22] 国家标准化管理委员会,中央网信办,科技部,等.关于印发《“十四五”推动高质量发展的国家标准体系建设规划》的通知[EB/OL].(2021-12-06)[2024-11-02]. https://www.sac.gov.cn/xxgk/zcwj/art/2021/art_51ab9411394a44d78985f6f5efdc80a7.html.
- [23] 国家标准化管理委员会,中央网信办,工业和信息化部,等.关于印发《关于实施公共安全标准化筑底工程的指导意见》的通知[EB/OL].(2024-05-17)[2024-11-02]. https://www.gov.cn/zhengce/zhengceku/202406/content_6956115.htm.
- [24] 工业和信息化部,中央网络安全和信息化委员会办公室,国家发展和改革委员会,等.工业和信息化部中央网络安全和信息化委员会办公室国家发展和改革委员会 国家标准化管理委员会关于印发国家人工智能产业综合标准化体系建设指南(2024版)的通知[EB/OL].(2024-06-05)[2024-11-02]. https://www.gov.cn/zhengce/zhengceku/202407/content_6960720.htm.
- [25] 孙韩林,刘建华.公众网络统一身份认证服务及标准研究[J].电信科学,2013,29(2):84-88.
- [26] 中国电子技术标准化研究院,全国信息技术标准化技术委员会生物特征识别分技术委员会.生物特征识别技术与标准化研究报告(2023)[EB/OL].(2024-04-03)[2024-11-02]. <https://www.cesi.cn/cesi/202404/9835.html>.
- [27] National Institute of Standards Technology. NIST SP 800-63-4: digital identity guidelines[EB/OL].(2024-07-31)[2024-10-19]. <https://src.nist.gov/News/2024/nist-sp-800-63-4-2pd-digital-identity-guidelines>.
- [28] TEMOSHOK D, PROUD-MADRUGA D, YEE-YIN C, et al. NIST SP 800-63-4 second public draft, Digital Identity Guidelines[EB/OL]. [2024-10-19]. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.2pd.pdf>.
- [29] 北京中盾安信科技发展有限公司. CTID平台可信赋能 构建数字身份生态[EB/OL].(2024-11-12). <https://www.anicert.cn/platform.html?md=1>.