

行业洞察

2025年

中国身份认证行业研究

从安全到信任，解码千亿级数字身份新赛道？

企业标签：CFCA

China Identity Verification Industry

中国デジタル本人認証産業

报告提供的任何内容（包括但不限于数据、文字、图表、图像等）均系头豹研究院独有的高度机密性文件（在报告中另行标明出处者除外）。未经头豹研究院事先书面许可，任何人不得以任何方式擅自复制、再造、传播、出版、引用、改编、汇编本报告内容，若有违反上述约定的行为发生，头豹研究院保留采取法律措施、追究相关人员责任的权利。头豹研究院开展的所有商业活动均使用“头豹研究院”或“头豹”的商号、商标，头豹研究院无任何前述名称之外的其他分支机构，也未授权或聘用其他任何第三方代表头豹研究院开展商业活动。

研究框架

◆ 全球及中国身份认证行业概况	-----	3
• 身份认证概念与分类	-----	3
• 核验技术分类	-----	4
• 技术原理	-----	5
• 应用场景及客户群体	-----	6
• 应用场景需求特征	-----	7
• 主要参与者	-----	8
◆ 业务合作	-----	9
◆ 方法论及法律声明	-----	10

全球及中国身份认证行业概况——身份认证概念与分类

- 身份认证是验证个人、企业/机构及设备主体所声明身份真实性、合法性和有效性的安全过程，基于权威数据源完成可信身份确认，是身份管理和访问控制的基础能力

身份认证概念与分类

身份认证是验证主体所声称身份的真伪或一致性的安全过程，是身份管理与访问控制的基础能力，其设计与实施必须符合国际标准与国家法规要求。

核验主体分类	定义	认证目标	数据源与验证依据
个人	指通过对个人身份要素（如姓名、身份证号、人脸、手机号等）进行验证，确认其社会身份真实合法性或数字身份一致性。	验证用户在权威数据源中登记的社会真实身份；或验证用户是否与某一数字身份账户绑定一致。	国家居民身份证数据库（公安部居民身份证系统）； 运营商实名制登记库、银联银行卡库； 企业内部注册账户库。
企业/机构	指通过对单位、企业、机构等法人主体的注册信息与法人代表身份进行核验，确认其合法性、注册有效性以及可签约能力。	验证组织是否在权威登记机关合法注册； 验证认证请求方是否为该组织的合法授权代表。	国家企业信用信息公示系统（市场监管总局）； 行业协会或主管部门登记信息； 企业法人四要素（企业名称+统一社会信用代码+法定代表人+法人身份证号）； 电子营业执照。
设备/终端	指通过识别设备的唯一标识或数字指纹，确认其为可信接入设备，常见于物联网（IoT）、智能终端、区块链节点、电子票据等场景中。	确保接入网络的设备是合法注册、可信任的终端； 防止设备伪造、冒用、克隆或篡改。	设备唯一标识符（IMEI、MAC 地址、序列号等）；可信平台模块（TPM）/硬件安全模块（HSM）签发的证书； 区块链登记的设备身份元数据。

来源：专家访谈，企业公告，头豹研究院

全球及中国身份认证行业概况——核验技术分类

- 当前身份认证技术框架分为基于生物特征、要素比对、行为特征和去中心化身份，分别依托主体固有特征、权威登记数据一致性、上下文行为模式和区块链等去中心化信任机制实现安全、可信的身份验证

核验技术分类：生物特征、要素比对、基于行为、去中心化身份（DID）

- 生物特征是指通过采集、提取并比对主体固有的生理或行为特征完成身份认证。 - 代表技术： <u>静态生物特征：人脸识别、指纹识别、虹膜识别、掌纹识别、声纹识别。</u> <u>动态行为生物特征：签名动态轨迹、步态识别、击键节奏。</u>	- 要素比对是通过用户提供的信息与权威登记数据或系统记录的一致性进行比对验证。 - 代表技术： <u>二/三要素实名比对：姓名+身份证号、银行卡号、手机号。</u> <u>数字证书认证（PKI体系）、硬件Token、动态口令（OTP）。</u> <u>短信验证码、一次性链接。</u>
生物特征	要素比对
- 基于行为是指通过分析认证主体的行为模式、上下文环境特征、风险信号完成身份判定。 - 代表技术： <u>设备指纹、浏览器指纹。</u> <u>IP地址、地理位置、时区、登录时间段。</u> <u>用户行为图谱、鼠标轨迹、击键频率。</u>	- DID是指采用去中心化身份标识符（DID）框架和区块链等去中心化信任基础设施实现身份认证。 - 代表技术： <u>DID标识符、公私钥签名认证。</u> <u>DID文档链上存证、零知识证明。</u> <u>去中心化身份网络等实现。</u>
基于行为	DID

■ 当前身份认证体系正经历从中心化向去中心化、从静态验证向动态行为分析的演进过程。四类主流身份验证路径各有侧重：

生物特征类基于人体固有的生理或行为特征（如人脸、虹膜、签名轨迹等），强调“唯一性”和“不可复制性”，适用于高安全性场景。但其部署成本较高，隐私保护要求严格。

要素比对类依赖用户提供的静态信息（如姓名、证件号）与后台系统比对，操作简便但面临伪造与信息泄露风险，故常与双因子认证技术（如OTP、数字证书）组合使用以增强安全性。

基于行为的认证通过分析用户的设备操作轨迹、地理位置、登录时间等行为模式，构建动态识别能力，适用于对抗中间人攻击和账号共享等风控场景，是“无感认证”的重要支撑手段。

去中心化身份（DID）体系则基于区块链等技术构建去中心化信任框架，以可验证凭证（VC）与分布式身份文档（DID Document）实现身份的自治管理和隐私保护，正成为数字身份的未来方向，特别适用于Web3、跨平台认证等新兴场景。

来源：专家访谈，企业公告，头豹研究院

全球及中国身份认证行业概况——技术原理

- 身份认证技术正朝着融合化、安全增强、用户自控方向演进。传统的要素比对已难以应对复杂场景，需与生物识别、行为认证等手段融合，构建多因子认证体系

技术原理

核验技术分类	技术原理
生物特征	生理特征：不可遗忘且难以伪造。 采集 → 特征提取 → 特征模板比对 → 计算相似度 → 判断是否通过。
要素比对	知识型要素：用户知道的秘密信息（如密码、PIN）。 持有型要素：用户持有的安全介质（如手机、动态口令、数字证书）。
基于行为	收集用户行为和上下文信号，计算风险分数，动态决定是否允许访问或触发二次认证。
去中心化身份（DID）	DID 由用户自行生成并持有，记录在区块链等去中心化账本上； 用户对请求进行签名，验证者根据链上DID文档中的公钥验签确认身份。

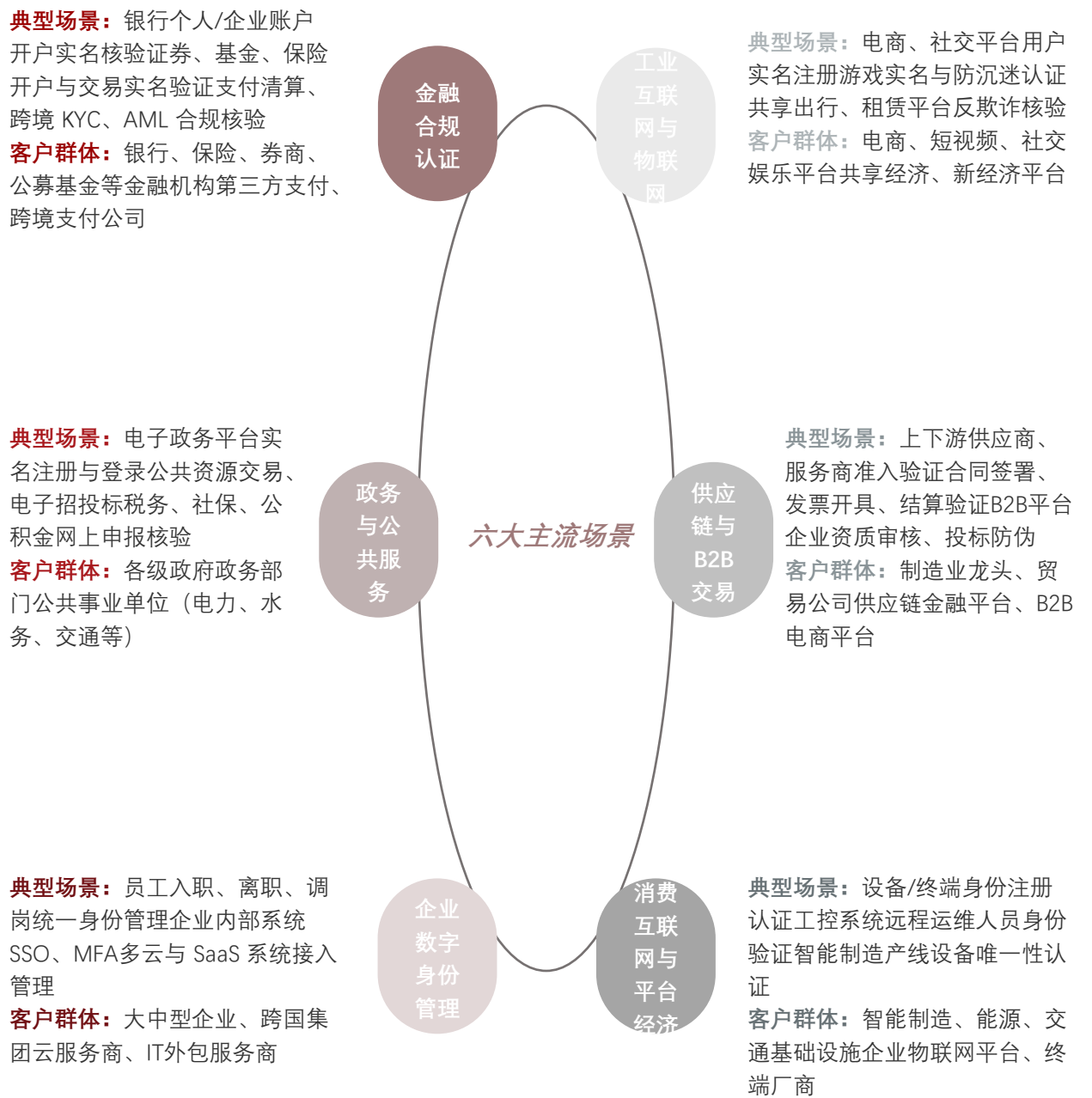
- 生物特征识别技术：以“不可伪造性”构筑第一道生物安全边界生物特征技术（如指纹、面部、虹膜等）因其“唯一性+不可遗忘性+难以伪造”的优势，被广泛用于金融支付、出入境控制、移动终端解锁等场景。其技术路径包括“特征采集 → 特征模板生成 → 模板比对 → 相似度计算 → 决策判断”，本质是统计学相似度问题。尽管安全性较高，但仍存在模板被盗用、攻击面集中等风险，因此往往需结合第二重认证机制（如OTP、PIN等）提升抗攻击能力。
- 要素比对技术：传统认证的主流，向多因子融合演进要素型认证划分为“知识型”（如密码、PIN）与“持有型”（如动态令牌、USB Key、手机SIM等）两类，具备低成本、易部署等优势，但单点依赖性强，易受钓鱼、撞库等攻击。近年来，企业普遍引入多因子认证（MFA）机制，通过跨维度要素组合（如“密码+生物识别”、“手机号+数字证书”）提升整体认证安全等级，已成为数字政务、金融合规与云安全部署的基础要求。
- 基于行为的动态认证：强化连续认证与风控能力行为认证通过收集用户的操作行为（如打字节奏、鼠标轨迹、设备信息）与上下文（如IP、时间、位置信息等），动态评估风险分值并实现隐形认证。这类机制适合在不打扰用户的前提下，进行无感认证与风控拦截，广泛用于电商平台、互联网金融、企业办公系统中，以实现“首次认证+事中风控+事后审计”的闭环管理，体现出身份认证向智能化与风险驱动型演进的趋势。
- 去中心化身份（DID）：构筑以用户为中心的可信身份体系DID通过用户自生成、自持有的身份标识，结合区块链技术实现身份记录上链、防篡改、可验证。验证者通过公钥签名验证身份，无需依赖中心化身份服务提供者，避免“单点泄露”与“信任集中”，更适用于Web3、隐私计算、跨平台身份互信等场景。该技术正在被W3C、EBSI（欧洲区块链服务基础设施）等机构推进标准化，成为未来数字身份治理的关键基础设施。

来源：专家访谈，企业公告，头豹研究院

全球及中国身份认证行业概况——应用场景及客户群体

- 身份认证正从高合规性和权威性场景向广泛、多元化场景延伸，呈现出由“监管驱动”向“业务驱动”“用户体验驱动”并重的演进趋势，行业客户在安全性、灵活性、隐私保护和成本效率之间的权衡成为关键挑战

主流应用场景及客户群体



来源：专家访谈，企业公告，头豹研究院

全球及中国身份认证行业概况——应用场景需求特征

- 身份认证在不同行业场景中呈现出多维需求差异，金融、政务和供应链更侧重权威性、合规性和法律效力，消费互联网和企业数字身份管理更重视高并发、易用性和风险感知，而工业物联网则偏向设备可信与低门槛接入，体现出应用场景驱动下的多元化需求特征

应用场景需求特征分析

	权威性/法律效力	高并发/低延迟	合规性/标准化	隐私保护	风险感知/反欺诈	易用性/低门槛
金融合规认证	★★★★	★★	★★★★	★★	★★★	★★
政务与公共服务	★★★★	★★	★★★★	★★★	★★	★★
企业数字身份管理	★★	★★	★★	★★	★★	★★★★
消费互联网与平台经济	★★★	★★★★	★★	★★	★★★	★★★★
供应链与B2B交易	★★★★	★★	★★★	★★	★★★	★★
工业互联网与物联网	★★	★★★	★★	★★	★★	★★

身份认证的应用需求呈现场景驱动、多维权衡的结构性差异

金融与政务场景对“权威性、合规性与隐私保护”要求最高，是法律效力与标准规范最为严苛的领域；消费互联网与平台经济则更强调“高并发、低延迟与易用性”，认证需兼顾体验与安全；企业数字身份管理场景则呈现“合规+风险控制”并重的均衡需求；而工业物联网与供应链B2B场景的关注点更多聚焦于“可信接入与低门槛部署”，认证需嵌入设备端并具备高度兼容性。

认证体系正在走向“场景分化+技术融合+信任分层”

从横向维度看，身份认证正在从传统“用户-平台”认证模型，转向面向多角色、多对象、多终端的全域可信身份体系建设；从纵向维度看，身份认证需求也呈现出“合规优先→安全增强→用户体验优化”的动态演进轨迹。

未来，领先平台应构建基于以下三大能力的差异化身份认证系统：

- 分行业合规适配能力：应对不同法律环境与监管要求；
- 多因子融合能力：实现“人+设备+行为”的复合认证；
- 身份信任运营能力：支持风险动态调整与数据闭环审计。

来源：专家访谈，企业公告，头豹研究院

全球及中国身份认证行业概况——主要参与者

- 身份认证行业呈现出多层次专业分工格局，由持牌认证机构提供权威合规能力，IDaaS平台满足企业IT统一身份管理，风控与硬件厂商强化风险防御和终端可信，DID创新服务探索自主隐私保护

主要参与者

企业类型	代表企业	优势应用场景	能力特点
持牌权威认证机构	CFCA、中国金融认证中心、北京数字认证（BDO）、上海CA等	金融合规认证 政务与公共服务 供应链招投标	权威性高，司法可采信，接入国家权威数据源，法律效力
IDaaS服务商	阿里云、腾讯云、Okta、Ping Identity等	企业数字身份管理SSO MFA企业IT场景	部署灵活，低成本，快速上线，适应多云和企业内部管理
风控/反欺诈技术厂商	数美科技、同盾科技、百融云创等	消费互联网平台经济 金融交易反欺诈 游戏防作弊	高并发动态分析，行为识别，低门槛用户体验
硬件/嵌入式安全厂商	华大智宝、飞天诚信、TPM模块厂商等	工业互联网 物联网设备认证 智能卡支付终端	提供硬件信任根，保障终端唯一性和设备链可信
DID/区块链创新服务商	Evernym、Sovrin、Ontology（本体）等	Web3 去中心化身份 供应链防伪溯源 隐私保护	用户自主、去中心化、最小化披露，前沿技术探索

- 持牌权威认证机构：**依托国家密钥管理体系和CA体系，提供具备司法可信性与法定效力的数字证书服务，广泛用于金融合规认证、政务服务平台、供应链电子招标等场景，是当前身份认证体系中权威性最高、接入门槛最高的一类主体。
- IDaaS服务商：**提供的“身份即服务（IDaaS）”平台，已成为企业IT统一身份管理与SSO、MFA落地的核心能力支撑。其优势在于部署灵活、低成本、支持多租户和多端统一管理，适配云原生、SaaS化与远程办公等新型IT环境，加速企业身份体系的“平台化迁移”。
- 风控/反欺诈技术厂商：**依托大数据、机器学习与设备指纹等技术，构建行为建模+实时风险分析+反欺诈策略引擎的闭环能力，主要用于消费互联网、金融交易风控、游戏防作弊等高欺诈风险场景，强调高并发下的实时智能拦截能力。
- 嵌入式/硬件安全厂商：**面向工业物联网、智能终端、支付设备等低延迟、强隔离场景，提供硬件级可信根、加密芯片与模块化身份识别方案，是“身份认证前置到设备端”的重要路径。该类厂商注重可信计算、边缘安全与抗物理攻击能力。
- DID/区块链创新服务商：**探索去中心化身份体系的未来路径，正构建基于DID（去中心化标识符）和VC（可验证凭证）的身份架构，强调用户自主管理身份、最小披露原则与跨平台可验证性。其应用场景涵盖Web3生态、链上交易、数据主权保护等，引领身份认证向“去平台化+数据自控”的未来范式演化。

来源：专家访谈，企业公告，头豹研究院

业务合作

会员账号

可阅读全部原创报告和百万数据，提供PC及移动端，方便触达平台内容

定制报告/词条

行企研究多模态搜索引擎及数据库，募投可研、尽调、IRPR等研究咨询

定制白皮书

对产业及细分行业进行现状梳理和趋势洞察，输出全局观深度研究报告

招股书引用

研究覆盖国民经济19+核心产业，内容可授权引用至上市文件、年报

市场地位确认

对客户竞争优势进行评估和证明，助力企业价值提升及品牌影响力传播

行研训练营

依托完善行业研究体系，帮助学生掌握行业研究能力，丰富简历履历

报告作者



袁栩聪
首席分析师



王利华
行业分析师

• service@leadleo.com

业务咨询

- 客服电话：400-072-5588
- 官方网站：www.leadleo.com



商务咨询与深度合作

深圳办公室

广东省深圳市南山区粤海街道华润置地大厦E座4105室

邮编：518057

上海办公室

上海市静安区南京西1717号会德丰国际广场 2701室

邮编：200040

南京办公室

江苏省南京市栖霞区经济开发区兴智科技园B栋401

邮编：210046



头豹 www.leadleo.com
LeadLeo 400-072-5588

方法论

- ◆ 头豹研究院布局中国市场，深入研究19大行业，持续跟踪532个垂直行业的市场变化，已沉淀超过100万行业研究价值数据元素，完成超过1万个独立的研究咨询项目。
- ◆ 研究院依托中国活跃的经济环境，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。
- ◆ 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- ◆ 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- ◆ 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明

- ◆ 本报告著作权归头豹所有，未经书面许可，任何机构或个人不得以任何形式翻版、复刻、发表或引用。若征得头豹同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“头豹研究院”，且不得对本报告进行任何有悖原意的引用、删节或修改。
- ◆ 本报告分析师具有专业研究能力，保证报告数据均来自合法合规渠道，观点产出及数据分析基于分析师对行业的客观理解，本报告不受任何第三方授意或影响。
- ◆ 本报告所涉及的观点或信息仅供参考，不构成任何投资建议。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。在法律许可的情况下，头豹可能会为报告中提及的企业提供或争取提供投融资或咨询等相关服务。本报告所指的公司或投资标的的价值、价格及投资收入可升可跌。
- ◆ 本报告的部分信息来源于公开资料，头豹对该等信息的准确性、完整性或可靠性不做任何保证。本文所载的资料、意见及推测仅反映头豹于发布本报告当日的判断，过往报告中的描述不应作为日后的表现依据。在不同时期，头豹可发出与本文所载资料、意见及推测不一致的报告和文章。头豹不保证本报告所含信息保持在最新状态。同时，头豹对本报告所含信息可在不发出通知的情形下做出修改，读者应当自行关注相应的更新或修改。任何机构或个人应对其利用本报告的数据、分析、研究、部分或者全部内容所进行的一切活动负责并承担该等活动所导致的任何损失或伤害。