ICS 35.240
CCS L 70

中华人民共和国国家标准

GB/T XXXXX—XXXX

数据基础设施 用户身份管理和接入要求

Data infrastructure—User identity management and access requirements

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　　言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 2
5 总体要求 2
5.1 总体架构 2
5.2 管理对象 3
5.3 主要参与方功能 4
6 身份信息构成 5
6.1 概述 5
6.2 接入主体身份信息内容 5
6.3 接入连接器身份信息内容 5
6.4 平台身份信息内容 5
7 身份注册认证流程 6
7.1 接入主体身份注册认证 6
7.2 接入连接器身份注册认证 10
7.3 平台身份注册认证 13
8 接口对接要求 14
8.1 总体架构 15
8.2 接口列表 15
9 管理与安全要求 16
9.1 基本要求 16
9.2 安全措施 17
9.3 记录与审计措施 18
附　录　A　（规范性）　接入主体身份信息 19
A.1 个人用户身份信息 19
A.2 法人或其他组织身份信息 20
A.3 受托执行者身份信息 22
A.4 接入连接器身份信息内容 23
A.5 平台身份信息内容 24
附　录　B　（规范性）　可信身份凭证结构 26
参考文献 27

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。

本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。

本文件起草单位：北京交通大学、北京化工大学、中国联合健康医疗大数据有限责任公司、北京物资学院、蚂蚁科技集团股份有限公司、上海零数众合信息科技有限公司、杭州安恒信息技术股份有限公司、上海数据交易所有限公司、国家信息中心、中国信息通信研究院、中国移动通信集团有限公司、中国电信集团有限公司、中国联合网络通信集团有限公司、北京易华录信息技术股份有限公司、湖南天河国云科技有限公司、北京信息基础设施建设股份有限公司、华北计算技术研究所（中国电子科技集团公司第十五研究所）、公安部第一研究所、中国电子技术标准化研究院、北京数据先行区服务有限公司、北京新材道数智科技有限公司、联通数据智能有限公司、西安电子科技大学、中国移动通信有限公司研究院、中移动信息技术有限公司、蓝象智联（杭州）科技有限公司、华控清交信息科技（北京）有限公司、数据空间研究院、下一代互联网关键技术和评测北京市工程研究中心有限公司、中国科学院信息工程研究所、浪潮云信息技术股份公司、北京泰尔英福科技有限公司、西安市数据局、三六零数字安全科技集团有限公司、中移（杭州）信息技术有限公司、中电数据产业集团、浙江蚂蚁密算科技有限公司、西安交通大学、北京邮电大学、洞见科技（雄安）有限公司。

文件主要起草人：宫大庆、张向宏、刘世峰、张真继、李宾、涂群、张闯、张茜茜、秦源、尚小溥、海楠、韦韬、兰春嘉、陈星、刘圣威、马英、王亦澎、茹志强、张鑫、杨瑞、李杰、谭林、刘斌、刘忠良、张鸿冉、曲薇、国伟、许紫媛、徐泺、石庆华、李慧玲、张芬、任晓明、张帆、王超、靳晨、林传文、刘东、牛犇、张鹏、张发振、孔宪光、李峥、郭锐、昌文婷、杨珍、林明峰、于百程、司宏伟、景越、王军、李冠洲、李锋、李金夏、程宏、刘齐军、李昕龙、廖宇桥、贾宏、刘笑辰、刘健帅、段平霞、谢云龙、伊然、刘少鹏、张旭东、杨倩、刘运强、田伯成、王帅、陈学顺、王晓思、何军权、李隆玉、崔瀚予、王畅畅、胡振泉、耿贵宁、咸静、胡成盛、张辙、崔玲龙、张晓蒙、潘无穷、肖翔、惠维、何帅、孟猛猛、李博、冯新宇

数据基础设施 用户身份管理和接入要求

1 范围

本文件规范了统一用户身份的总体要求、身份信息构成、注册及认证流程、跨平台身份互联互通机制以及相关接口与安全管理要求，旨在保障接入主体、接入连接器及平台的身份可信，支撑数据访问、服务调用和跨域协同的安全开展，以实现用户身份的跨节点互联互通，支撑全网范围内的统一身份管理和明确的职责分工。

本文件适用于数据基础设施中用户身份管理系统的开发、建设、运行和维护，指导数据基础设施涉及的接入主体、接入连接器、平台的用户身份注册认证、核验注销等工作，并兼顾人工智能相关服务场景下的身份管理需求。

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 4754-2017 国民经济行业分类

GB/T 25069 信息安全技术 术语

GB/T 31504 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 35273 信息安全技术 个人信息安全规范

GB/T 42573 信息安全技术 网络身份服务安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

接入连接器 access connector

连接接入主体与接入主体，或连接接入主体与业务节点的规范化软硬件系统，数据供需双方均可通过接入连接器接入数据基础设施。

[来源：20255407-T-907，3.4.19]

3.2

可信身份权威机构 trusted identity authority

存储和管理用户真实身份信息，提供真实身份鉴别服务的机构。由国家指定主管机构担任。

[来源：GB/T 31504-2015，3.12]

3.3

用户授权令牌 user authorization token

用户授权令牌是一个安全且不可预测的加密字符串或数字序列，由系统生成并分配给特定的用户或应用程序，作为在有效期内有效的临时凭证，用于验证用户身份并授权其访问受保护的资源或服务。

3.4

可信身份凭证 trusted identity credential

一种基于数字加密等技术的身份凭证，它允许个人或组织以安全、隐私保护的方式，证明和验证其身份、资格、属性或其他信息。

[来源：20255407-T-907，3.7.4]

3.5

失效身份凭证 invalid credential

指凭据无效或已过期的身份凭证，包括资格、属性或其他信息（扩展）变更导致的身份失效。

[来源：20255407-T-907，3.7.5]

3.6

可信身份凭证提供商 trusted identity credential provider

负责签发、存储和维护可信用户身份凭证的受信任机构。

3.7

访问令牌 access token

由认证服务颁发的短期数字令牌，用于代表用户身份向资源服务器请求授权访问特定资源。

3.8

跨域身份认证 cross-domain identity authentication

在一个已注册重要功能设施完成注册的接入主体，在另一个重要功能设施上使用其身份凭证进行身份认证的过程。

4 缩略语

下列缩略语适用于本文件。

CA：证书认证机构（Certificate Authority）

DID：去中心化身份（Decentralized Identifier）

MAC：媒体存取控制位址（Media Access Control Address）

OTP：一次性口令（One-Time Password）

SN：序列号（Serial Number）

5 总体要求

5.1 总体架构

在数据基础设施的数据流通利用体系中，接入主体通过接入连接器与平台建立连接，发起数据访问或服务请求。接入连接器作为桥梁，负责承载接入主体的身份凭证和访问指令，并将其安全、高效地传递至平台；平台则作为数据流通与服务的提供方，响应接入请求并完成业务交互。三者共同构成了数据接入的核心路径，实现了身份映射、资源调用与服务分发的协同机制。

数据基础设施的用户身份管理与接入体系应支撑各类数据访问、服务调用和跨域协同场景下的可信接入，并满足人工智能相关服务在数据调用、服务协同和跨域互通中的身份管理需求。同时，可利用人工智能技术提升身份核验、状态同步、风险识别、访问控制和运行维护等能力，提高身份管理与接入体系的自动化、智能化和协同化水平。为确保身份管理的可信性和接入操作的安全性，应保障接入主体、接入连接器以及平台在身份认证及管理维度上的可信认证与有效绑定。数据基础设施的用户身份管理与接入的总体架构如图1所示：

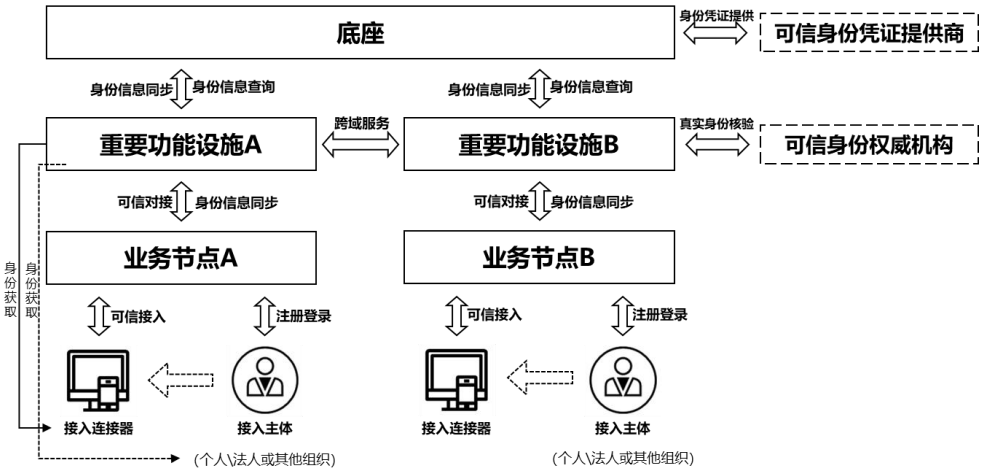

图 1　总体架构

在该架构中：

a) 接入主体可通过业务节点或重要功能设施完成注册流程，获取并应用其在国家数据基础设施内的用户身份；

b) 接入连接器的身份注册应由重要功能设施统一受理和管理，注册成功并取得可信身份凭证后，方可安全接入业务节点或其他相关系统，实现可信接入；

c) 重要功能设施负责对接可信身份权威机构，对接入主体身份进行核验；完成核验后，将身份信息同步至底座，并通过底座申请签发用户身份凭证

d) 底座对接可信身份凭证提供商为接入主体、接入连接器和平台签发用户身份凭证；

e) 平台的接入应由重要功能设施统一管理，确保平台用户身份的有效性和可信性。

f) 对涉及模型服务、推理服务、智能编排、自动化调用等人工智能相关服务的场景，应能够通过接入主体、接入连接器和平台的可信身份体系，支撑其可信接入、合规调用和跨域协同。

5.2　管理对象

5.2.1　概述

数据基础设施用户身份管理包括接入主体、接入连接器与平台三类管理对象，应明确各对象的身份获取流程与管理要求。对于涉及模型服务、推理服务、智能编排、自动化调用等人工智能相关服务的场景，可分别依托接入主体、接入连接器和平台进行身份管理，并在身份信息、注册认证、接口调用和管理要求中体现相关服务属性、责任关系和调用边界。

5.2.2　接入主体

接入主体包括以下三类：

a) 个人用户：指以自然人身份参与数据流通活动的个体；

b) 法人或其他组织用户：指具备独立法人地位或组织资格的单位，包括但不限于政府机关、企事业单位、社会团体等；

c) 受托执行者：指经个人、法人或其他组织授权，代表其发起数据访问、服务调用或其他数据流通利用相关操作的执行主体。受托执行者可以是自然人，也可以是经授权的应用程序、智能体或其他自动化执行单元；其中，法人或其他组织授权的自然人受托执行者可称为经办人。

接入主体应向业务节点或重要功能设施提交用户身份注册申请。重要功能设施应对接可信身份权威机构完成对接入主体的身份信息核验。完成核验后重要功能设施将身份信息同步至底座，并向底座申请签发用户身份凭证，底座对接可信身份凭证提供商为接入主体签发用户身份凭证。

5.2.3 接入连接器

接入连接器指连接接入主体与接入主体或接入主体与业务节点的规范化软硬件系统，应向重要功能设施申请注册/接入，由重要功能设施审核，并通过底座完成可信身份凭证颁发。其他系统与接入连接器进行服务互通时，可基于接入连接器的可信身份凭证验证其身份有效性。在涉及人工智能相关服务场景时，接入连接器可作为自动化调用、服务转接和跨节点协同的接入载体。

5.2.4 平台

平台指各种业务节点对应的数据流通利用系统，应向重要功能设施申请注册/接入，由重要功能设施审核，并通过底座完成可信身份凭证颁发。在涉及人工智能相关服务场景时，平台可作为模型服务、推理服务、智能编排、智能分析或其他相关能力的承载载体。其他系统与平台进行服务互通时，可基于平台的可信身份凭证验证其身份有效性。

5.3 主要参与方功能

5.3.1 底座

底座承担以下功能：

a) 汇聚并管理全国范围内的可信身份信息资源，提供统一的身份信息查询服务；
b) 建立并维护数据基础设施体系内的可信身份凭证提供商的权威清单，为各级节点提供标准化对接依据；
c) 对接可信身份凭证提供商，为符合条件的接入主体、接入连接器和平台签发可信身份凭证。

5.3.2 重要功能设施

重要功能设施承担以下功能：

a) 面向本区域或本行业提供统一的身份管理与身份认证服务，支持接入主体、接入连接器及平台的身份注册与身份认证；
b) 对接可信身份权威机构，对自然人、法人或其他组织身份进行核验；
c) 对接底座，实现可信身份凭证的签发和管理，并将身份基础信息同步至底座；
d) 依托可信身份凭证，与底座、重要基础设施或业务节点建立互信链，实现多方身份可信互认与联动调用；
e) 提供跨域身份信息查询服务，支持完成跨域身份互认所需的必要身份信息查询；
f) 支持面向人工智能相关服务场景的身份管理与协同调用需求，为自动化调用、服务编排和跨域协同提供身份支撑。

5.3.3 业务节点

业务节点宜承担以下功能：

a) 以嵌套或调取接口等方式代理重要功能设施面向参与数据流通利用的企业/个人提供接入主体身份注册，面向接入连接器提供注册；
b) 基于可信身份凭证，支持与其他重要功能设施、业务节点的跨系统身份可信互认；
c) 基于可信身份凭证，实现与接入连接器之间的身份互认，保障系统间访问请求的可信来源；

d) 支持数据访问、服务调用和人工智能相关服务场景下的身份校验、关系识别和调用衔接。

6 身份信息构成

6.1 概述

在数据基础设施中，身份信息应进行统一结构描述，以支撑统一、可信、可追溯的身份识别和互认机制。身份信息一般由以下两部分组成：

a) 基础信息：一个确定的身份应具备的基础数据信息，用于身份互认，是身份认证、授权和追踪的基础。

b) 附属信息：用于补充说明或增强身份对象业务属性、服务属性、授权关系和管理属性的辅助性信息，有助于减少在多平台环境中重复信息录入，提升身份服务一致性、管理精细化水平和跨域协同能力。

6.2 接入主体身份信息内容

6.2.1 个人身份信息

个人用户身份信息用于唯一识别和标识特定个人用户的信息集合，包含姓名、证件类型、证件号码、手机号等信息。为确保跨系统互操作与隐私合规性，按“最小化、必要化”原则采集及处理，基础信息与附属信息进行分别维护，便于分级授权与数据最小化处理，证件号码、证件有效期起始日期、证件有效期截止日期、手机号等个人信息在完成身份认证后不留存。个人用户身份信息的基础信息与附属信息详细内容见附录A.1。

6.2.2 法人或其他组织身份信息

法人或其他组织身份信息包含法人或其他组织名称、统一社会信用代码、法定代表人或负责人等信息。法人身份信息主要用于确认组织在法律框架下的合法性和身份。基础信息与附属信息详细内容见附录A.2。

6.2.3 受托执行者身份信息

受托执行者身份信息用于标识经个人、法人或其他组织授权，代表其发起数据访问、服务调用或其他数据流通利用相关操作的执行主体。受托执行者可以是自然人，也可以是经授权的应用程序、智能体或其他自动化执行单元；其中，法人或其他组织授权的自然人受托执行者可称为经办人。

受托执行者身份信息应能够体现其与责任主体之间的授权关系和绑定关系。自然人受托执行者身份信息可包含姓名、证件号码、责任主体名称等信息；非自然人受托执行者身份信息可包含执行者标识、所属责任主体标识、授权类型等信息。基础信息与附属信息详细内容见附录A.3。

6.3 接入连接器身份信息内容

接入连接器身份信息用于识别具备用户身份服务功能的设备或系统组件。其唯一标识由重要功能设施下发，需绑定其网络访问信息（IP、域名）和部署实体的组织信息。在涉及人工智能相关服务的场景中，接入连接器身份信息还可用于标识其作为自动化调用、服务转接和跨节点协同接入载体的相关属性。接入连接器身份信息包括基础信息与附属信息，详细内容见附录A.4。

6.4 平台身份信息内容

平台身份信息包含平台名称、平台身份标识、所属法人或其他组织名称等。在涉及人工智能相关服务的场景中，平台身份信息还可用于标识其作为模型服务、推理服务、智能编排、智能分析或其他相关能力承载载体的服务属性。基础信息与附属信息详细内容见附录A.5。

7 身份注册认证流程

7.1 接入主体身份注册认证

7.1.1 用户身份注册

7.1.1.1 个人/法人或其他组织身份注册

个人/法人或其他组织进行身份注册流程见下图：

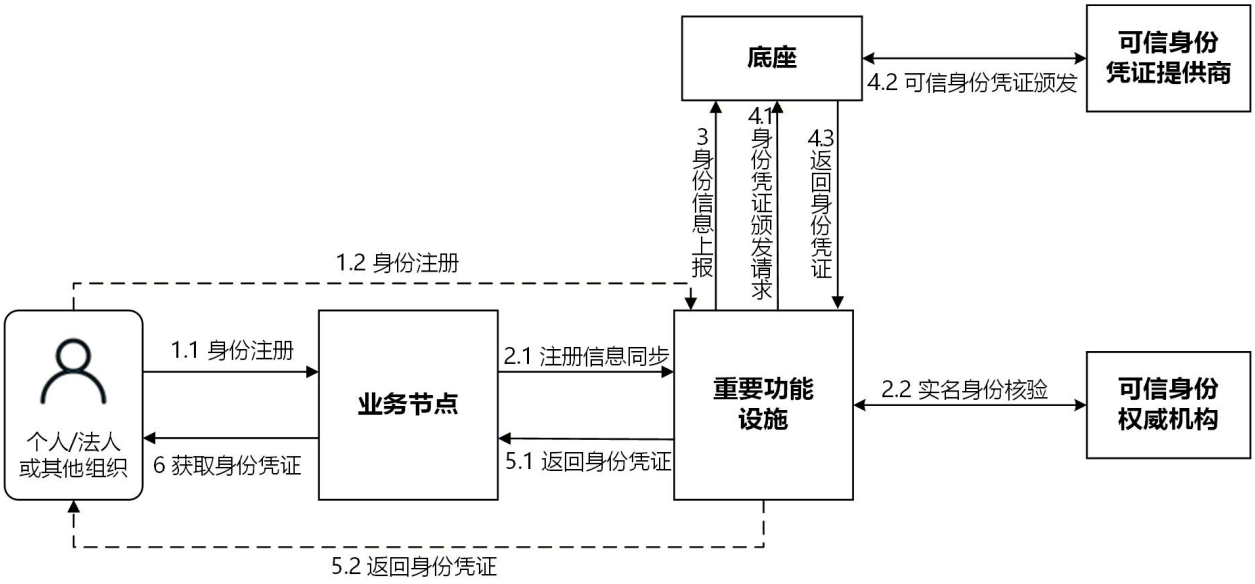

图 2 用户身份注册流程

流程说明：

a) 注册申请：个人/法人或其他组织在业务节点或重要功能设施发起身份注册，并按照实名认证要求提交身份核验材料；

b) 信息同步：如在业务节点发起注册，业务节点将注册信息同步至对应的重要功能设施，重要功能设施向可信身份权威机构申请身份核验，获取核验结果；

c) 凭证签发：完成核验后重要功能设施将身份信息同步至底座，并向底座申请签发用户身份凭证，底座对接可信身份凭证提供商签发可信身份凭证；

d) 注册完成：可信身份凭证返回至重要功能设施，由重要功能设施下发至业务节点或直接向用户反馈注册结果，完成身份注册。

已完成身份注册的个人、法人或其他组织，可根据业务需要授权受托执行者代其发起数据访问、服务调用或跨域协同，相关登记要求见7.1.1.2。

7.1.1.2 受托执行者登记

当个人、法人或其他组织授权受托执行者代其参与数据流通利用活动、发起数据访问、服务调用或跨域协同时，应进行受托执行者登记。受托执行者可以是自然人，也可以是经授权的应用程序、智能体或其他自动化执行单元；其中，法人或其他组织授权的自然人受托执行者可称为经办人。

受托执行者登记应基于已完成注册的个人、法人或其他组织身份开展，并应体现责任主体与受托执行者之间的授权关系。完成登记后，受托执行者方可在授权范围内代理开展相关业务活动。

7.1.2 用户身份变更

7.1.2.1 个人/法人或其他组织身份变更

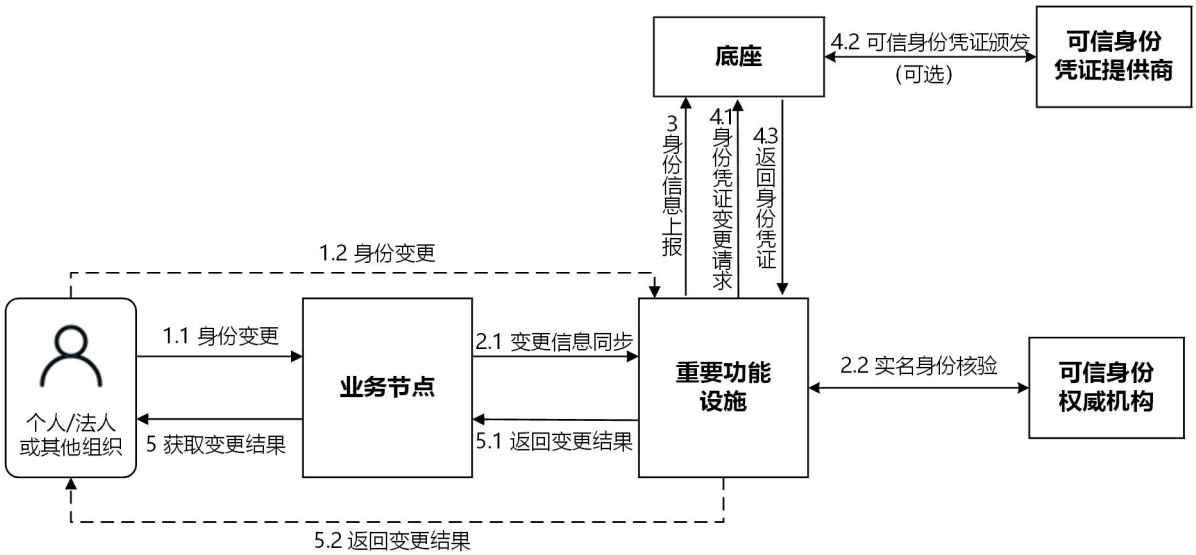

图 3 用户身份变更流程

流程说明：

a) 发起申请：个人/法人或其他组织在业务节点或重要功能设施提交身份变更请求，需同步提交实名认证所需的更新材料；

b) 信息同步转交：如在业务节点发起身份变更，业务节点应将变更信息同步至重要功能设施；

c) 实名复核：重要功能设施向可信身份权威机构申请身份核验，获取核验结果；

d) 凭证重签发：完成核验后，重要功能设施将变更后的身份信息同步至底座，并向底座申请签发用户身份凭证，底座对接可信身份凭证提供商将旧凭证注销，并为主体重新签发可信身份凭证；

e) 反馈结果通知：可信身份凭证返回至重要功能设施，由重要功能设施下发至业务节点并通知用户，用户可在任一节点查询变更处理结果。

已完成身份注册的个人、法人或其他组织，如其授权的受托执行者信息发生变化，相关变更要求见7.1.2.2。

7.1.2.2 受托执行者身份变更

当个人、法人或其他组织需调整受托执行者信息、更换受托执行者，或变更受托执行者的授权范围、授权期限等内容时，应在业务节点或重要功能设施发起受托执行者变更申请。

受托执行者变更应基于已完成注册的责任主体身份开展，并应对责任主体与受托执行者之间的授权关系进行核验。变更完成后，更新后的受托执行者方可在授权范围内继续代表责任主体参与数据流通利用活动、发起数据访问、服务调用或跨域协同。

7.1.3 用户身份注销

7.1.3.1 个人/法人或其他组织身份注销

个人、法人或其他组织用户在业务节点进行身份注销，流程见下图：

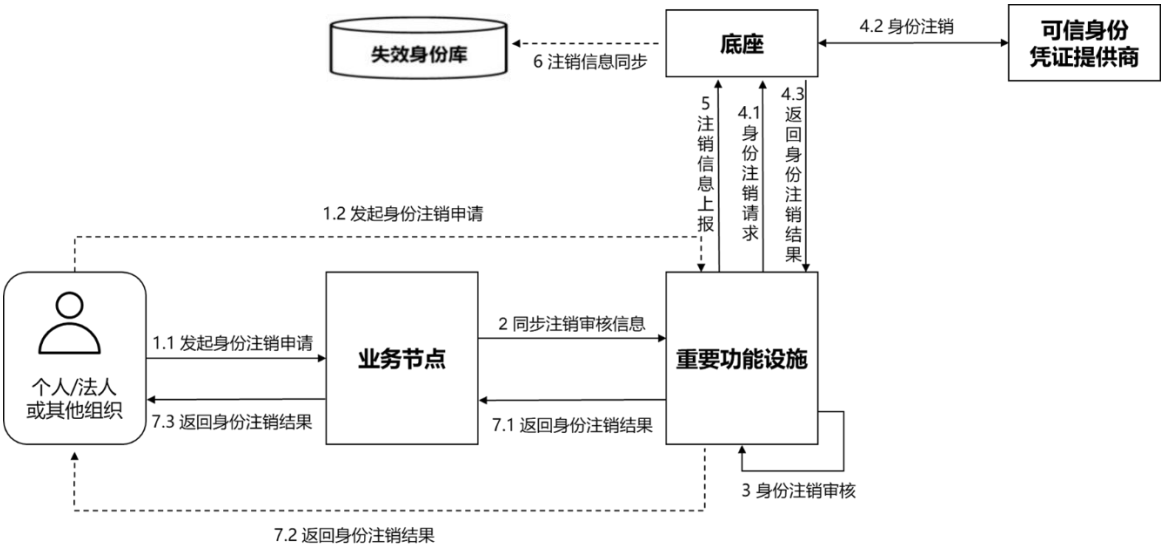

图 4 用户身份注销流程

流程说明：

a) 发起申请：个人、法人或其他组织在业务节点或重要功能设施发起身份注销申请；
b) 信息同步转交：如在业务节点发起注销申请，业务节点将注销信息同步至重要功能设施；
c) 重要功能设施审核：重要功能设施对申请主体身份、注销请求的合规性进行审核，包括检查在重要功能设施和其他重要功能设施上，该主体是否存在未结算业务、未完成授权操作或安全风险提示等；
d) 注销请求：完成审核后重要功能设施向底座请求凭证吊销；
e) 注销操作：底座对接可信身份凭证提供商将旧凭证注销；
f) 身份信息同步：注销结果返回至重要功能设施，重要功能设施将身份状态标记为“已注销”并同步至底座，由底座将注销身份信息同步至失效身份库；
g) 反馈结果通知：重要功能设施下发注销结果至业务节点或直接通知用户，用户可在任一节点查询注销处理结果。

当已注销主体存在受托执行者登记关系时，相关受托执行者不得再以该主体名义继续开展代理活动。受托执行者相关注销要求见 7.1.3.2。

7.1.3.2 受托执行者身份注销

当个人、法人或其他组织不再授权受托执行者代表其参与数据流通利用活动、发起数据访问、服务调用或跨域协同时，应在业务节点或重要功能设施发起受托执行者注销申请，使其不再以该责任主体名义代理开展相关业务。

受托执行者注销操作不影响责任主体身份的持续存在。对于自然人受托执行者，注销其受托执行资格不影响其作为自然人主体身份的持续存在；对于应用程序、智能体或其他自动化执行单元，注销后不得再以该责任主体名义继续发起相关操作。若用户需注销其个人、法人或其他组织主体身份，可参考7.1.3.1 单独发起申请。

7.1.4 用户登录认证

7.1.4.1 概述

在用户访问业务节点时，通过安全验证手段确认其用户身份合法性与有效性。登录认证应支持对责任主体本人以及其授权受托执行者的身份校验，并能够结合可信身份凭证、DID等方式完成身份认证。在涉及自动化调用、程序化调用或智能体代为调用的场景下，应能够识别责任主体与实际执行者之间的关系，并据此建立登录或调用状态。

7.1.4.2 可信身份凭证登录

用户采用可信身份凭证方式登录业务节点，流程见下图：

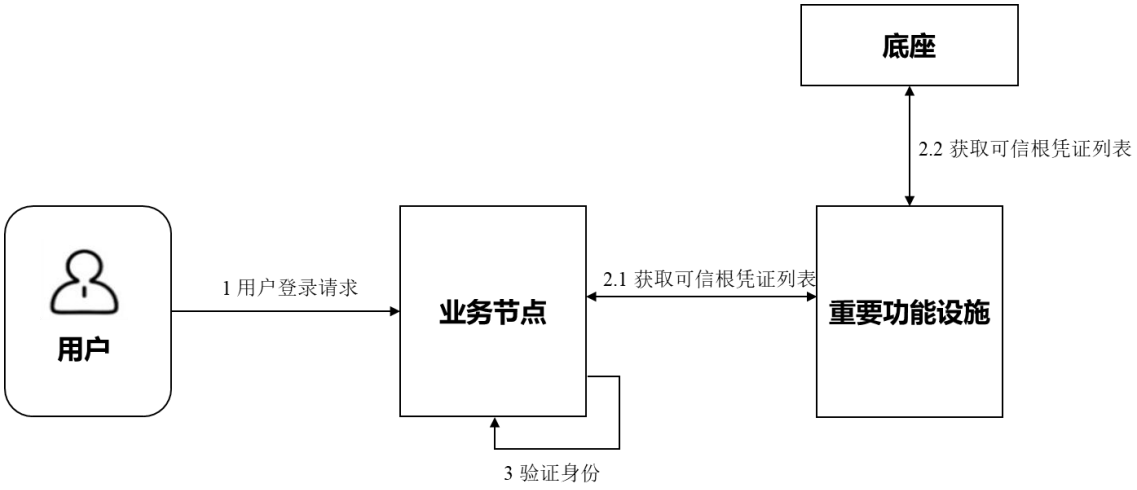

图 5 平台登录认证流程（可信身份凭证登录）

流程说明：

a) 登录发起：用户选择以可信身份凭证方式进行登录，并向业务节点提交客户端持有的可信身份凭证；当由受托执行者发起登录或调用时，还应提交能够反映其与责任主体之间授权关系的相关信息；
b) 获取凭证：业务节点可通过重要功能设施获取可信根凭证列表，重要功能设施可通过底座获取重要功能设施可信根凭证列表；
c) 签名验证：业务节点依据获取的可信根凭证列表，完成身份验证；在由受托执行者发起的场景下，还应结合授权关系对责任主体与实际执行者之间的一致性进行校验。

7.1.4.3 DID（去中心化身份）登录

用户选择以DID方式登录时，向业务节点提交基于其DID与可验证凭证生成的认证材料。业务节点依据DID解析结果和既定信任策略，对相关凭证的签名有效性、完整性与一致性进行校验，并在验证通过后建立本地登录状态。当登录或调用由受托执行者发起时，还应提交能够反映责任主体与受托执行者关系的相关认证材料。业务节点在验证 DID 文档和可验证凭证的基础上，应进一步校验责任主体与实际

执行者之间的授权关系。在跨域场景下，业务节点可根据所采用的DID方法及信任体系，通过相应的DID解析或身份服务，对DID文档或凭证状态进行补充校验，以获取最新的身份或凭证有效性信息，完成认证流程。

7.2 接入连接器身份注册认证

7.2.1 接入连接器身份注册

接入连接器身份注册流程见下图：

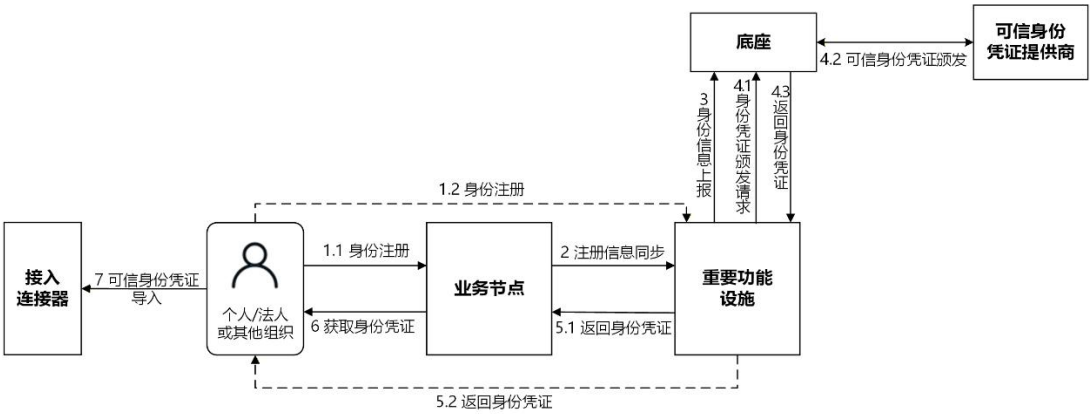

图 6 接入连接器身份注册流程

流程说明：

a) 注册申请：在主体身份已注册并认证的前提下，接入主体（个人/法人或其他组织/受托执行者）在业务节点或重要功能设施发起连接器身份注册，并提交接入连接器身份信息、部署信息及相关核验材料；

b) 信息同步：如在业务节点发起注册，业务节点将注册信息同步至对应的重要功能设施；

c) 凭证签发：完成核验后重要功能设施将身份信息同步至底座，并向底座申请签发用户身份凭证，底座对接可信身份凭证提供商签发可信身份凭证；

d) 注册完成：可信身份凭证返回至重要功能设施，由重要功能设施下发至业务节点或直接向用户反馈注册结果完成身份注册；

e) 凭证导入与启用：接入主体将接收到的可信身份凭证导入接入连接器，系统启用后，即具备可验证身份能力，可用于平台接入认证、自动化调用认证及跨节点协同认证。

可信身份凭证结构见附录 B。

7.2.2 接入连接器身份注销

接入连接器身份注销流程见下图：

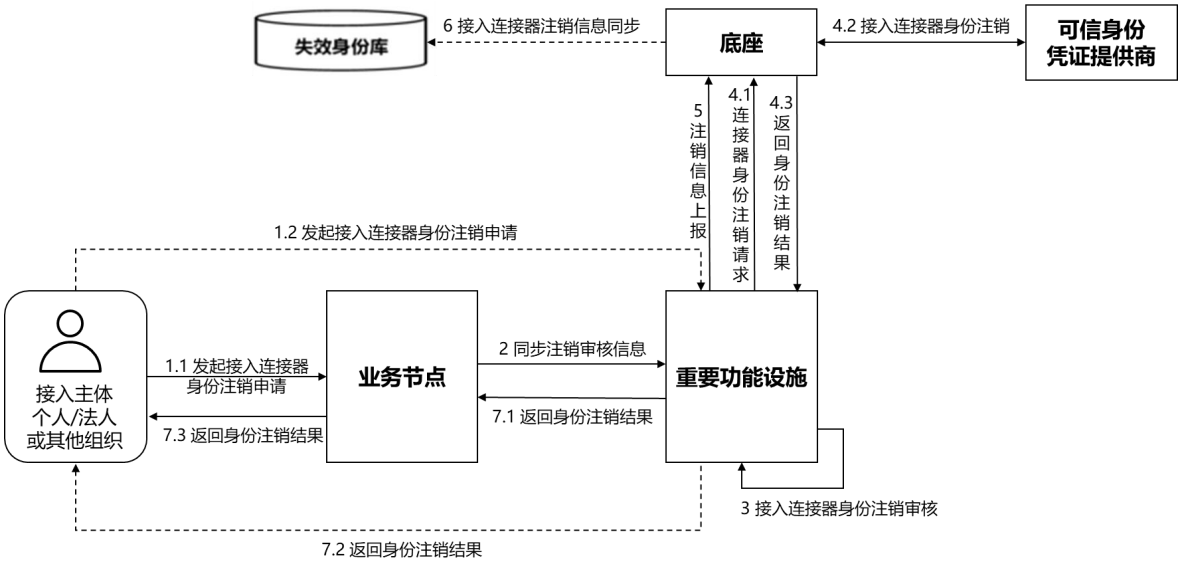

图 7　接入连接器身份注销流程

流程说明：

a）　发起申请：接入主体向业务节点或重要功能设施发起接入连接器身份注销申请；

b）　信息同步转交：如在业务节点发起注销，业务节点将注销信息同步至重要功能设施；

c）　重要功能设施审核：重要功能设施对注销请求的合规性进行审核；

d）　注销请求：完成审核后重要功能设施向底座请求凭证吊销；

e）　注销操作：底座对接可信身份凭证提供商将旧凭证注销；

f）　身份信息同步：注销结果返回至重要功能设施，重要功能设施将身份状态标记为“已注销”并同步至底座，由底座将注销身份信息同步至失效身份库；

g）　反馈结果通知：重要功能设施下发注销结果至业务节点或直接通知用户，用户可在任一节点查询注销处理结果。

接入连接器身份注销后，不得再用于平台接入、自动化调用或跨节点协同认证。

7.2.3　接入连接器身份验证

7.2.3.1　接入连接器与重要功能设施双向认证

接入连接器与重要功能设施的双向认证流程如下：

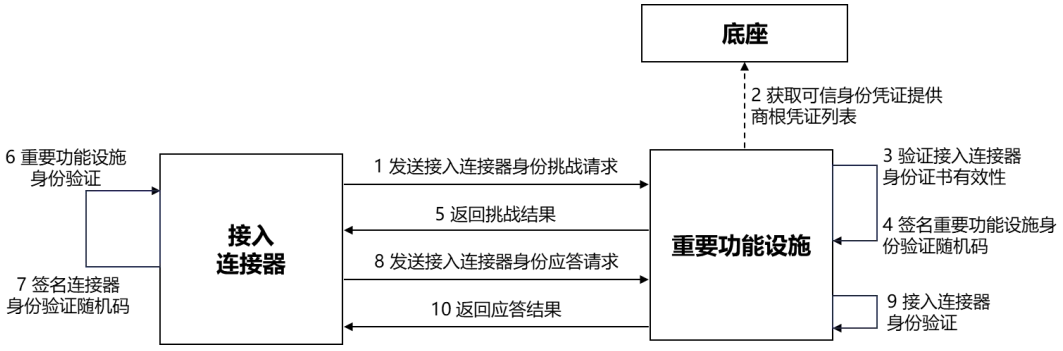

图 8　接入连接器与重要功能设施双向认证流程

流程说明：

a) 发送接入连接器身份挑战请求：接入连接器向重要功能设施发起身份挑战请求，提交连接器证书等必要信息；

b) 获取可信身份凭证提供商根凭证列表：重要功能设施向底座获取可信身份凭证提供商根凭证列表，并在本地缓存；

c) 验证接入连接器身份证书有效性：重要功能设施基于根凭证列表校验连接器证书有效性；

d) 签名重要功能设施身份验证随机码：重要功能设施使用自身私钥签名身份验证随机码，同时生成连接器身份验证随机码；

e) 返回挑战结果：重要功能设施返回挑战结果，包括重要功能设施身份验证随机码签名密文及连接器身份验证随机码；

f) 重要功能设施身份验证：接入连接器使用已知的重要功能设施证书验证重要功能设施身份验证随机码签名密文，确认重要功能设施身份；

g) 签名连接器身份验证随机码：接入连接器使用其证书对应私钥对连接器身份验证随机码进行签名，生成签名密文；

h) 发送接入连接器身份应答请求：接入连接器向重要功能设施发送身份应答请求，提交连接器身份验证随机码签名密文；

i) 接入连接器身份验证：重要功能设施使用连接器证书验证连接器身份验证随机码签名密文，确认接入连接器身份；

j) 返回应答结果：验证通过返回授权码，验证失败返回报错信息。

认证通过后，接入连接器可基于该认证结果开展平台接入、自动化调用、模型服务调用中转或跨节点协同。

7.2.3.2 接入连接器之间双向认证

连接器之间的身份认证流程如下图所示。

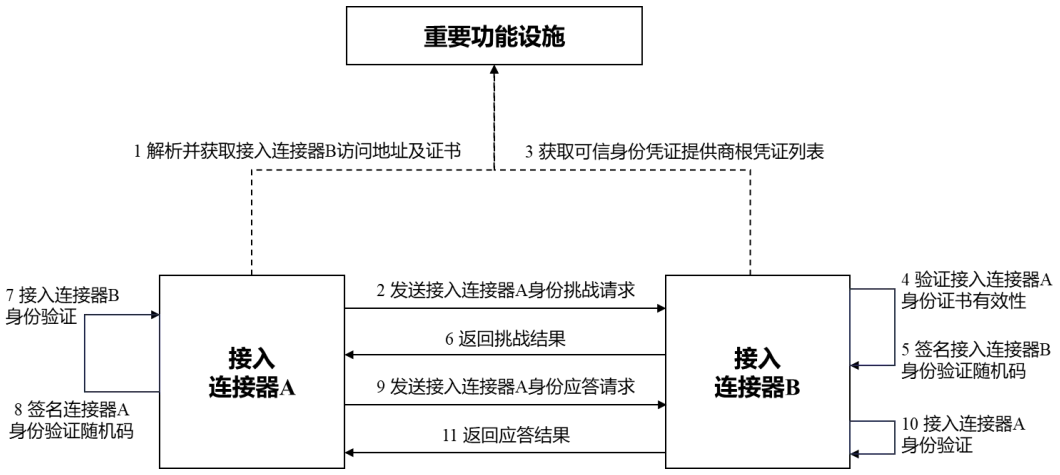

图 9 接入连接器之间双向认证流程

流程说明：

a) 接入连接器 A 解析并获取接入连接器 B 的访问地址及证书：接入连接器 A 解析接入连接器 B 的标识，获取接入连接器 B 访问地址及接入连接器 B 证书；

b) 发送接入连接器 A 身份挑战请求：接入连接器 A 向接入连接器 B 发起身份挑战请求，提交连接器 A 证书及连接器 A 身份验证随机码；

c） 接入连接器 B 获取可信身份凭证提供商根凭证列表：接入连接器 B 向重要功能设施获取可信身份凭证提供商根凭证列表，并在本地缓存；

d） 接入连接器 B 验证接入连接器 A 证书有效性：接入连接器 B 基于根凭证列表校验连接器 A 证书有效性；

e） 签名连接器 B 身份验证随机码：接入连接器 B 使用自身私钥签名身份验证随机码，同时生成接入连接器 A 身份验证随机码；

f） 返回挑战结果：接入连接器 B 向接入连接器 A 返回挑战结果，包括连接器 B 身份验证随机码签名密文及连接器 A 身份验证随机码；

g） 接入连接器 A 验证接入连接器 B 身份：接入连接器 A 使用步骤 1 获取的接入连接器 B 证书验证连接器 B 身份验证随机码签名密文，确认接入连接器 B 身份；

h） 签名连接器 A 身份验证随机码：接入连接器 A 使用其证书对应私钥签名身份验证随机码，生成签名密文；

i） 发送接入连接器 A 身份应答请求：接入连接器 A 向接入连接器 B 发送身份应答请求，提交连接器 A 身份验证随机码签名密文；

j） 验证接入连接器 A 身份：接入连接器 B 使用接入连接器 A 证书验证接入连接器 A 身份验证随机码签名密文，确认接入连接器 A 身份；

k） 返回应答结果：验证通过返回授权码，验证失败返回报错信息。

认证通过后，接入连接器之间可基于该认证结果开展数据访问、服务转接、自动化调用或人工智能相关服务协同。

7.3 平台身份注册认证

7.3.1 平台身份注册

平台身份注册流程见下图：

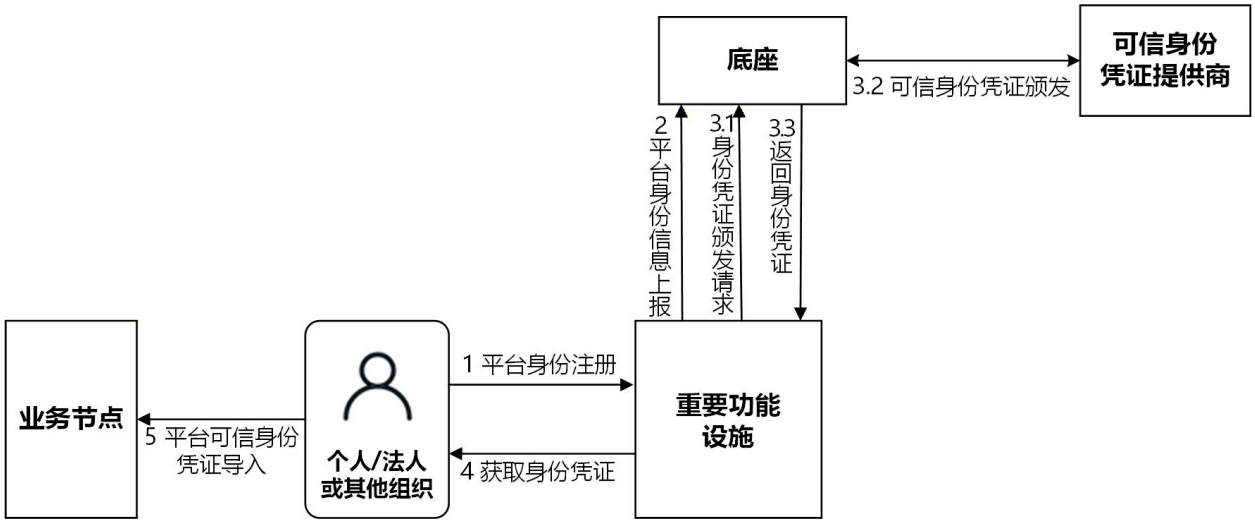

图 10 平台身份注册流程

流程说明：

a) 注册申请：在主体身份已注册前提下，接入主体在重要功能设施发起身份注册，并提交平台身份信息、平台功能说明及相关核验材料；
b) 凭证签发：完成核验后重要功能设施将身份信息同步至底座，并向底座申请签发用户身份凭证，底座对接可信身份凭证提供商签发可信身份凭证；
c) 注册完成：可信身份凭证返回至重要功能设施，由重要功能设施向用户反馈注册结果，用户获取可信身份凭证，完成身份注册；
d) 凭证导入与启用：用户将接收到的平台可信身份凭证导入业务节点，系统启用后，即具备可验证身份能力，可用于平台接入认证、人工智能相关服务接入认证和跨节点协同。

7.3.2 平台身份注销

平台身份注销流程如下图所示。

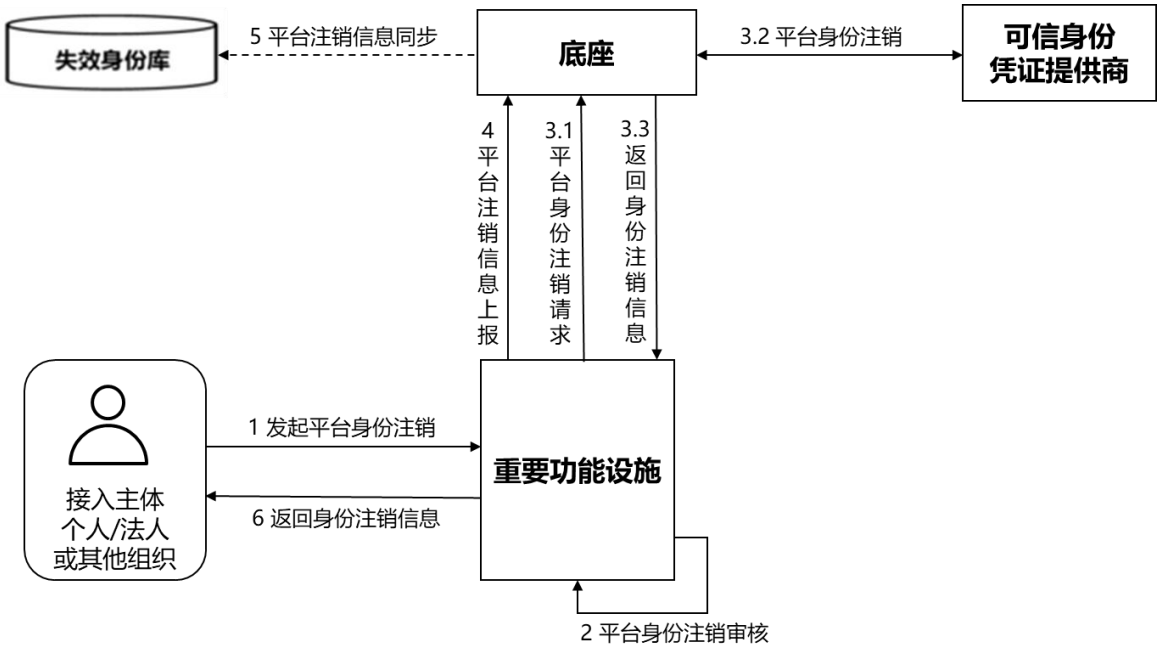

图 11 平台身份注销认证流程

流程说明：

a) 发起申请：接入主体向重要功能设施提交平台身份注销申请，申请应说明注销原因与关联资源处置情况；
b) 重要功能设施审核：重要功能设施对注销请求的合规性进行审核；
c) 注销请求：完成审核后重要功能设施向底座请求凭证吊销；
d) 注销操作：底座对接可信身份凭证提供商将旧凭证注销；
e) 身份信息同步：注销结果返回至重要功能设施，重要功能设施将身份状态标记为“已注销”并同步至底座，由底座将注销身份信息同步至失效身份库；
f) 反馈结果通知：注销结果返回至重要功能设施，由重要功能设施通知用户注销处理结果。

平台身份注销后，不得再用于平台接入、模型服务、推理服务、智能编排、自动化调用或跨节点协同。

8 接口对接要求

8.1 总体架构

统一用户身份管理和接入过程，主要涉及身份注册、查询、注销、跨节点身份核验等业务过程，接口对接总体架构图如下：

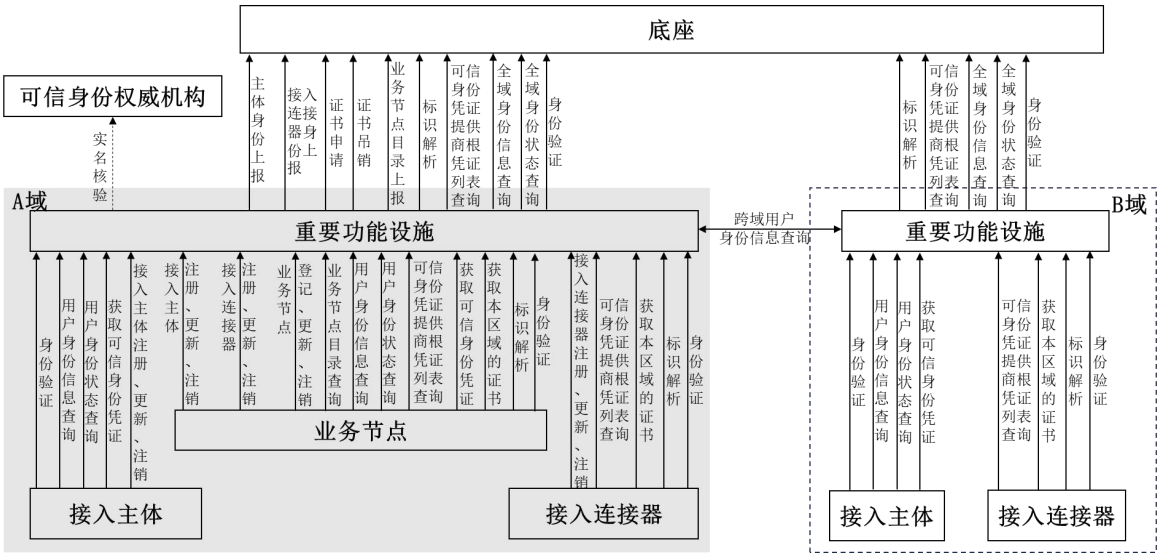

图 12 统一用户身份管理和接入总体架构图

8.2 接口列表

接口列表见表1。

表 1 接口列表

序号	接口名称	接口编码	调用方	提供方
1	挑战应答（身份验证）	globalIdentityVerify	重要功能设施	底座
2	证书申请	regionApplyCert	重要功能设施	底座
3	证书吊销	regionRevokeCert	重要功能设施	底座
4	主体身份上报	enterpriseReport	重要功能设施	底座
5	接入连接器身份上报	SyncConnectorInfo	重要功能设施	底座
6	业务节点目录上报	serviceNodeReport	重要功能设施	底座
7	标识解析	globalNodeResolution	重要功能设施	底座
8	可信身份凭证提供商根凭证列表查询接口	GetIdentityProviderList	重要功能设施	底座
9	全域身份信息查询接口	GetIdentityInfo	重要功能设施	底座
10	全域身份状态查询接口	getIdentityStatus	重要功能设施	底座
11	挑战应答（身份验证）	identityVerify	业务节点、接入主体、接入连接器	重要功能设施
12	接入主体注册	enterpriseRegistry	接入主体、业务节点	重要功能设施
13	接入主体更新	enterpriseUpdate	接入主体、业务节点	重要功能设施

14	接入主体注销	enterpriseClose	接入主体、业务节点	重要功能设施
15	业务节点登记	serviceNodeRegistry	业务节点	重要功能设施
16	业务节点更新	serviceNodeUpdate	业务节点	重要功能设施
17	业务节点注销	serviceNodeClose	业务节点	重要功能设施
18	接入连接器注册	connectorRegistry	接入连接器、业务节点	重要功能设施
19	接入连接器更新	connectorUpdate	接入连接器、业务节点	重要功能设施
20	接入连接器注销	connectorClose	接入连接器、业务节点	重要功能设施
21	业务节点目录查询	regionSyncListQuery	业务节点	重要功能设施
22	用户身份信息查询	GetEnterpriseInfo	接入主体、业务节点	重要功能设施
23	可信身份凭证提供商根凭证列表查询接口	GetIdentityProviderList	业务节点、接入连接器	重要功能设施
24	获取可信身份凭证接口	getIdentityCredential	接入主体、业务节点	重要功能设施
25	用户身份状态查询接口	getIdentityStatus	接入主体、接入连接器、业务节点	重要功能设施
26	获取本区域的证书	getRegionCert	业务节点、接入连接器	重要功能设施
27	标识解析	regionNodeResolution	业务节点、接入连接器	重要功能设施

9 管理与安全要求

9.1 基本要求

a) 面向人工智能相关服务的管理要求：数据基础设施中的用户身份管理与接入体系应支撑模型服务、推理服务、智能编排、自动化调用等人工智能相关服务的可信接入、合规调用和跨域协同；同时，可利用人工智能技术提升身份核验、状态同步、异常识别、运行维护和跨域协同管理能力，但不应削弱身份可信、权限可控、过程可审计和责任可追溯等基本要求。

b) 运行维护组织与责任制度：底座、重要功能设施、业务节点及接入连接器应设立专责的运行维护组织，明确各类运维岗位职责，建立日常值守、问题响应、系统变更等管理流程，保障身份管理系统持续、稳定运行。对涉及人工智能相关服务的平台、接入连接器和自动化调用场景，应明确相应的运行维护责任、业务管理责任和安全管理责任。

c) 应急预案与演练机制：应制定包含故障恢复、数据泄露、非法接入、系统攻击、自动化异常调用、模型服务异常或跨域协同异常等场景的应急预案，并定期组织演练和效果评估，提升故障处置能力和业务恢复效率。

d) 日志记录与保留：应确保网络设备、主机设备、应用系统及数据库系统具备日志采集功能。日志记录内容包括但不限于用户登录、身份变更、凭证签发、访问行为等，保存时间不少于180天，并应支持归档和审计溯源。对由受托执行者、应用程序、智能体或其他自动化执行单元发起的操作，应能够记录责任主体、实际执行者、执行通道、调用用途和处理结果。

e) 数据一致性与冗余清理：应定期清理和校验用户数据、系统数据，排查冗余记录与失效身份，确保数据结构完整、状态准确、权限匹配。对涉及受托执行者关系、自动化调用配置和人工智能相关服务属性的信息，也应纳入一致性校验和冗余清理范围。

f) 跨域互信保障机制：各级节点应建立身份状态同步机制，确保注销、变更、吊销等关键状态可在全网范围内实时感知与一致性更新，避免因信息不同步导致的信任失效或安全漏洞。同

时，应坚持跨域节点的“三统一”原则，即统一标准、统一流程、统一接口，推进用户信息的集中管理和全网互认；在跨域信息同步过程中，应采用分级同步策略，仅同步必要的基础信息，敏感信息由注册节点进行安全隔离和保管，确保用户隐私安全。在涉及人工智能相关服务的跨域协同场景下，应支持责任主体、实际执行者、接入连接器和平台之间关系信息的必要同步与校验。

g) 用户隐私保护与数据采集合规：应严格遵循国家有关个人信息保护法律法规和数据安全要求，制定并执行数据最小化原则，限制对用户敏感信息的采集范围和使用场景，确保仅收集为身份管理所必需的信息。应完善用户授权和知情机制，保障用户对其身份信息采集、使用、存储和删除等行为的知情权、同意权和查询权，确保用户隐私安全与数据使用合法合规。对人工智能相关服务场景下涉及的调用关系、授权关系和自动化执行信息，应遵循最小必要原则采集和使用。

9.2 安全措施

9.2.1 账户安全措施

a) 异常登录识别与风险感知：应支持基于登录时间、登录地点、设备指纹、访问频率、历史行为模式等信息，对异常登录、异常身份使用和高风险访问行为进行识别与预警。
b) 动态认证等级适配：应支持结合访问对象敏感性、访问场景风险、行为异常程度等因素，动态调整认证等级要求；对高风险访问行为可触发附加认证、重新认证或限制访问。
c) 多因素认证机制：对高权限用户、关键操作、高风险访问和异常行为触发场景，应启用多因素认证机制，结合动态口令、指纹、人脸识别等多因子手段增强安全性。
d) 应急身份冻结机制：当检测到身份被盗用、异常调用、持续高频失败或其他重大安全风险时临时冻结可疑身份，启用多因素认证机制，保障用户账户安全。

9.2.2 数据安全措施

a) 数据定期备份与离线存储：定期对系统和数据进行备份，并生成加密存储，以防止数据丢失或损坏。备份数据定期验证可用性。
b) 数据加密：使用符合国家和密码行业标准的密码算法或基于硬件级安全保护模块对平台数据进行加密，防止数据在存储、传输过程中被窃取和篡改。
c) 访问控制最小权限原则：对数据访问实施严格控制，结合最小权限原则和角色访问控制等机制，分级分域管理数据，防止未经授权的用户访问或泄露数据。应支持结合身份属性、调用上下文、历史行为和风险状态，对数据访问实施动态、细粒度的权限控制，提高权限管理的准确性和适配性。
d) 硬件级安全保护：应支持使用硬件级安全模块对密钥和敏感数据进行硬件隔离和安全存储，防止物理攻击和非法访问。同时，支持数据存储、密钥管理、数字签名及数据加密等功能，保障数据的机密性、完整性和可用性。
e) 敏感信息分离存储：对用户名、口令等敏感信息可采用安全硬件模块或安全容器进行分离存储，进一步降低数据安全风险。

9.2.3 应用软件安全措施

a) 全生命周期安全管理：从开发、测试、部署到运维，均应嵌入安全审查流程，包括代码审计、渗透测试、第三方组件漏洞评估等环节。

b) 应用软件进行更新和维护：定期更新和维护应用软件，包括操作系统和应用程序，以修复已知的漏洞和安全问题。
c) 安全开发和测试：在应用软件的开发和测试过程中，考虑安全因素，遵循安全最佳实践和安全编码标准。
d) 补丁管理与版本控制：应建立安全补丁发布机制，对操作系统、中间件、应用软件进行版本迭代记录和补丁推送。重大漏洞应在 24 小时内完成应急修复或风险隔离。

9.2.4 数据需求分级与认证等级要求

a) 业务节点、重要功能设施应结合数据基础设施中的数据类型、业务敏感性及访问风险，对数据访问需求进行分级管理，并基于分级结果明确相应的用户身份认证等级要求。业务节点、重要功能设施除应结合数据类型、业务敏感性及访问风险进行分级外，还应结合用户行为特征、调用场景、历史记录和实时风险状态，对访问需求进行动态评估。
b) 数据需求分级可参考以下划分示例（可根据行业特性和安全需求进一步细化）：
   - 低风险数据（如基础信息、非敏感统计数据）：对应0级认证（无实名认证或最低实名核验要求）。
   - 中等风险数据（如敏感用户信息、部分业务操作数据）：对应1级认证（身份证或社保卡实名认证）。
   - 高风险数据（如核心业务数据、重要资源操作权限）：对应2级及以上认证（基于身份证实名认证+人脸识别或其他多因子认证）。
c) 认证等级应与业务需求和数据风险相适配，高敏感度数据访问必须具备相应的认证等级要求，不得以低认证等级替代高认证等级访问，确保数据安全性和合规性。对高风险行为、异常调用、自动化访问或跨域敏感数据访问，不得因调用方式变化降低应满足的认证等级要求。
d) 认证等级划分标准应由重要功能设施根据实际应用场景及行业监管要求制定，并同步至底座备案，确保认证策略的统一性和可扩展性。
e) 当认证等级发生调整时，系统应具备相应的动态适配机制，及时同步认证状态变更，保障用户体验与安全合规并重。当访问场景、行为风险、调用方式或身份状态发生变化时，系统应能够动态调整认证等级、校验要求和访问控制策略，实现认证要求与风险状态的实时适配。

9.3 记录与审计措施

a) 身份全生命周期记录：底座、重要功能设施、业务节点和接入连接器应对用户身份生成、更新、使用、授权、销毁等全生命周期行为建立详尽日志，记录内容应包括时间、责任主体、实际执行者、执行通道、操作对象、结果与 IP 信息等。
b) 日志不可篡改存储：应采用链式哈希、区块链或只读归档机制保障审计日志的不可篡改性，支持事后取证与合规监管。
c) 定期审计与行为分析：明确安全审计策略，定期对日志记录进行审计，并支持利用人工智能技术对异常登录、异常身份使用、越权访问、异常频率、异常路径、异常授权关系和跨节点异常协同行为进行识别、分析与预警。
d) 审计记录安全备份与多地分发：审计日志应定期加密备份至异地安全节点，避免受到未预期的删除、修改和覆盖。

附 录 A （规范性）
接入主体身份信息

A.1 个人用户身份信息

个人用户身份信息基础信息与附属信息详细内容见表A.1、A.2，其中基础信息为必选项。

表 A.1 个人用户身份基础信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	姓名	individualName	String	50	必填	姓名
2	个人认证方式	authType	String	1	必填	0-中华人民共和国公安部、中华人民共和国人力资源和社会保障部等国家权威部门的实名和匿名服务 1-国家政务服务平台实名服务 2-微信、支付宝、通信运营商等第三方服务入口 3-身份证或社保卡实名核验
3	证件类型	individualType	String	10	必填	0-中华人民共和国居民身份证 1-护照 2-军官证
4	证件号码	individualIdCode	String	50	必填	证件号码,身份证不允许更新该字段，证件号原文
5	手机号	individualPhone	String	11	必填	手机号
6	证件有效期起始日期	individualPeriodBegin	String	10	必填	证件有效期起始日期,yyyy-MM-dd
7	证件有效期截止日期	individualPeriodEnd	String	10	必填	证件有效期截止日期,yyyy-MM-dd
8	证件照片-正	individualIdCardz	Base64	-	必填	证件-正面
9	证件-正面-文件格式	individualIdCardzType	String	10	必填	证件-正面-文件格式（png，jpg 等）
10	证件照片-反	individualIdCardf	Base64	-	可选	证件-反面（身份证的时候必选）
11	证件-反面-文件格式	individualIdCardfType	String	10	可选	证件-反面-文件格式（png，jpg 等）（身份证的时候必选）

表 A.2 个人用户身份附属信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	国籍	nationality	String	50	选填	个人所属国家或地区，通常用于国际业务、跨境场景或身份核验
2	性别	gender	String	2	选填	
3	出生年月	birthDate	String	7	选填	格式为 YYYY-MM，需与身份证信息保持一致
4	社保卡卡号	socialSecurityCardNo	String	20	选填	采用社保卡认证时需提供
5	社保卡发放地	socialSecurityCardIssuer	String	50	选填	采用社保卡认证时需提供
6	支付宝账号	alipayAccount	String	100	选填	与身份关联的支付宝账号信息，用于授权委托、电子支付或快捷认证
7	微信账号	wechatAccount	String	100	选填	与身份关联的微信账号信息，用于授权委托、电子支付或快捷认证
8	邮箱	email	String	100	选填	用户常用邮箱地址，作为辅助认证、通知通道及密码找回手段
9	联系地址	contactAddress	String	200	选填	常驻居住地或通信地址，用于物流交付、线下服务或区域管理服务
10	其它	extendedInfo	JSON	-	选填	扩展项如微博 ID、学历、兴趣偏好等，视平台实际场景启用，须说明收集目的与授权机制

A.2 法人或其他组织身份信息

法人或其他组织身份信息基础信息与附属信息详细内容见表A.3、A.4，其中基础信息为必选项。

表 A.3 法人或其他组织用户身份基础信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	法人或其他组织名称	enterpriseName	String	50	必填	法人或其他组织名称
2	统一社会信用代码	enterpriseCode	String	50	必填	统一社会信用代码
3	法人或其他组织类型	enterpriseType	String	2	必填	0- 机关法人 1- 企事业单位法人 2- 社会团体法人 3- 非法人组织 4- 其它
4	经营期限起始	operatingPeriodBegin	String	10	必填	经营期限起始(yyyy-MM-dd)
5	经营期限截止	operatingPeriodEnd	String	20	必填	经营期限截止(yyyy-MM-dd)
6	实名认证方式	authType	String	2	必填	0- 实名认证方式
7	法定代表人或负责人姓名	legalPerson	String	50	必填	法定代表人或负责人姓名
8	法定代表人或负责人证件号	legalPersonCertno	String	50	必填	法定代表人或负责人证件号

表 A.3 法人或其他组织用户身份基础信息（续）

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
9	法定代表人或负责人实名等级	legalPersonAuthLevel	Integer	2	必填	法定代表人或负责人实名等级 0-未实名 1-身份证实名核验或社保卡实名核验 2-在实名核验基础上增加人脸识别或其他生物特征核验
10	法定代表人或负责人实名认证方式	legalPersonAuthType	Integer	1	必填	同表 A.1 中个人实名或匿名认证方式
11	法定代表人或负责人身份证-正面	contactIdCardz	String/Base64	-	选填	法定代表人或负责人身份证-正面
12	法定代表人或负责人身份证-正面-文件格式	contactIdCardzType	String	10	选填	法定代表人或负责人身份证-正面-文件格式（png，jpg 等）
13	法定代表人或负责人身份证-反面	contactIdCardf	String/Base64	-	选填	法定代表人或负责人身份证-反面
14	法定代表人或负责人身份证-反面-文件格式	contactIdCardfType	String	10	选填	法定代表人或负责人身份证-反面-文件格式（png，jpg 等）

表 A.4 法人或其他组织用户身份附属信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	注册地址	enterpriseAddress	String	200	选填	工商登记注册地址
2	注册金额	regAmount	String	50	选填	注册金额，以人民币计，单位万元
3	注册日期	regDate	String		选填	注册日期(yyyy-MM-dd)
4	经营范围	businessScope	String		选填	经营范围，登记机关认可的业务范围
5	行业类型	industryCategory	String	50	选填	参照《GB/T 4754—2017 国民经济行业分类》进行行业分类工作
6	电子营业执照或其他组织机构证书	businessLicense	String	-	选填	电子营业执照 Base64
7	电子营业执照-文件格式	businessLicenseType	String	-	选填	电子营业执照-文件格式（png，jpg 等）
8	法定代表人或负责人手机号	legalPersonPhone	String	11	选填	法定代表人或负责人手机号
9	法定代表人或负责人邮箱	legalPersonEmail	String	50	选填	法定代表人或负责人邮箱
10	服务角色	serviceRole	String	100	选填	组织在数据基础设施中的角色,如数据提供方、数据使用方、平台运营方、模型服务提供方、智能应用提供方等
11	服务类型	serviceType	String	200	选填	涉及的服务类型,如模型服务、推理服务、智能编排、智能分析、数据处理服务等,可多值填写
12	自动化调用说明	automationDescription	String	200	选填	说明该组织是否存在自动化调用、程序化调用或智能体代为调用等情形

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
13	调用边界说明	callBoundary	String	200	选填	对相关服务的数据访问、服务调用或跨域协同边界进行说明
14	责任部门	responsibilityDept	String	100	选填	负责数据流通、模型服务或智能应用管理的内部部门名称
15	服务联系人	serviceContact	String	50	选填	负责相关服务接入、调用管理或人工智能业务的联系人姓名

A.3 受托执行者身份信息

受托执行者身份信息基础信息、附属信息详细内容见表A.5、A.6，其中基础信息为必选项。

表 A.5 受托执行者身份基础信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	受托执行者类型	executorType	String	2	必填	0-自然人；1-应用程序；2-智能体；3-其他自动化执行单元
2	受托执行者姓名或名称	executorName	String	100	必填	自然人填写姓名；非自然人填写应用程序、智能体或自动化执行单元名称
3	受托执行者证件或标识类型	executorCertType	String	20	条件必填	自然人填写居民身份证、护照、军官证等；非自然人填写应用标识、服务标识、实例标识等
4	受托执行者证件或标识号码	executorCertNo	String	128	条件必填	自然人填写证件号码;非自然人填写服务实例编号、应用编号或其他可识别标识
5	受托执行者实名认证等级	executorAuthLevel	Integer	1	条件必填	自然人适用：0-未实名；1-身份证实名核验或社保卡实名核验；2-在实名核验基础上增加人脸识别或其他生物特征核验
6	受托执行者实名认证方式	executorAuthType	Integer	1	条件必填	自然人适用：1-公安部、人社部等国家权威部门实名服务；2-国家监管部门授权或认可的CA机构；3-第三方服务入口
7	授权方式	authorizationType	Integer	1	必填	1-管理员确认；2-上传授权书；3-短信或邮件确认；4-协议配置授权；5-接口令牌授权
8	责任主体类型	principalType	String	2	必填	0-个人；1-法人或其他组织
9	责任主体姓名或名称	principalName	String	100	必填	个人填写自然人姓名；法人或其他组织填写主体名称
10	责任主体证件号码或统一社会信用代码	principalCode	String	50	必填	个人填写证件号码；法人或其他组织填写统一社会信用代码
11	授权起始日期	authorizationBegin	String	10	选填	授权生效日期，格式 yyyy-MM-dd
12	授权截止日期	authorizationEnd	String	10	选填	授权失效日期，格式 yyyy-MM-dd

表 A.6 受托执行者身份附属信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	责任主体所属部门	principalDept	String	100	选填	受托执行者所属的责任主体内部部门名称
2	授权文件	authorizationDocument	String/Base64	256	选填	授权书、委托协议、系统授权配置文件等
3	授权文件格式	authorizationDocumentType	String	20	选填	授权文件格式，如 pdf、png、jpg、xml、json 等
4	受托执行事项说明	authorizationDescription	String	200	选填	说明受托执行者可代表责任主体开展的事项
5	调用用途说明	callingPurpose	String	200	选填	说明数据访问、服务调用或跨域协同的用途
6	自动化运行方式	executionMode	String	20	选填	人工、半自动、自动
7	服务或智能体版本	executorVersion	String	50	选填	非自然人受托执行者适用，填写应用程序、智能体或自动化执行单元版本信息
8	服务提供方	providerName	String	100	选填	非自然人受托执行者适用，填写服务提供方名称
9	调用边界说明	callBoundary	String	200	选填	对数据访问、服务调用或跨域协同范围进行补充说明
10	联系手机号	contactPhone	String	20	选填	受托执行者联系人手机号
11	联系邮箱	contactEmail	String	100	选填	受托执行者联系人邮箱

A.4 接入连接器身份信息内容

接入连接器身份信息基础信息与附属信息详细内容见表A.7、A.8，其中基础信息为必选项。

表 A.7 接入连接器身份基础信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	接入连接器名称	connectorName	String	100	必填	接入连接器名称，需与部署文档一致
2	接入连接器地址	connectorNetworkList	String	-	必填	接入连接器地址
2.1	接入连接器接口服务地址	connectorNetworkList[].apiUrl	String	256	必填	接入连接器的接口服务地址，必须是 https
3	网络接入类型	connectorJoinType	Integer	4	必填	1- 专线 2- 互联网（固定公网 IP） 3- 互联网（无固定公网 IP） 4- 高速数据网 5- 其他
4	所属接入主体名称	ownerIdentityName	String	100	必填	所属接入主体名称
5	身份标识	ownerIdentityId	String	128	必填	所属接入主体身份标识
6	供应商名称	supplierName	String		必填	供应商名称
7	供应商统一社会	supplierCode	String		必填	供应商统一社会信用代码

	信用代码					
8	SN 号	connectorSN	String		选填	产品 SN 号
9	版本号	connectorVersion	String		必填	产品版本号
10	连接器类型	connectorType	Integer		必填	连接器类型 1-标准型接入连接器 2-全功能型接入连接器
11	物理设备唯一标识	connectorMac	String		必填	物理设备唯一标识符（若有多台，只登记管理服务器 mac 地址）
12	CSR 文本	csr	String		必填	凭证请求文件：CA 体系中为 csr 文件

表 A.8 接入连接器身份附属信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	接入连接器访问地址	connectorNetworkList[].serverUrl	Sting	50	选填	接入连接器的访问地址，必须是 https
2	服务类型	serviceType	String	200	选填	数据访问、模型调用中转、智能编排、自动化调用等，可多值填写
3	自动化调用说明	automationDescription	String	200	选填	是否承载自动化调用、程序化调用或智能体代为调用等场景
4	跨节点协同说明	crossNodeCollaborationDescription	String	200	选填	是否支持跨业务节点、跨区域或跨行业协同接入
5	调用边界说明	callBoundary	String	200	选填	对可承载的访问、调用或协同范围进行说明

A.5 平台身份信息内容

平台身份信息基础信息与附属信息详细内容见表A.9、A.10，其中基础信息为必选项。

表 A.9 平台身份基本信息

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	业务节点登记名称	entryName	String	100	必填	业务节点登记中文名称
2	业务节点地址	addresses	Array[object]		必填	
3	业务功能简介	introduction	String	255	必填	核心业务介绍
4	业务功能证明材料	supportingDocuments	String	-	必填	核心业务证明材料，例如评测证书、评测报告等 Base64
5	业务功能证明材料文件名	supportingDocumentsFileName	String	255	必填	
6	业务节点版本	version	String	20	必填	业务节点当前版本
7	所属法人或其他组织名称	enterpriseName	String	255	必填	
8	身份标识	enterpriseIdentityId	String	255	必填	所属法人或其他组织身份标识
9	CSR 文本	csr	String	255	必填	凭证请求文件：CA 体系中为 csr 文件

10	业务功能类型	type	String	500	必填	业务节点类型，单选： 1-应用侧基础设施 2-数据交易类 3-数据开发利用类 4-公共数据授权运营平台类 5-公共服务平台类 6-其他业务平台
12	业务节点平台地址	serverUrl	String	255	必填	业务节点平台地址，必须是 https
13	业务节点接口地址	apiUrl	String	255	必填	业务节点接口服务地址，必须是 https，需填写能够用于调用业务节点接口的正确地址，例如：https://xxx.xxx.x.xxx:8080/api/v1

表 A.10 平台身份附属信息

序号	平台附加信息	字段名称	数据类型	长度	约束类型	取值说明
1	安全责任人联系方式	securityOfficerContact	String	50	选填	用于审计或响应事件对接（如应急处置、违规行为举报）
2	运维服务商名称	maintenanceProvider	String	100	选填	平台系统维护单位，如使用托管或第三方安全服务
3	系统部署环境说明	deploymentEnv	Integer	4	选填	1-公有云 2-私有云 3-混合云 4-本地化部署
4	备注	reserveNotes	String	255	选填	如平台内部分级名称、子模块划分、用户接入量级等，可根据接入要求进行自定义填充
5	人工智能服务类型	aiServiceType	String	200	选填	模型服务、推理服务、智能编排、智能分析、智能检索等，可多值填写
6	自动化调用说明	automationDescription	String	200	选填	是否支持自动化调用、程序化调用或智能体代为调用等场景
7	服务边界说明	serviceBoundary	String	200	选填	对平台可提供的相关服务边界进行说明
8	业务责任部门	responsibilityDept	String	100	选填	负责平台相关服务或业务管理的内部部门名称

附 录 B （规范性）
可信身份凭证结构

接入主体、接入连接器和平台的可信身份凭证由底座对接的可信身份凭证提供商签发。

可信身份凭证结构见表B.1。

表 B.1 证书结构

项名称	描述
tbsCertificate	基本证书域
signatureAlgorithm	签名算法域
signatureValue	签名值域

基本证书域见表B.2。

表 B.2 基本证书域

证书域	描述	备注
version	版本号	
serialNumber	序列号	
signature	签名算法	
issuer	颁发者	
validity	有效期	
subject	主体	CN 项：身份标识码
subjectPublicKeyInfo	主体公钥信息	
extensions	扩展项	可选，可自定义

参考文献

[1] GB/T 32419.6-2017 信息技术 SOA技术实现规范 第6部分 身份管理服务
[2] GB/Z 24294.3-2017 信息安全技术 基于互联网电子政务信息安全实施指南 第3部分 身份认证与授权管理
[3] GB/T 31072-2014 科技平台 统一身份认证
[4] 国家发展改革委、国家数据局、工业和信息化部《国家数据基础设施建设指引》（发改数据〔2024〕1853
[5] 国家数据局关于印发《可信数据空间发展行动计划（2024—2028年）》的通知
[6] 《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》
[7] NDI-TR-2025-01 数据基础设施 参考架构
[8] NDI-TR-2025-04 数据基础设施 标识管理规范
[9] NDI-TR-2025-02 数据基础设施 互联互通基本要求
[10]NDI-TR-2025-05 数据基础设施 接入连接器技术要求