



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)

(草案)

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 核心管理对象 3

 5.3 主要参与方职责 4

6 身份信息构成 4

 6.1 接入主体身份信息内容 5

 6.2 接入连接器身份信息内容 9

 6.3 平台身份信息内容 10

7 身份注册认证流程 11

 7.1 接入主体身份注册认证 12

 7.2 接入连接器身份注册认证 18

 7.3 平台身份认证 20

8 接口对接要求 22

 8.1 总体架构 22

 8.2 接口总体要求 23

 8.3 接口定义 24

9 管理与安全要求 33

 9.1 基本要求 33

 9.2 安全措施 34

 9.3 记录与审计措施 34

附录 A （规范性） 可信身份凭证结构 36

附录 B （资料性） 报文样例 37

附录 C （规范性） 返回码定义 39

附录 D （规范性） Token 结构 41

参考文献 42

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：

本文件主要起草人：

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构成要求、身份注册及验证、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，以实现用户身份的跨节点互联互通。

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、运行和维护单位，用于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。

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 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

NDI-TR-2025-01 数据基础设施 参考架构

NDI-TR-2025-04 数据基础设施 标识管理规范

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，数据可通过接入连接器接入数据基础设施。

3.2

平台 platform

位于业务节点上，面向区域、行业及企业的数据流通利用平台。

3.3

可信身份提供商 trusted identity provider

负责签发、存储和维护可信用户身份的受信任实体。

3.4

可信身份权威机构 trusted identity authority

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

[来源：GB/T 31504-2015，3.12]

3.5

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。

3.6

可信身份凭证 trusted identity credential

可信身份凭证是一种基于数字加密技术的凭证，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。

3.7

失效身份凭证 invalid credential

失效身份凭证是凭据无效或已过期的身份凭证，指当用户身份颁发后，因业务或工作职责变更，身份颁发机构对身份凭证进行了注销或变更，导致身份失效。

3.8

身份凭证 identity credentials

用于认证用户身份的数据或物理媒介，通过证明用户身份的真实性以完成初始身份验证。

3.9

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。

3.10

跨域身份认证 cross-domain identity authentication

在一个已注册区域/行业功能节点完成注册的接入主体，在另一个区域/行业使用其原始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：一次性密码，One-Time Password

SN：序列号（产品编号），Serial Number

TEE：可信执行环境，Trusted Execution Environment

SBOM：软件物料清单，Software Bill of Materials

5 总体要求

5.1 总体架构

在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。

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见图1。

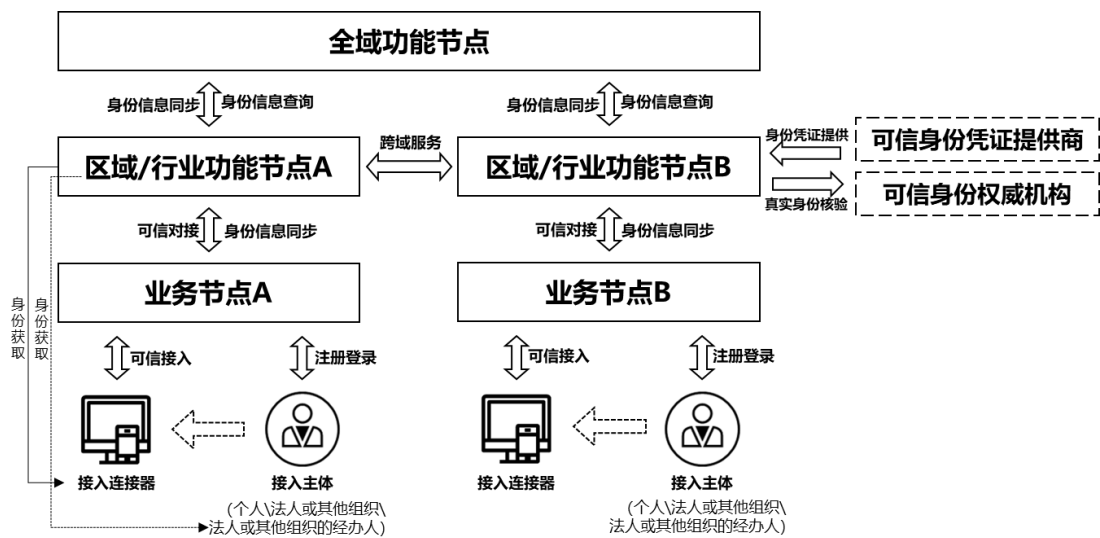


图1 总体架构

在该架构中：

- a) 接入主体可通过业务节点或区域/行业功能节点完成注册流程，获取其在国家数据基础设施内的用户身份；
- b) 区域/行业功能节点负责对接可信身份凭证提供商，为接入主体签发用户身份凭证，并协同可信身份权威机构完成身份真实性核验；
- c) 接入连接器的身份注册需由用户在区域/行业功能节点完成，并通过业务节点实现可信接入；
- d) 平台的接入应由区域/行业功能节点统一管理，确保平台用户身份的有效性和可信性。

5.2 核心管理对象

本节定义数据基础设施用户身份管理中的三类核心管理对象：接入主体、接入连接器与平台，明确各类对象的身份获取流程与管理要求。

5.2.1 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) 法人或其他组织经办人用户：指受法人或组织委托，负责办理与数据流通相关事务的人员。

接入主体应向业务节点或区域/行业功能节点提交用户身份注册申请。区域/行业功能节点应负责与可信身份权威机构对接，完成对接入主体的实名信息核验。核验通过后，应由区域/行业功能节点为接入主体生成并分配唯一用户身份凭证，作为其在数基础设施中的身份标识。该凭证应具有唯一性、可验证性和可追溯性，确保系统内部身份信息一致、安全可控。

5.2.2 接入连接器

接入连接器应向区域/行业功能节点发起接入申请，并获取平台分配的唯一身份标识。随后，可信身份凭证提供商应基于该标识信息、域名信息等，为连接器签发可信用用户身份凭证，用于在系统中验证连接器的身份合法性，支持其与平台的可信互通。

5.2.3 平台

平台需申请并获取由可信身份服务提供方签发的唯一可信身份凭证。平台间进行身份互认与服务调用时,应基于该身份凭证完成验证,确保跨平台的数据交换具备身份可信、安全可控与互操作性基础。

5.3 主要参与方职责

在国家数据基础设施用户身份管理体系中,全域功能节点、区域/行业功能节点及业务节点作为核心参与方,分别承担不同层级的身份管理与认证服务职责。其职能划分如下:

5.3.1 全域功能节点

全域功能节点作为国家级统一服务支撑枢纽,承担以下职责:

- 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与可信身份权威机构的权威清单,为各级节点提供标准化对接依据。

5.3.2 区域/行业功能节点

区域或行业功能节点作为身份注册与认证的关键承载单元,应履行以下职责:

- a) 支持接入主体、接入连接器及平台的用户身份注册与认证申请处理;
- b) 对接可信身份凭证提供商,为符合条件的接入连接器或平台签发可信身份凭证;
- c) 收集并维护本辖域内可信身份凭证提供商的基本信息,并定期向全域功能节点进行备案报告;
- d) 通过对接国家公安、人力资源社会保障等部门,或国家认定的第三方身份认证平台,对自然人身份进行实名核验;通过对接市场监管总局、民政部门等国家级可信身份权威机构,对法人或其他组织身份进行核验;
- e) 依托可信身份凭证,与全域功能节点、其他区域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;
- f) 提供跨域身份信息查询服务,支持身份数据的跨域同步与共享。

5.3.3 业务节点

- a) 支持接入主体用户注册和身份凭证获取;
- b) 提供接入主体的身份认证服务,包括但不限于登录认证、行为验证等安全机制;
- 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。

6 身份信息构成

在数据基础设施中,接入主体(包括个人用户、法人或其他组织用户、法人或其他组织经办人用户)、接入连接器与平台均应具备结构化的用户身份信息,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三部分组成:

- a) 基础信息:一个确定的用户身份应具备的基础数据信息,用于全域身份互认,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画像的辅助性信息,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和用户体验。

- c) 可验附件：由第三方权威机构签发、具备可验证性的数字凭证，以附件形式上传，用于证明接入主体具备某些特定身份属性、资质或行为信誉。该类信息不作为身份识别的必要信息，但在高等级安全验证、跨域信任交互、资质核验等场景中具有关键支撑作用。

6.1 接入主体身份信息内容

在数据基础设施中，接入主体包括个人用户、法人或其他组织用户和法人或其他组织经办人用户。

6.1.1 个人身份信息

个人用户身份信息用于定义和标识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。个人用户身份信息用于唯一标识自然人在数据流通体系中的合法身份，以证件类型、证件号码为唯一标识。为确保跨系统互操作与隐私合规性，基础信息、附属信息与可验附件进行分别维护，便于分级授权与数据最小化处理，个人用户身份信息的基础信息、附属信息与可验附件详细内容见表1-3。

表1 个人用户身份基础信息

序号	用户身份信息	说明
1	姓名	姓名
2	用户身份标识	由区域/行业功能节点生成，唯一标识用户身份
3	证件类型	证件类型：中华人民共和国居民身份证、护照、军官证等
4	证件号码	证件号码，唯一
5	证件号码有效起始日期	证件号码有效起始日期
6	证件号码有效截止日期	证件号码有效截止日期
7	手机号	手机号，唯一
8	个人实名认证等级	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
9	个人实名认证方式	1-公安部、人社部实名服务 2-国家政务服务平台实名服务 3-微信、支付宝、通讯运营商等第三方平台
10	实名认证时间	完成实名认证的时间
11	身份状态	0-不可用 1-可用

表2 个人用户身份附属信息

序号	用户附加信息	说明
1	国籍	可选，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	可选
3	出生年月	可选，格式为 YYYY-MM
4	社保卡卡号	可选，采用社保卡认证时需提供
5	社保卡发放地	可选，采用社保卡认证时需提供
6	支付宝账号	可选，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	可选
8	邮箱	可选，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	可选，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	可选，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

表3 个人用户身份可验附件

序号	用户可验信息	说明
1	学历/学位证书	可选，由教育部或高校签发的学历/学位认证信息，包含证书编号、专业、授予单位等，支持电子验证
2	职业资格证书	可选，如教师资格证、会计证、医师执业证等，由相关主管部门或考试机构颁发
3	信用报告摘要	可选，由征信机构（如中国人民银行征信中心、芝麻信用）生成的用户信用评分或信用等级
4	数字作品/知识产权登记	可选，包括数字签名作品认证、软件著作权证书等，适用于数字创作平台
5	授权委托书	可选，经认证的个人对法人单位或第三方授权操作的电子文书，含授权对象、期限、用途等
6	其他第三方认证信息	可选，如跨境身份认证、公证机构签发的个人声明、志愿服务记录等，须具备签发来源与验证机制

6.1.2 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，法人或其他组织用户身份以“统一社会信用代码”为唯一标识，其身份信息结构应适配企业实名认证、工商注册信息、行业分类与可信业务接口等实际管理需要。基础信息、附属信息与可验附件详细内容见表4-6。

表4 法人或其他组织用户身份基础信息

序号	用户身份信息	说明
1	法人或其他组织名称	工商注册或主管机关登记的法定名称
2	法人或其他组织身份标识	平台生成的唯一标识法人或其他组织身份
3	统一社会信用代码	统一社会信用代码，唯一
4	法人或其他组织类型	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
5	经营期限起始	经营期限起始时间（格式：YYYY-MM-DD）
6	经营期限截止	经营终止时间或“长期”
7	实名认证状态	0- 未认证 1- 已认证
8	实名认证方式	0- 人工核验 1- 对公账户打款（采用此方式需要法人提供法人对公账户、开户银行、开户名） 2- 市场监管总局认证 3- 其它
9	实名认证时间	完成实名认证时间
10	法定代表人或负责人姓名	法定代表人姓名
11	法定代表人或负责人证件号	法定代表人公民身份号码
12	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
13	法定代表人或负责人实名认证方式	同个人身份标准
14	身份状态	0- 不可用 1- 可用

表5 法人或其他组织用户身份附属信息

序号	用户附加信息	说明
1	注册地址	可选，工商登记注册地址
2	注册金额	可选，以人民币计，单位万元
3	注册日期	可选，企业成立日期
4	经营范围	可选，登记机关认可的业务范围
5	行业类型	可选，参照《GB/T 4754—2017 国民经济行业分类》进行行业分类工作
6	行业小类	可选，参照《GB/T 4754—2017 国民经济行业分类》进行行业分类工作
7	电子营业执照	可选，数字化副本，支持扫码验真

序号	用户附加信息	说明
8	核准机构	可选，登记机关或审批部门
9	社保卡卡号	可选，法定代表人采用社保卡认证时需提供
10	社保卡发放地	可选，法定代表人采用社保卡认证时需提供
11	纳税人识别号	可选，用于税务或跨境业务

表6 法人或其他组织用户身份可验附件

序号	用户可验信息	说明
1	行业资质证书	可选，如建筑资质、电信业务许可证、ICP 证等
2	产品或服务合规认证	可选，如 ISO9001、ISO27001、CMMI、绿色认证等
3	企业信用评级	可选，如 AAA 级信用企业、征信报告评分等，来自第三方信用机构
4	纳税信用等级	可选，由税务部门签发的年度纳税信用评价等级
5	商标/知识产权登记	可选，商标局/版权局签发，支持二维码在线验真
6	其他第三方可信声明	可选，如工商联会、认证联盟、区块链联盟等发布的业务合规证明或会员资质

6.1.3 法人或其他组织经办人身份信息

法人或其他组织经办人身份信息包含法人或其他组织经办人姓名、法人或其他组织经办人身份证号码、法人或其他组织名称、统一社会信用代码等信息，使用“统一社会信用代码+经办人证件号码”作为唯一标识。

法人或其他组织经办人用户身份信息包括基础信息、附属信息与可验附件，详细内容见表7-9。

表7 法人经办人用户身份基础信息

序号	经办人身份信息	说明
1	经办人姓名	经办人姓名
2	经办人身份标识	由区域/行业功能节点生成，唯一标识经办人身份
3	经办人证件类型	经办人证件类型：中华人民共和国居民身份证、护照、军官证等
4	经办人证件号码	经办人证件号码
5	经办人实名认证等级	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
6	经办人实名认证方式	1-公安部、人社部实名服务 2-国家政务服务平台实名服务 3-微信、支付宝、通讯运营商等第三方平台
7	经办人授权方式	1- 管理员确认 2- 上传授权书 3- 短信或邮件确认
8	统一社会信用代码	统一社会信用代码

序号	经办人身份信息	说明
9	身份状态	0- 不可用 1- 可用
10	认证日期	首次实名认证通过时间（格式：YYYY-MM-DD）

表8 法人或其他组织经办人用户身份附属信息

序号	经办人附加信息	说明
1	法人或其他组织名称	法人或其他组织名称
2	法人统一社会信用代码	统一社会信用代码
3	电子营业执照	可选，电子营业执照
4	社保卡卡号	可选，法定代表人采用社保卡认证时需提供
5	社保卡发放地	可选，法定代表人采用社保卡认证时需提供
6	支付宝账号	可选
7	微信账号	可选

表9 法人或其他组织经办人身份可验附件

序号	经办人可验信息	说明
1	授权书/委托书	可选，经由电子签章/认证方式签发的正式代理授权文件，明确授权范围、权限、期限
2	公证处出具的代理声明	可选，如需要在跨地区或跨国业务中使用，具备法律效力的身份与权限声明文件
3	行业资质类委托备案证明	可选，如经办人代表企业申请电信、建筑类业务时附带的实名责任书或行业备案文件
4	其他第三方可验证信息	可选，如由 CA 机构、联盟平台或行业监管机构签发的用户身份或角色凭证

6.2 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。其唯一标识由区域/行业功能节点下发，需绑定其网络访问信息（IP、域名）和部署实体的组织信息。接入连接器身份信息包括基础信息、附属信息与可验附件，详细规格见表10-12。

表10 接入连接器身份基础信息

序号	接入连接器身份信息	说明
1	接入连接器名称	接入连接器的注册名称，需与部署文档一致
2	接入连接器身份标识	由区域/行业功能节点下发，唯一标识连接器身份
3	IP 地址列表	与网络接口绑定的静态/动态 IP，支持多地址配置，格式：IPv4/IPv6
4	域名列表	域名列表，以数组方式提交
5	接入方式	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
6	所属法人或其他组织名称	所属法人或其他组织名称
7	所属法人或其他组织统一社会信用代码	所属法人或其他组织统一社会信用代码
8	可信身份凭证	凭证信息（数字证书、DID 等），由平台认可的签发机构生成
9	凭证颁发日期	凭证颁发日期（格式：YYYY-MM-DD）

表11 接入连接器身份附属信息

序号	接入连接器附加信息	说明
1	可验证身份签发单位	可信身份凭证的签发单位
2	供应商名称	供应商名称
3	供应商代码	供应商代码
4	产品 SN 号	出厂唯一 SN 编号
5	产品版本号	产品版本号，用于补丁管理和漏洞响应
6	连接器类型	0-标准型 1-全功能型
7	设备 MAC 地址	物理设备唯一标识符（若有多台，只登记管理服务器 mac 地址）

表12 接入连接器身份可验附件

序号	接入连接器可验信息	说明
1	网络接入资质认证	如工信部核发的互联网接入服务许可、VPN 接入资质等
2	等级保护（等保 2.0）测评结果	具备国家网络安全等级保护测评资质，含系统/设备测评等级与有效期
3	网络安全产品备案证明	如国家网信办或公安机关备案的防火墙/网关产品登记信息
4	加密模块认证	如密码管理局颁发的 SM 系列算法模块认证书
5	软件供应链合规声明	包含安全 SBOM 清单、安全更新机制合规性声明
6	安全漏洞修复声明	由供应商出具的修复已知漏洞的声明，附漏洞编号与修复记录
7	通信协议兼容性认证	如支持 OIDC/SAML 等跨平台协议的互操作性报告
8	硬件可信执行环境（TEE）认证	具备可信启动、安全执行、物理隔离能力的设备认证
9	接入行为审计合规报告	具备行为记录留存、数据访问控制和审计能力的外部审计报告
10	第三方认证声明	如由行业联盟、CA 机构等出具的合规性、互操作性、性能认证等声明材料

6.3 平台身份信息内容

平台身份信息分为业务节点、区域/行业功能节点、全域功能节点三种类型，包含平台名称、平台标识、所属法人或其他组织名称等。平台身份信息以平台标识为唯一标识。基础信息、附属信息与可验附件详细内容见表13-15。

表13 平台身份基本信息

序号	平台身份信息	说明
1	平台名称	平台名称
2	平台身份标识	平台身份的唯一标识，唯一
3	平台 IP 地址列表	平台 IP 地址列表，以数组方式提交
4	平台域名列表	平台域名列表，以数组方式提交
5	所属法人或其他组织名称	所属法人或其他组织名称
6	所属法人或其他组织统一社会信用代码	所属法人或其他组织统一社会信用代码
7	可信身份凭证	可信身份凭证信息（数字证书、DID 等）
8	凭证颁发日期	凭证颁发日期

表14 平台身份附属信息

序号	平台附加信息	说明
1	平台节点类型	0-业务节点，1-区域功能节点，2-全域功能节点
2	所属行业分类代码	按照《GB/T 4754—2017》分类，用于监管与统计分析
3	服务覆盖范围	指定平台业务服务的行政区或行业边界（如“北京市”“电力行业”
4	安全责任人联系方式	用于审计或响应事件对接（如应急处置、违规行为举报）
5	运维服务商名称	平台系统维护单位，如使用托管或第三方安全服务
6	系统部署环境说明	云上/本地/混合部署，并注明所属平台
7	其他可选说明字段	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

表15 平台身份可验附件

序号	平台可验信息	说明
1	平台备案信息	工信部、网信办或行业主管部门的备案号与核准状态
2	平台合规性审计报告	如 ISO27001 审计报告、数据合规评估报告等
3	API 安全网关认证	平台对外提供接口的认证网关安全性评估结果
4	第三方评估/联盟认证	包括行业联盟认证、国家新型基础设施试点平台认定等

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图2。

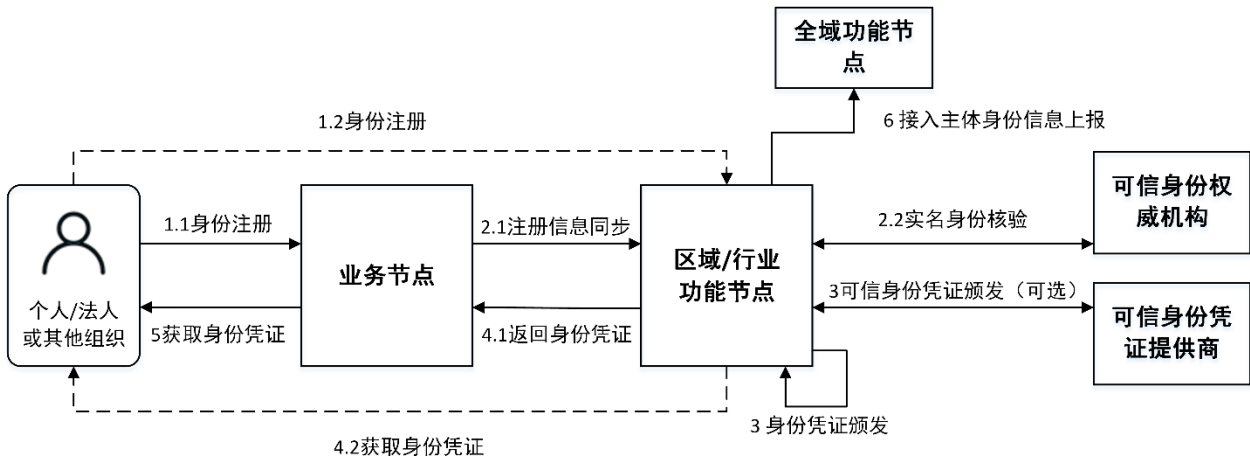


图2 个人身份注册流程

流程说明：

- a) **注册申请：**个人/法人或其他组织在业务节点或区域/行业功能节点发起身份注册，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，业务节点应将注册信息同步至对应的区域/行业功能节点，区域/行业功能节点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：**核验通过后，区域/行业功能节点可自行签发或通过可信身份凭证提供商签发可信身份凭证，凭证应具备唯一性、完整性、可验证性；
- d) **注册完成：**身份凭证返回至业务节点，由业务节点或区域/行业功能节点向用户反馈注册结果，完成身份注册；
- e) **上报归档：**区域/行业功能节点应将注册成功的主体身份信息上报至全域功能节点备案，支持跨域互信、全网可识别。

7.1.1.2 法人或其他组织经办人身份注册

当法人或其他组织委托业务经办人代表法人或其他组织参与数据流通业务活动时，需在进行法人或其他组织经办人身份注册，流程见图3。

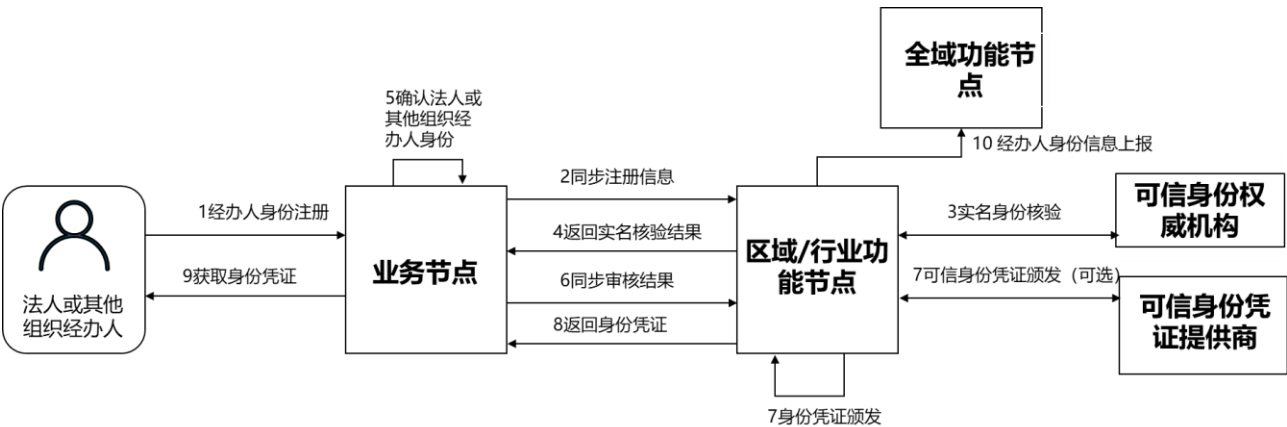


图3 法人或其他组织经办人身份注册流程

流程说明：

- a) **注册申请：**经办人在业务节点进行身份注册，提交个人实名材料及法人授权材料，系统应绑定法人统一社会信用代码与经办人证件号码，构成联合唯一标识；
- b) **信息同步：**业务节点将注册信息同步至对应的区域/行业功能节点，区域/行业功能节点对接身份权威机构申请身份核验，获取核验结果并返回至业务节点；
- c) **经办人身份确认：**业务节点依据法人单位提供的授权方式（如授权书上传、管理员确认）完成经办人身份合规性审核，并同步结果至区域/行业功能节点；
- d) **凭证签发与反馈：**区域/行业功能节点根据确认结果为经办人签发可信身份凭证，并反馈至业务节点；
- e) **注册完成：**经办人通过业务节点查询注册结果，凭已签发的身份凭证可代表法人或组织开展数据流通活动；
- f) **上报归档：**最后，区域/行业功能节点将经办人身份信息上报全域功能节点备案。

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

个人/法人或其他组织进行身份变更流程见图4。

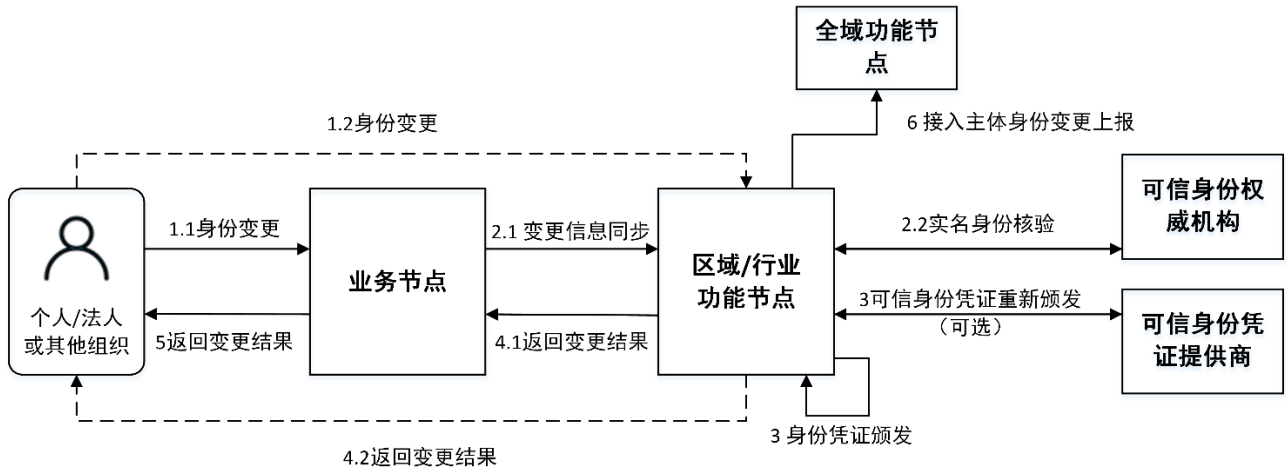


图4 个人/法人或其他组织身份变更流程

流程说明：

- 发起变更申请：**个人/法人或其他组织在业务节点或区域/行业功能节点提交身份变更请求，需同步提交实名认证所需的更新材料；
- 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区域/行业功能节点；
- 实名复核：**区域/行业功能节点向可信身份权威机构申请身份核验，获取核验结果；
- 凭证重签发：**区域/行业功能节点确认身份真实性之后，为主体重新签发身份凭证，并注销旧凭证；
- 反馈结果通知：**区域/行业功能节点反馈可信身份凭证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；
- 全域归档上报：**用户完成注册后，区域/行业功能节点将更新后的主体身份信息上报至全域功能节点。

7.1.2.2 法人或其他组织经办人身份变更

法人或其他组织经办人进行身份变更流程见图5。

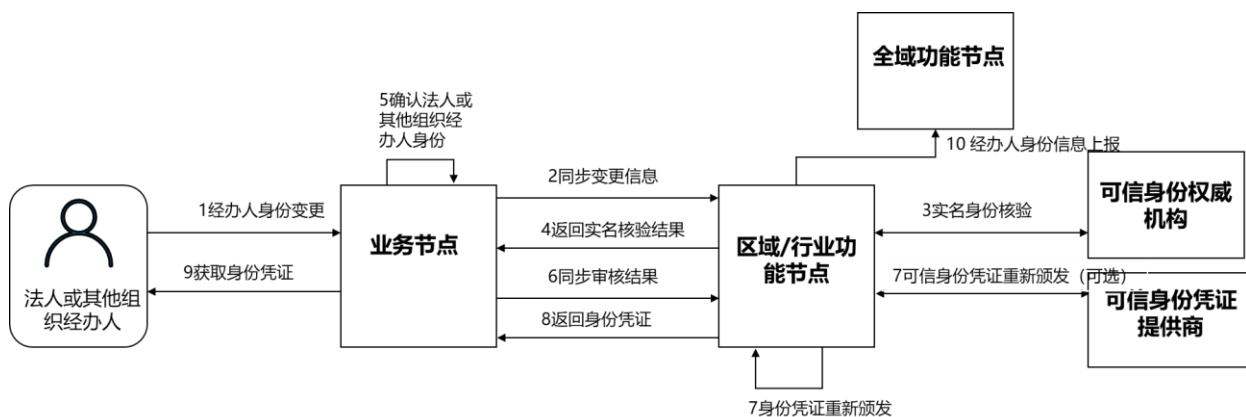


图5 法人或其他组织经办人身份变更流程

流程说明：

- 发起变更申请：**法人或其他组织经办人在业务节点提交身份变更申请，更新个人实名或授权信息；
- 信息转交与实名核验：**业务节点将身份变更请求转交区域/行业功能节点。区域/行业功能节点调用可信身份权威机构，对经办人更新后的实名信息进行复核，获取核验结果；区域/行业功能节点将身份核验结果返回至业务节点；
- 法人授权重确认：**业务节点需重新核实经办人与法人之间的授权关系，并将经办人确认结果同步至区域/行业功能节点；
- 凭证重签发：**区域/行业功能节点依据审核结果为经办人重签身份凭证；
- 结果反馈与归档：**凭证同步返回至业务节点，由其反馈给经办人确认完成变更操作；区域/行业功能节点同时上报更新后的身份信息至全域功能节点。

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，流程见图6。

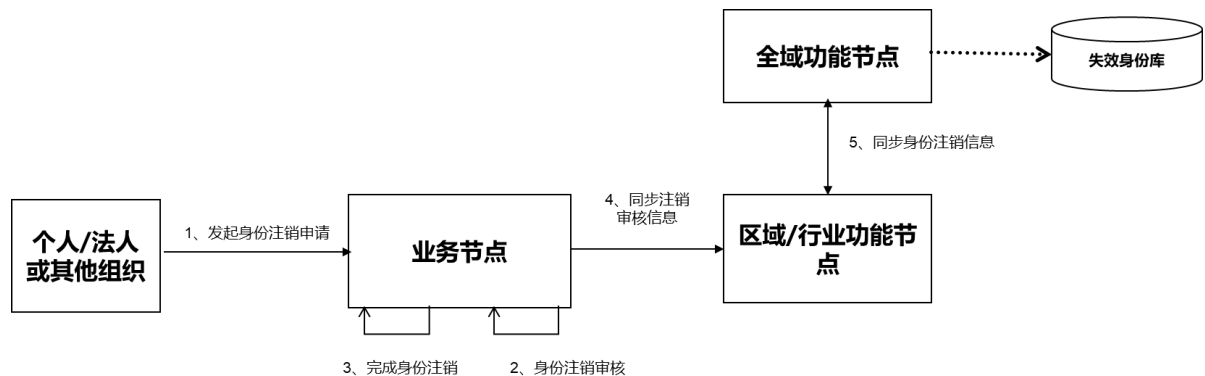


图6 个人、法人或其他组织身份注销流程

流程说明：

- a) **注销申请提交：**个人、法人或其他组织向业务节点可在业务节点发起身份注销申请。对于法人/其他组织用户，应先完成所关联经办人的身份凭证注销后方可继续注销法人身份；
- b) **业务节点审核：**业务节点对申请主体身份、注销请求的合规性进行审核，包括检查是否存在未结算业务、未完成授权操作或安全风险提示等；
- c) **信息同步处理：**审核通过后，业务节点将注销信息同步至所属区域/行业功能节点；
- d) **状态变更与归档：**区域/行业功能节点将该身份状态标记为“已注销”或“失效”，并将身份注销信息同步上报至全域功能节点。

7.1.3.2 法人或其他组织经办人身份注销

法人或其他组织经办人因业务变更或离职后，应在业务节点完成注销，并向其它区域/行业功能节点以及全域功能节点同步，身份注销流程见图7。

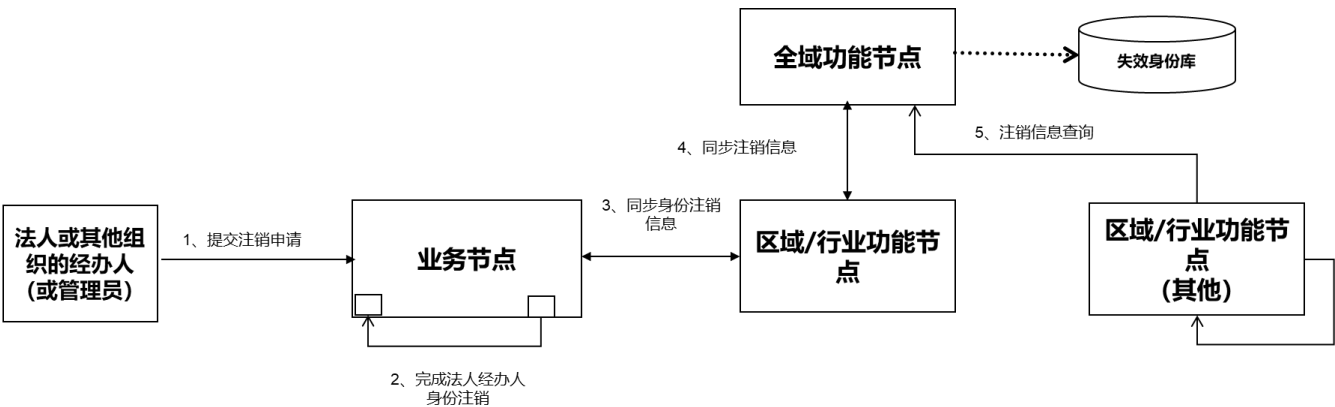


图7 法人或其他组织经办人身份注销流程

流程说明：

- a) **注销发起：**法人或其他组织的经办人或法人或其他组织管理员登录业务节点，提交身份注销申请；
- b) **本地同步与执行：**业务节点进行法人或其他组织的经办人身份注销，同步身份注销信息至区域/行业功能节点；

- c) **全域同步归档：**区域/行业功能节点接收到注销信息后，同步身份注销信息至全域功能节点；全域功能节点将该身份纳入失效身份数据库，并对各节点开放查询接口
- d) **失效同步机制：**其它区域/行业功能节点可按需调用接口查询该身份状态，自动同步失效身份处理流程；
- e) **主体保留机制：**经办人注销操作不影响其自然人主体身份的持续存在。若用户需注销个人身份，可参考 7.1.3.1 流程单独发起申请。

7.1.4 用户登录认证

用户登录认证是指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的过程。本节定义常见登录认证方式及其技术处理流程，包括账号口令、数字证书、DID等。

7.1.4.1 账号口令登录

用户采用账号口令方式登录业务节点，流程见图8。

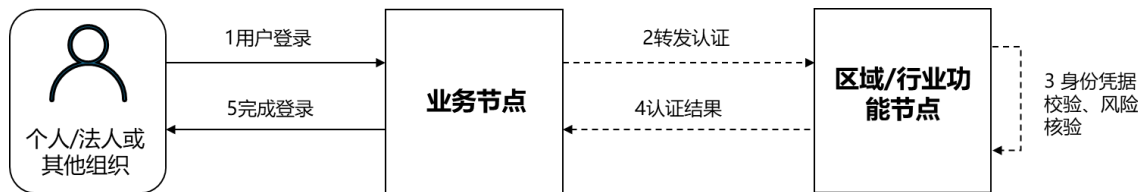


图8 平台登录认证流程（账号口令登录）

流程说明：

- a) **登录发起：**用户通过用户名与口令组合方式向业务节点发起登录请求，系统可配置双因素认证（如短信验证码、一次性口令器 OTP 等）增强安全性；
- b) **凭证验证：**业务节点将认证信息转发至区域/行业功能节点，由后者完成账号与凭证（密码、验证码等）的一致性校验及风险评估（如设备指纹识别、IP 地理异常判断），然后返回认证结果给业务节点；
- c) **登录建立：**认证通过后，业务节点向数据流通平台发起会话建立请求，并根据结果完成用户登录。系统应记录登录日志并生成登录令牌用于后续操作授权。

7.1.4.2 数字证书登录

用户采用数字证书方式登录业务节点，流程见图9。

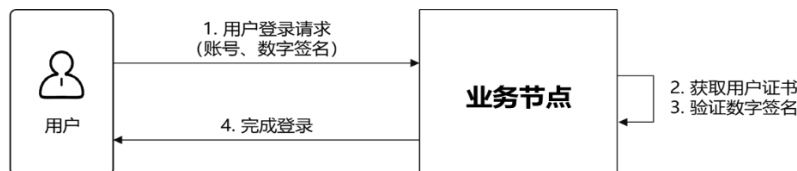


图9 平台登录认证流程（数字证书登录）

流程说明：

- a) **登录发起：**用户选择以数字证书方式进行登录，并向业务节点提交客户端持有的数字证书；
- b) **签名验证：**业务节点依据平台预置的 CA 根证书，完成对用户提交的证书合法性校验与数字签名验证；
- c) **登录确认：**认证通过后，系统为用户建立登录会话，并返回认证成功结果。

7.1.4.3 DID（去中心化身份）登录

用户通过DID方式登录业务节点，流程见图10。

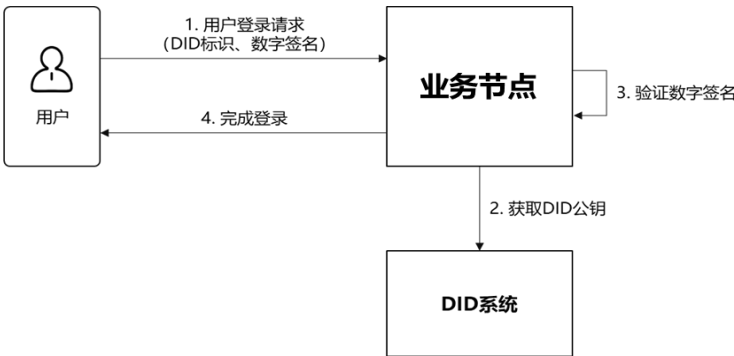


图10 平台登录认证流程（DID 登录）

流程说明：

- a) **登录发起：**用户使用 DID 私钥发起登录认证，采用挑战响应机制生成签名响应；
- b) **公钥获取：**系统从 DID 解析服务获取用户绑定的公钥，用于验证用户签名；
- c) **认证完成：**用户验证 DID 数字签名，返回登录结果，完成用户登录认证。

7.1.5 跨域身份认证

跨域身份认证是指接入主体（包括个人、法人或其他组织及其经办人）在已完成用户身份注册的情况下，尝试在新地域或行业场景下登录时，其原注册节点通过可信链路实现身份数据调用与认证授权的过程，流程见图11。

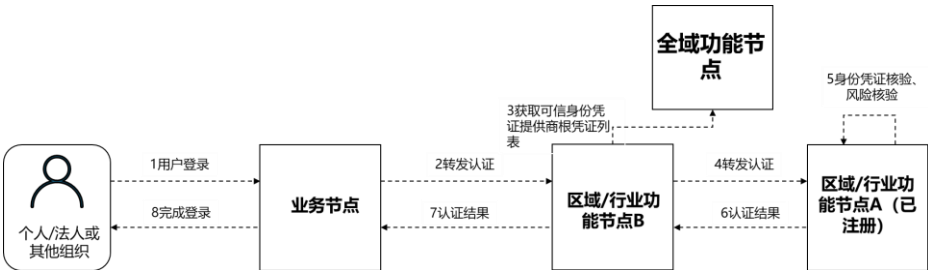


图11 跨域用户身份信息认证流程

流程说明：

- a) **跨域登录发起：**用户（已在 A 市注册）首次尝试在 B 市业务节点登录，触发跨域身份认证流程；
- b) **身份认证请求转发：**B 市区域/行业功能节点向用户注册所在地——A 市区域/行业功能节点发起身份认证重定向请求；
- c) **原始节点认证与授权：**A 市区域/行业功能节点对用户发起登录认证流程，用户在本地节点完成授权，系统根据授权策略生成跨域授权令牌；
- d) **授权令牌传递与验证：**用户将获取的授权令牌提交至 B 市区域/行业功能节点，后者依据令牌校验机制验证其合法性后，向 A 市节点请求用户身份数据；
- e) **身份数据传输与缓存：**A 市节点将授权范围内的身份信息返回至 B 市节点。B 市区域/行业功能节点根据接入策略缓存用户身份信息，并完成本地身份认证流程。

7.2 接入连接器身份注册认证

接入连接器是连接接入主体与数据流通平台之间的关键组件，其身份的合法性、唯一性与可验证性直接影响系统的可信边界。本节定义接入连接器身份注册与注销的管理流程。

7.2.1 接入连接器身份注册

接入连接器身份注册流程见图12。

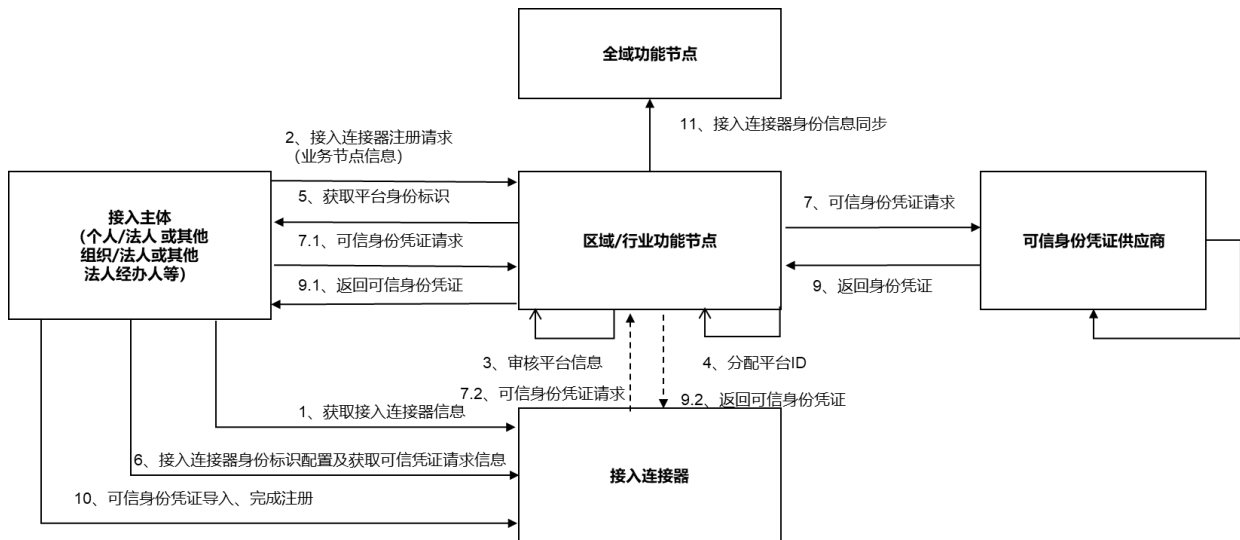


图12 接入连接器身份注册流程

流程说明：

- a) **获取设备信息：**用户完成接入连接器软硬件准备，获取设备基础信息；
- b) **注册申请提交：**用户向所属区域/行业功能节点提交接入连接器注册请求，并同步上传相关身份基础信息及可验附件；
- c) **信息审核与身份标识生成：**区域/行业功能节点依据接入要求及可信供应商清单，审核提交信息，审核通过后生成并分配接入连接器唯一身份标识区域/行业功能节点审核接入连接器信息；
- d) **身份标识下发：**区域/行业功能节点将接入连接器身份标识反馈给用户，由用户配置至接入连接器本地系统；
- e) **凭证申请生成：**配置完成后，接入连接器生成可信身份凭证请求（包括身份标识、设备公钥、域名/IP 等），由用户提交至区域/行业功能节点；
- f) **凭证签发请求转发：**区域/行业功能节点审核凭证请求后，转发至可信身份凭证提供商；
- g) **可信凭证签发与返回：**可信身份凭证提供商签发设备专属用户身份凭证，并经由区域/行业功能节点返回用户；
- h) **凭证导入与启用：**用户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。

可信身份凭证结构见附录 A。

7.2.2 接入连接器身份注销

接入连接器身份注销流程见图13。

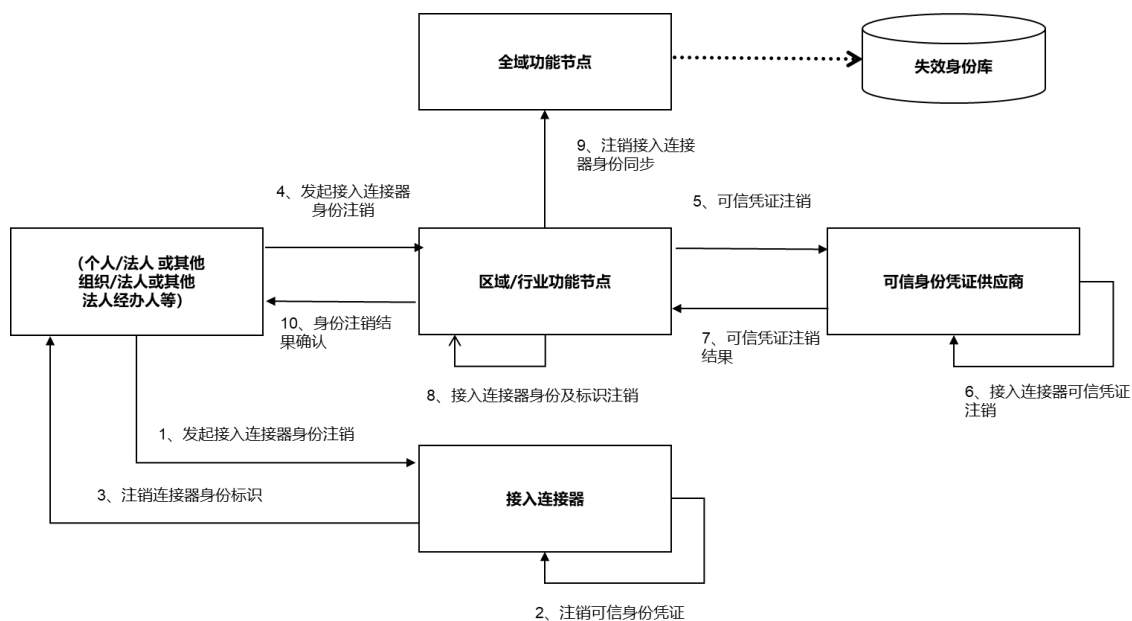


图13 接入连接器身份注销流程

流程说明：

- a) **信息准备与注销申请：**用户获取已注册的接入连接器身份信息，并向区域/行业功能节点发起身份注销申请；
- b) **信息核验与注销处理：**区域/行业功能节点对接入连接器身份信息进行审核，确认后将其状态置为待注销，并向可信身份凭证提供商发起凭证吊销请求；
- c) **凭证吊销与反馈：**可信身份供应商对接入连接器可信凭证进行吊销，并将结果返回区域/行业功能节点；
- d) **标识注销与同步：**区域/行业功能节点完成接入连接器身份标识注销，并将注销结果同步至全域功能节点；
- e) **注销结果反馈：**区域/行业功能节点将身份注销结果确认信息返回至用户。

7.2.3 接入连接器身份验证

7.2.3.1 接入连接器与区域/行业功能节点双向认证

接入连接器与区域/行业功能节点的双向认证流程见图14。

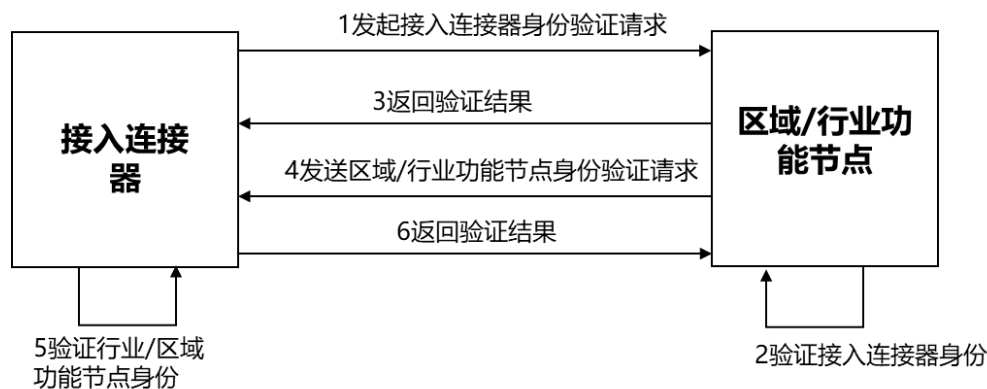


图14 接入连接器与区域/行业功能节点双向认证流程

流程说明：

- a) **连接器发起验证：**接入连接器向区域/行业功能节点发起身份验证请求，包含可信身份凭证及签名等信息；
- b) **节点验证连接器身份：**区域/行业功能节点验证接入连接器的身份校验连接器身份凭证的签发机构、有效期、吊销状态等，并校验签名的合法性，返回验证结果；
- c) **节点发起反向验证：**为防止仿冒平台节点，区域/行业功能节点也应向连接器发起身份验证请求，并附带自身可信身份凭证与签名；
- d) **连接器验证节点身份：**接入连接器校验平台凭证签发来源、有效性和签名后反馈结果，完成双向身份验证。

7.2.3.2 接入连接器之间双向认证

接入连接器之间基于可信身份凭证完成双向认证，即通过交换可信身份凭证以及对双方数字签名的验证实现身份认证，接入连接器的可信身份平台证由可信身份提供商颁发。具体认证过程通过HTTPS协议完成。连接器之间的身份认证流程见图15。

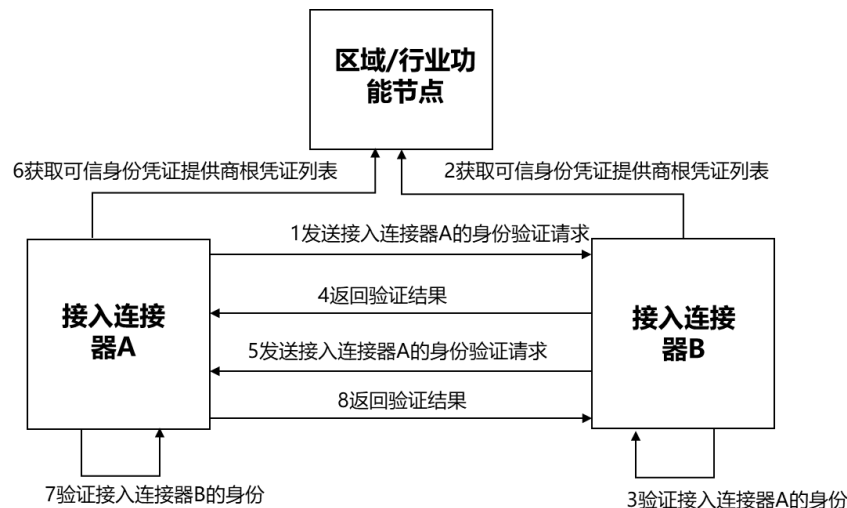


图15 接入连接器之间双向认证流程

流程说明：

- a) **A 发起认证请求：**接入连接器 A 向接入连接器 B 发起身份验证请求，包含可信身份凭证及签名等信息；
- b) **B 获取根凭证：**接入连接器 B 向区域/行业功能节点获取可信身份提供商根凭证列表，并在本地缓存；
- c) **B 验证 A 身份：**连接器 B 完成凭证链合法性校验、数字签名验证，并将认证结果返回给 A；
- d) **B 发起认证请求：**接入连接器 B 向接入连接器 A 发起身份验证请求，包含可信身份凭证及签名等信息；
- e) **A 获取根凭证：**接入连接器 A 向区域/行业功能节点获取可信身份提供商根凭证列表，并在本地缓存；
- f) **A 验证 B 身份：**连接器 A 完成对 B 的身份凭证及签名校验，验证结果返回 B，完成双向身份认证。

7.3 平台身份认证

7.3.1 平台身份注册

平台身份注册流程见图16。

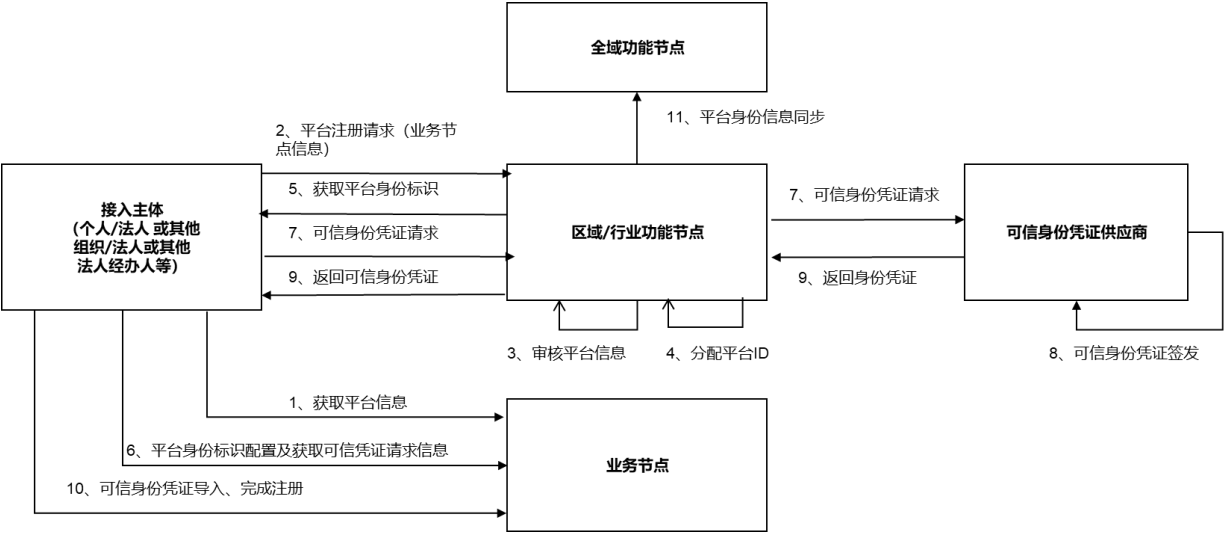


图16 平台身份注册流程

流程说明：

- a) **信息准备：**用户获取待注册平台的关键信息；
- b) **注册申请提交：**用户向所属区域/行业功能节点提交平台注册申请，并附带平台基础信息及身份相关可验附件；
- c) **信息审核与标识分配：**区域/行业功能节点对平台资质、部署架构与接入用途进行审核，审核通过后为平台分配唯一平台身份标识；
- d) **标识获取与配置：**用户获取平台身份标识后，应将其绑定配置于平台系统中，用于后续凭证生成与身份标识统一；
- e) **凭证请求生成：**平台根据身份标识生成可信身份凭证请求（包含接入身份标识、域名信息、公钥等）；
- f) **凭证签发请求提交：**用户上传可信身份凭证请求至区域/行业功能节点，区域/行业功能节点审核后转发至可信身份提供商请求平台的可信身份凭证；
- g) **可信凭证签发与回传：**可信身份提供商签发可信身份凭证，并经由区域/行业功能节点返回用户；
- h) **凭证导入与启用：**用户将平台用户身份凭证导入平台系统，完成身份认证配置。
- i) **全域同步归档：**区域/行业功能节点将已认证平台身份信息同步至全域功能节点。

7.3.2 平台身份注销

平台身份注销流程见图17。

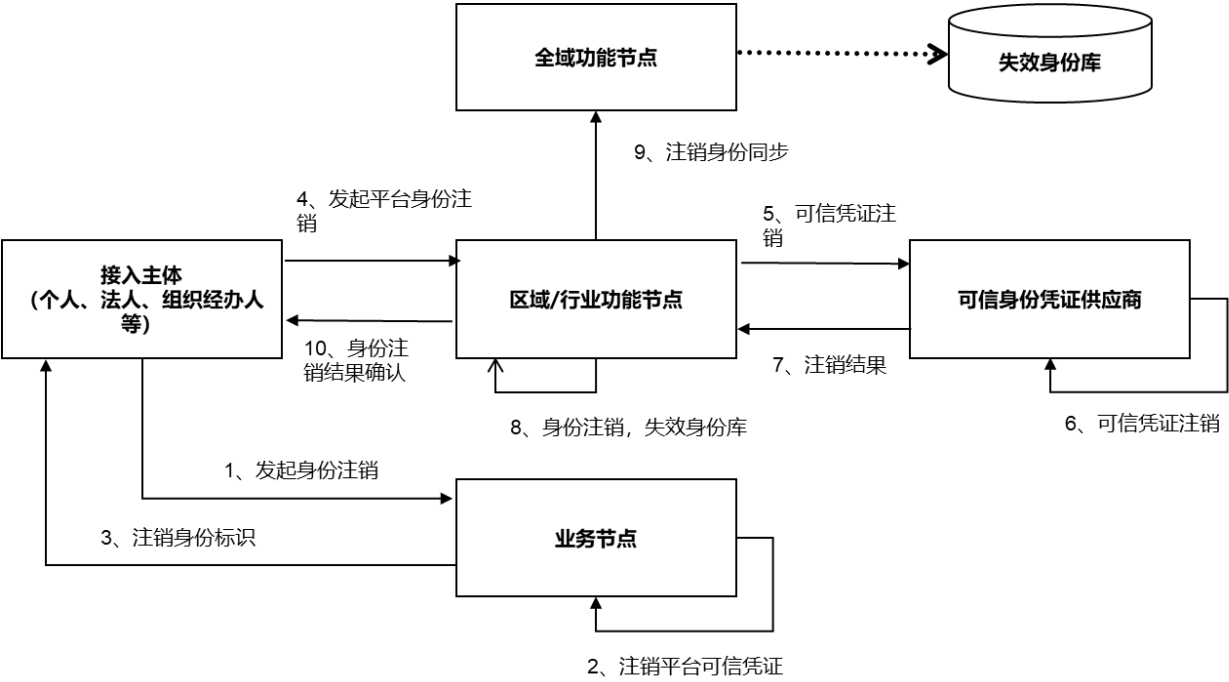


图17 平台身份注销认证流程

流程说明：

- a) **信息准备：**用户获取平台信息；
- b) **注销申请提交：**用户向区域/行业功能节点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；
- c) **信息审核与凭证吊销：**区域/行业功能节点审核注销请求后，将平台身份凭证吊销指令发送至可信身份凭证提供商；
- d) **凭证注销处理：**可信身份凭证提供商执行平台凭证吊销操作，并返回吊销结果至区域/行业功能节点；
- e) **标识注销与归档：**区域/行业功能节点将该平台标识设为“已注销”，并同步注销信息至全域功能节点；
- f) **注销结果反馈：**区域/行业功能节点向用户反馈注销完成确认信息，注销流程结束。

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见图18。

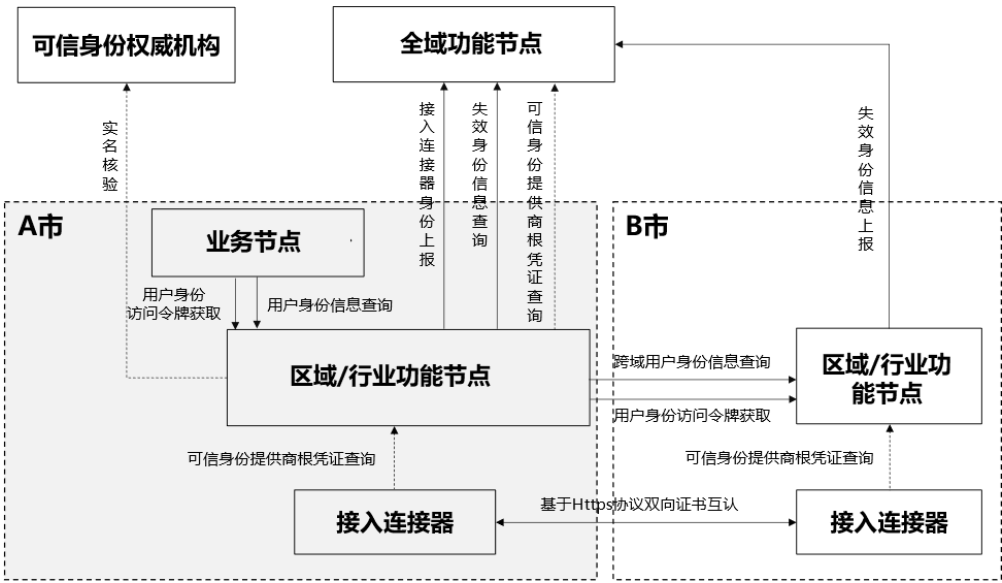


图18 统一用户身份管理和接入总体架构图

8.2 接口总体要求

8.2.1 通讯协议

本标准涉及的所有接口均使用HTTPS协议。

8.2.2 请求方式要求

本标准涉及的所有接口均采用POST请求方式调用。

8.2.3 消息头要求

Http消息头应包含见表16。

表16 Http 消息头

字段名称	约束	类型	长度	取值说明
msgcode	必选	String	20	接口编码，用于判断请求方调用接口，取值参见章节 8.3.1
msgversion	必选	String	20	接口版本
timestamp	必选	String	13	请求方时间戳，毫秒级 示例：1562589083316
sequenceNum	必选	String	32	流水号用于标识一次报文请求，由请求方生成
signValue	必选	String	128	签名值，由调用方的可信身份凭证对除签名值外的所有参数进行签名

8.2.4 请求参数要求

请求参数应当以JSON格式进行组织，JSON消息中的所有字段均为小写，使用UTF-8格式进行编码并序列化后进行参数。

8.2.5 返回消息格式要求

消息体返回接口请求的应答信息，包括返回消息状态码（code字段）和返回结果描述（message字段）及应答的内容（data字段）三部分，见表17。

表17 返回消息

序号	参数名称	数据类型	长度	约束	取值说明
1	code	String	64	必选	返回消息的状态码
2	message	String	255	必选	返回消息结果描述
3	data	--	--	必选	返回接口响应的具体数据

报文样例见附录B。

8.3 接口定义

8.3.1 接口列表

接口列表见表18。

表18 接口列表

序号	接口名称	接口编码	调用方	提供方
1	身份信息访问令牌获取接口	GetToken	业务节点 区域/行业功能节点	区域/行业功能节点
2	个人用户身份信息查询接口	GetPersonInfo	业务节点	区域/行业功能节点
3	法人或其他组织用户身份信息查询接口	GetEnterpriseInfo	业务节点	区域/行业功能节点
4	法人或其他组织经办人用户身份信息查询接口	GetOperatorInfo	业务节点	区域/行业功能节点
5	跨域个人用户身份信息查询接口	GetPersonBaseInfo	区域/行业功能节点	区域/行业功能节点
6	跨域法人或其他组织用户身份信息查询接口	GetEnterpriseBaseInfo	区域/行业功能节点	区域/行业功能节点
7	跨域法人或其他组织经办人用户身份信息查询接口	GetOperatorBaseInfo	区域/行业功能节点	区域/行业功能节点
8	可信身份提供商根凭证列表查询接口	GetIdentityProviderList	接入连接器	区域/行业功能节点
9	接入连接器身份信息上报接口	SyncConnectorInfo	区域/行业功能节点	全域功能节点
10	经办人失效身份信息上报接口	SyncLogoffInfo	区域/行业功能节点	全域功能节点
11	经办人失效身份信息查询接口	GetOperatorStatus	区域/行业功能节点	全域功能节点

12	可信身份提供商根凭证列表查询接口	GetIdentityProviderList	区域/行业功能节点	全域功能节点
----	------------------	-------------------------	-----------	--------

8.3.2 区域/行业功能节点对接接口

8.3.2.1 身份信息访问令牌获取接口

接口名称	身份信息访问令牌获取接口				GetToken	
接口访问地址	/GetToken				HTTP Method	POST
功能	本接口适用于两种场景 1、 业务节点注册时，业务节点携带用户授权令牌向区域/行业功能节点发起请求，获取用户身份信息访问令牌。 2、 跨平台身份信息同步时，区域/行业功能节点携带用户授权令牌向区域/行业功能节点（用户已注册）发起请求，获取用户身份信息访问令牌。					
请求参数						
序号	参数名称	数据类型	长度	约束	说明	
1	authCode	String	64	必选	通过区域/行业功能节点完成身份信息授权后，为用户生成的授权令牌	
响应参数						
序号	参数名称	数据类型	长度	约束	说明	
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）	
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）	
3	data				接口响应数据	
3.1	token	String	64	必选	身份信息访问令牌，格式见附录 D	

8.3.2.2 个人用户身份信息查询接口

接口名称	个人用户身份信息查询接口				GetPersonInfo	
接口访问地址	/GetPersonInfo				HTTP Method	POST
功能	在个人用户在区域/行业功能节点完成注册，并通过业务节点登录时，业务节点向区域/行业功能节点发起登录认证（重定向），经过用户进行身份信息授权后返回用户授权令牌（token），业务节点调用本接口，查询个人用户身份信息。					
请求参数						
序号	参数名称	数据类型	长度	约束	说明	
1	token	String	64	必选	通过授权令牌获取的用户身份信息访问令牌，用于验证并获取用户身份信息，见附录 D	
响应参数						
序号	参数名称	数据类型	长度	约束	说明	
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）	
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）	
3	data				接口响应数据	
3.1	baseInfo	--			身份基本信息	

3.1.1	identityCode	String	64	必选	唯一身份标识
3.1.2	fullName	String	50	必选	姓名
3.1.3	certType	String	2	必选	证件类型
3.1.4	certCode	String	50	必选	证件号码
3.1.5	certEffdate	String	Date	必选	证件号码有效起始日期
3.1.6	certExpdate	String	Date	必选	证件号码有效截止日期
3.1.7	phone	String	11	必选	手机号，唯一
3.1.8	authLevel	String	2	必选	个人实名认证等级
3.1.9	authType	String	2	必选	个人实名认证方式
3.1.10	authTime	String	Date	必选	实名认证时间
3.1.11	identityStatus	String	2	必选	身份状态
3.2	extendInfo	--			身份附加信息
3.2.1	nationality	String	100	可选	国籍
3.2.2	sex	String	20	可选	性别
3.2.3	birthDate	String	20	可选	出生年月
3.2.4	socialSecurityCard	String	50	可选	社保卡卡号
3.2.5	socialSecurityCardSite	String	100	可选	社保卡发放地
3.2.6	alipayAccount	String	50	可选	支付宝账号
3.2.7	weixinAccount	String	50	可选	微信账号
3.2.8	userEmail	String	50	可选	邮箱地址
3.2.9	userAddress	String	100	可选	联系地址
3.3	attachInfo	--			身份可验信息
3.3.1	attachType	String	20	可选	附件类型（如学历证书、职业资格证等）
3.3.2	attachName	String	100	可选	附件名称，如“xx 大学本科毕业证”
3.3.3	attachCode	String	64	可选	附件编号
3.3.4	issueOrg	String	100	可选	附件签发机构
3.3.5	issueDate	String	Date	可选	签发日期
3.3.6	expireDate	String	Date	可选	到期日期（如适用）
3.3.7	verifyUrl	String	255	可选	附件验证地址或区块链凭证索引
3.3.8	description	String	200	可选	附件描述信息

8.3.2.3 法人或其他组织用户身份信息查询接口

接口名称	法人或其他组织用户身份信息查询接口			GetEnterpriseInfo	
接口访问地址	/GetEnterpriseInfo			HTTP Method	POST
功能	在法人或其他组织用户在区域/行业功能节点完成注册，并通过业务节点登录时，业务节点向区域/行业功能节点发起登录认证（重定向），经过用户进行身份信息授权后返回用户授权令牌（token），业务节点调用本接口，查询用户身份信息。				
请求参数					
序号	参数名称	数据类型	长度	约束	说明
1	token	String	64	必选	通过授权令牌获取的用户身份信息访问令牌，用于验证并获取用户身份信息，见附录 D

响应参数					
序号	参数名称	数据类型	长度	约束	说明
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）
3	data				接口响应数据
3.1	baseInfo	--	--		身份基本信息
3.1.1	identityCode	String	64	必选	唯一身份标识
3.1.2	enterpriseName	String	50	必选	法人或其他组织名称
3.1.3	enterpriseCode	String	50	必选	统一社会信用代码
3.1.4	enterpriseType	String	2	必选	法人或其他组织类型
3.1.5	operatingPeriodBegin	Date	--	必选	经营期限起始
3.1.6	operatingPeriodEnd	Date	--	必选	经营期限截止
3.1.7	authType	String	2	必选	实名认证方式
3.1.8	authStatus	String	2	必选	实名认证状态
3.1.9	authDate	Date	--	必选	实名认证时间
3.1.10	legalPerson	String	50	必选	法定代表人或负责人姓名
3.1.11	legalPersonCertno	String	50	必选	法定代表人或负责人证件号
3.1.12	legalPersonAuthLevel	String	2	必选	法定代表人或负责人实名等级
3.1.13	legalPersonAuthType	String	2	必选	个人实名认证方式
3.1.14	identityStatus	String	2	必选	身份状态
3.2	extendInfo	--	--		身份附加信息
3.2.1	enterpriseAddress	String	200	可选	注册地址
3.2.2	regAmount	String	50	可选	注册金额
3.2.3	regDate	Date	--	可选	注册日期
3.2.4	businessScope	String	200	可选	经营范围
3.2.5	industryCategory	String	50	可选	行业类型
3.2.6	industryCategory2	String	50	可选	行业小类
3.2.7	businessLicense	String	200	可选	电子营业执照
3.2.8	approvalAuthority	String	100	可选	核准机构
3.2.9	socialSecurityCard	String	50	可选	社保卡卡号
3.2.10	socialSecurityCardSite	String	100	可选	社保卡发放地
3.2.11	legalPersonPhone	String	11	可选	法定代表人或负责人手机号
3.2.12	legalPersonEmail	String	50	可选	法定代表人或负责人邮箱
3.2.13	legalPersonStatus	String	2	可选	法定代表人或负责人身份状态
3.3	attachInfo	--	--		身份可验信息
3.3.1	attachType	String	50	可选	附件类型（如行业资质证书、信用评级等）
3.3.2	attachName	String	100	可选	附件名称，如“建筑施工总承包资质证书”
3.3.3	attachCode	String	64	可选	附件编号
3.3.4	issueOrg	String	100	可选	签发单位
3.3.5	issueDate	String	Date	可选	附件签发日期

3.3.6	expireDate	String	Date	可选	附件有效截止日期（如适用）
3.3.7	verifyUrl	String	255	可选	验证路径，可为官网 URL、区块链 Hash 或 API 接口地址
3.3.8	description	String	200	可选	附件说明或使用场景

8.3.2.4 法人或其他组织经办人身份信息查询接口

接口名称	法人或其他组织经办人身份信息查询接口				GetOperatorInfo	
接口访问地址	/GetOperatorInfo				HTTP Method	POST
功能	在法人或其他组织经办人用户在区域/行业功能节点完成注册，并通过业务节点登录时，业务节点向区域/行业功能节点发起登录认证（重定向），经过用户进行身份信息授权后返回用户授权令牌（token），业务节点调用本接口，查询法人或其他组织经办人用户身份信息。					
请求参数						
序号	参数名称	数据类型	长度	约束	说明	
1	token	String	64	必选	通过授权令牌获取的用户身份信息访问令牌，用于验证并获取用户身份信息，见附录 D	
响应参数						
序号	参数名称	数据类型	长度	约束	说明	
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）	
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）	
3	data				接口响应数据	
3.1	baseInfo	--	--		身份基本信息	
3.1.1	identityCode	String	64	必选	唯一身份标识	
3.1.2	operator	String	50	必选	经办人姓名	
3.1.3	operatorIdType	String	2	必选	经办人证件类型	
3.1.4	operatorId	String	50	必选	经办人证件编号	
3.1.5	operatorAuthLevel	String	2	必选	经办人实名认证等级	
3.1.6	operatorAuthType	String	2	必选	经办人实名认证方式	
3.1.7	authorizationType	String	2	必选	经办人授权方式	
3.1.8	enterpriseCode	String	50	必选	统一社会信用代码	
3.1.9	authStatus	String	2	必选	身份状态	
3.1.10	authTime	Date	--	必选	认证日期	
3.2	extendInfo	--	--		身份附加信息	
3.2.1	enterpriseName	String	100	必选	法人或其他组织名称	
3.2.2	businessLicense	String	100	必选	电子营业执照	
3.2.3	socialSecurityCard	String	50	可选	社保卡卡号	
3.2.4	socialSecurityCardSite	String	100	可选	社保卡发放地	
3.2.5	alipayAccount	String	50	可选	支付宝账号	
3.2.6	weixinAccount	String	50	可选	微信账号	
3.3	attachInfo	--	--		身份验证信息	
3.3.1	attachType	String	50	可选	附件类型（如授权委托书、公证声明等）	
3.3.2	attachName	String	100	可选	附件名称，如“法人授权委托书”	

3.3.3	attachCode	String	64	可选	附件编号
3.3.4	issueOrg	String	100	可选	签发单位，如公证处、行业协会等
3.3.5	issueDate	String	Date	可选	附件签发日期
3.3.6	expireDate	String	Date	可选	附件有效截止日期（如适用）
3.3.7	verifyUrl	String	255	可选	验证地址（如扫描二维码、在线验证页面或电子存证接口）
3.3.8	description	String	200	可选	附件说明或用途

8.3.2.5 跨域个人用户身份信息查询接口

接口名称	跨域用户身份信息查询接口				GetPersonBaseInfo	
接口访问地址	/GetPersonBaseInfo				HTTP Method	POST
功能	当个人用户在区域/行业功能节点完成注册后，在其他业务节点重新注册时，用户选择已注册区域/行业功能节点发起登录认证（重定向），经过用户进行身份信息授权后返回用户授权令牌（token），调用注册地区域/行业功能节点个人用户身份查询接口，获取个人用户身份信息。					
请求参数						
序号	参数名称		数据类型	长度	约束	说明
1	token		String	64	必选	通过授权令牌获取的用户身份信息访问令牌，用于验证并获取用户身份信息，见附录 D
响应参数						
序号	参数名称		数据类型	长度	约束	说明
1	code		String	10	必选	执行结果代码（详见附录 C 返回码定义）
2	message		String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）
3	data					接口响应数据
3.1	identityCode		String	64	必选	唯一身份标识
3.2	fullName		String	50	必选	姓名
3.3	certType		String	2	必选	证件类型
3.4	certCode		String	50	必选	证件号码
3.5	certEffdate		String	--	必选	证件号码有效起始日期
3.6	certExpdate		String	--	必选	证件号码有效截止日期
3.7	phone		String	11	必选	手机号，唯一
3.8	authLevel		String	2	必选	个人实名认证等级
3.9	authType		String	2	必选	个人实名认证方式
3.10	authTime		String	Date	必选	实名认证时间
3.11	identityStatus		String	2	必选	身份状态

8.3.2.6 跨域法人或其他组织用户身份信息查询接口

接口名称	跨域法人或其他组织用户身份信息查询接口			GetEnterpriseBaseInfo	
接口访问地址	/GetEnterpriseBaseInfo			HTTP Method	POST
功能	当法人或其他组织用户在区域/行业功能节点完成注册后，在其他业务节点重新注册时，用户选择已注册区域/行业功能节点发起登录认证（重定向），经过用户进行身份信息授权后返回用户授权令牌（token），调用注册地区域/行业功能节点法人或其他组织用户身份查询接口，获取用户身份信息。				

请求参数					
序号	参数名称	数据类型	长度	约束	说明
1	token	String	64	必选	通过授权令牌获取的用户身份信息访问令牌，用于验证并获取用户身份信息，见附录 D
响应参数					
序号	参数名称	数据类型	长度	约束	说明
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）
3	data				接口响应数据
3.1	identityCode	String	64	必选	唯一身份标识
3.2	enterpriseName	String	50	必选	法人或其他组织名称
3.3	enterpriseCode	String	50	必选	统一社会信用代码
3.4	enterpriseType	String	2	必选	法人或其他组织类型
3.5	operatingPeriodBegin	Date	--	必选	经营期限起始
3.6	operatingPeriodEnd	Date	--	必选	经营期限截止
3.7	authType	String	2	必选	实名认证方式
3.8	authStatus	String	2	必选	实名认证状态
3.9	authDate	Date	--	必选	实名认证时间
3.10	legalPerson	String	50	必选	法定代表人或负责人姓名
3.11	legalPersonCertno	String	50	必选	法定代表人或负责人证件号
3.12	legalPersonAuthLevel	String	2	必选	法定代表人或负责人实名等级
3.13	legalPersonAuthType	String	2	必选	个人实名认证方式
3.14	identityStatus	String	2	必选	身份状态

8.3.2.7 跨域法人或其他组织经办人身份信息查询接口

接口名称	跨域法人或其他组织经办人身份信息查询接口				GetOperatorBaseInfo	
接口访问地址	/GetOperatorBaseInfo				HTTP Method	POST
功能	当法人或其他组织经办人用户在区域/行业功能节点完成注册后，在其他业务节点重新注册时，用户选择已注册区域/行业功能节点发起登录认证（重定向），经过用户进行身份信息授权后返回用户授权令牌（token），调用注册地区域/行业功能节点法人或其他组织经办人用户身份查询接口，获取或其他组织用户身份信息。					
请求参数						
序号	参数名称	数据类型	长度	约束	说明	
1	token	String	64	必选	通过授权令牌获取的用户身份信息访问令牌，用于验证并获取用户身份信息，见附录 D	
响应参数						
序号	参数名称	数据类型	长度	约束	说明	
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）	
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）	
3	data				接口响应数据	

3.1	identityCode	String	64	必选	唯一身份标识
3.2	operator	String	50	必选	经办人姓名
3.3	operatorIdType	String	2	必选	经办人证件类型
3.4	operatorId	String	50	必选	经办人证件编号
3.5	operatorAuthLevel	String	2	必选	经办人实名认证等级
3.6	operatorAuthType	String	2	必选	经办人实名认证方式
3.7	authorizationType	String	2	必选	经办人授权方式
3.8	enterpriseCode	String	50	必选	统一社会信用代码
3.9	authStatus	String	2	必选	身份状态
3.10	authTime	Date	--	必选	认证日期

8.3.2.8 可信身份提供商根凭证列表查询接口

接口名称	可信身份提供商根凭证列表查询接口				GetIdentityProviderList	
接口访问地址	/GetIdentityProviderList				HTTP Method	POST
功能	接入连接器可调用此接口，查询对区域/行业功能节点在全域功能节点获取的已注册的可信身份提供商信息，用于验证可信身份凭证的合法性，查询结果可通过接入连接器缓存。					
请求参数						
序号	参数名称	数据类型	长度	约束	说明	
无请求参数						
响应参数						
序号	参数名称	数据类型	长度	约束	说明	
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）	
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）	
3	data	--	--	--	接口响应数据	
3.1	rootCertList	String[1..n]	2	必选	可信身份提供商根凭证列表，以数组形式返回	

8.3.3 全域功能节点对接接口

8.3.3.1 接入连接器身份信息上报接口

接口名称	接入连接器身份信息上报接口				SyncConnectorInfo	
接口访问地址	/SyncConnectorInfo				HTTP Method	POST
功能	接入连接器在区域/行业功能节点完成身份注册后，区域/行业功能节点调用本接口将接入连接器身份信息上报至全域功能节点					
请求参数						
序号	参数名称	数据类型	长度	约束	说明	
1	baseInfo				身份基本信息	
1.1	identityCode	String	64	必选	唯一身份标识	
1.2	connectorName	String	50	必选	接入连接器名称	
1.3	connectorIpList	String[1..n]	50	可选	IP 地址列表，以数组方式提交	
1.4	connectorDomainList	String[1..n]	50	可选	域名列表，以数组方式提交	
1.5	connectorJoinType	String	2	必选	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
1.6	enterpriseName	String	100	可选	所属法人或其他组织名称
1.7	enterpriseCode			必选	所属法人或其他组织 统一社会信用代码
1.8	identityStatus	String	2	必选	状态
1.9	authTime	Date	--	必选	颁发日期
2	extendInfo	--			身份附加信息
2.1	supplierName	String	50	可选	供应商名称
2.2	supplierCode	String	50	可选	供应商 统一社会信用代码
2.3	connectorSN	String	50	可选	产品 SN 号
2.4	connectorVersion	String	50	可选	产品版本号
2.5	connectorType	String	2	必选	连接器类型 1-标准型接入连接器 2-全功能型接入连接器
2.6	connectorMac	String	48	必选	物理设备唯一标识符（若有多台，只登记管理 服务器 mac 地址）
响应参数					
序号	参数名称	数据类型	长度	约束	说明
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）

8.3.3.2 经办人失效身份信息上报接口

接口名称	经办人失效身份信息上报接口				SyncLogoffInfo	
接口访问地址	/SyncLogoffInfo				HTTP Method	POST
功能	法人或其他组织经办人因业务变更或离职后，在区域/行业功能节点完成注销，区域/行业功能节点调用本接口，将失效信息上报至全域功能节点					
请求参数						
序号	参数名称	数据类型	长度	约束	说明	
1	identityCode	String	64	必选	经办人唯一身份标识	
响应参数						
序号	参数名称	数据类型	长度	约束	说明	
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）	
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）	

8.3.3.3 经办人失效身份信息查询接口

接口名称	经办人失效身份信息查询接口	GetOperatorStatus
------	---------------	-------------------

接口访问地址	/GetOperatorStatus			HTTP Method	POST
功能	当法人或其他组织经办人在业务节点开展数据流通业务活动时，在关键业务环节（如签订合同、订单支付时），区域/行业功能节点请求为保证用户身份的有效性，调用本接口查询经办人身份状态信息				
请求参数					
序号	参数名称	数据类型	长度	约束	说明
1	identityCode	String	64	必选	经办人唯一身份标识
响应参数					
序号	参数名称	数据类型	长度	约束	说明
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）
3	data	--	--	--	接口响应数据
3.1	authStatus	String	2	必选	身份状态

8.3.3.4 可信身份提供商根凭证列表查询接口

接口名称	可信身份提供商根凭证列表查询接口				GetIdentityProviderList	
接口访问地址	/GetIdentityProviderList				HTTP Method	POST
功能	区域/行业功能节点可调用此接口，查询对全域功能节点已注册的可信身份提供商信息，用于验证可信身份凭证的合法性，查询结果可通过区域/行业功能节点缓存。					
请求参数						
序号	参数名称	数据类型	长度	约束	说明	
无请求参数						
响应参数						
序号	参数名称	数据类型	长度	约束	说明	
1	code	String	10	必选	执行结果代码（详见附录 C 返回码定义）	
2	message	String	32	必选	执行结果信息（与结果代码对应，是执行结果的说明信息）	
3	data	--	--	--	接口响应数据	
3.1	rootCertList	String[1..n]	2	必选	可信身份提供商根凭证列表，以数组形式返回	

8.3.4 可信身份权威机构对接接口

区域/行业功能节点可按照可信身份权威机构对接规范要求完成认证，在本文件不做约束。

9 管理与安全要求

9.1 基本要求

- 运行维护组织与责任制度：全域功能节点、区域/行业功能节点、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。
- 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。

- c) 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。
- d) 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。
- e) 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。

9.2 安全措施

9.2.1 账户安全措施

- a) 强密码策略：应要求用户使用复杂的密码，应包括字母、数字和特殊字符，长度不少于 8 位，并要求定期更换。支持密码强度检测及到期提醒机制。
- b) 登录失败限制：限制登录失败次数，当登录失败次数达到一定限制时，自动锁定账户并触发安全通知，管理员可解锁或用户自助验证身份后恢复。
- c) 多因素认证机制：对高权限用户或关键操作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。

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) 数据加密存储：基于国家商用密码算法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) 数据访问控制：对数据进行访问控制，防止未经授权的用户访问或泄露数据。

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。

9.3 记录与审计措施

- a) 身份全生命周期记录：全域功能节点、业务节点、区域/行业功能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、操作人、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，对身份异常使用、越权访问、操作频率异常等行为进行识别与报警。

- 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）
可信身份凭证结构

接入连接器的可信身份凭证应由可信的可信身份提供商签发，各类平台的可信身份凭证由全域功能节点统一签发。

可信身份凭证结构见表A. 1。

表A. 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A.2。

表A. 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：域名或 IP OU 项：连接器或平台唯一标识
subjectPublicKeyInfo	主体公钥信息	
extensions	扩展项	可选，可自定义

附录 B（资料性） 报文样例

B.1 样例场景

法人或其他组织经办人因业务变更或离职后，在区域/行业功能节点完成注销，区域/行业功能节点调用本接口，将失效信息上报至全域功能节点。

B.2 报文样例

B.2.1 Http请求头样例

```
POST:http://ip:port/identity/operator/v1/
Host: 127.0.0.1:8080
Accept-Encoding: gzip
Content-Type: text/xml
msgcode: SyncLogoffInfo
msgversion: 1.0.0
timestamp: 1562589083316
sequenceNum: 990400000000003721209241622330001001
signValue
:
Sf1KxwRJSMekKF2QT4fwpMeJf36P0k6yJVXVCJ9.eyJzdWIjOiMTIzNDU2NzgOTAiLCJuYW11Ijoibm9obiBEb2UiLCJpYXQiOiE1MTYmM5MDIMn0.Sf1KxwRJSMekKF2QT4fwpMeJf36P0k6y
Content-Length: 1274
```

B.2.2 Http请求报文样例

```
{
  "identityCode ":"91310105575958172F/110105197812312345"
}
```

B.2.3 Http响应头样例

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding: gzip
Vary: Accept-Encoding
Date: Tue, 11 Sep 2024 00:44:01 GMT
timestamp: 1562589083316
sequenceNum: 990400000000003721209241622330001001
signValue
:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIjOiMTIzNDU2NzgOTAiLCJuYW11Ijoibm9obiBEb2UiLCJpYXQiOiE1MTYmM5MDIMn0.Sf1KxwRJSMekKF2QT4fwpMeJf36P0k6yJV_adQssw5c
Content-Length: 1524
```

B.2.4 Http响应报文样例

该示例接口请求的响应报文，如下所示：

```
{  
  "code": "003000",  
  "message": "注销成功"  
}
```

附录 C（规范性）
返回码定义

C.1 返回码格式定义

所有应答消息均使用统一定义的返回码，返回码一共6位，假设返回码格式为“ABCDEF”。其中，“A”表示返回码类型，各代码代表的模块类型如下：

- a) 0：成功
- b) 1：系统错误
- c) 2：参数错误
- d) 3：业务错误

“BC”表示业务模块类型，各代码代表的模块类型如下，具体实现时，可根据实际情况进行扩展：

- a) 00：通用功能模块
- b) 01：个人
- c) 02：法人或其他组织
- d) 03：法人或其他组织经办人
- e) 04：平台
- f) 05：接入连接器

“DEF”表示具体的返回值，具体实现时，可根据实际情况进行扩展。

C.2 返回码类型

按照以上格式说明，返回码的具体类型如下表所示（注：下述所有表格中返回码里的XX为业务模块类型）：

表A.3 成功类型表

返回码	内容
0XX000	请求成功

表A.4 系统错误类型表

返回码	内容
1XX000	未知错误
1XX001	系统忙
1XX002	操作超时
1XX003	网络异常
1XX004	未授权请求
1XX005	临时访问令牌已失效
1XX006	授权密钥无效
1XX007	非法的连接源 IP 地址

表A. 5 参数错误类型表

返回码	内容
2XX000	未知错误
2XX001	必选参数为空
2XX002	参数格式错误
2XX003	参数长度超出范围
2XX004	所有输入参数都为空
2XX005	版本号非法
2XX006	时间戳非法
2XX007	消息名称错误
2XX008	消息解析失败

表A. 6 业务错误类型表

返回码	内容
3XX000	未知错误
301001	个人用户身份信息不存在
301002	个人用户身份信息已失效
301003	个人用户身份信息重复注册
302001	法人或其他组织用户身份信息不存在
302002	法人或其他组织用户身份信息已失效
302003	法人或其他组织用户身份信息重复注册
303001	法人或其他组织经办人用户身份信息不存在
303002	法人或其他组织经办人用户身份信息已失效
303003	法人或其他组织经办人用户身份信息重复注册
304001	平台身份信息不存在
304002	平台身份信息已失效
304003	平台身份信息重复注册
305001	接入连接器身份信息不存在
305002	接入连接器身份信息已失效
305003	接入连接器身份信息重复上报

附录 D
(规范性)
Token 结构

Token结构包含头部（Header）、载荷（Payload）和签名（Signature）三部分，描述

表C.1 Token 结构

结构	项名称	描述
头部（Header）	Token 类型（typ）	标识 Token 的类型, 如 JWT、authToken
	算法（alg）	SM2
载荷（Payload）	签发方（iss）	签发方
	持有者（sub）	TOKEN 持有者
	授权节点（auth）	被授权可与之交互的节点
	签发时间（iat）	签发时间。时间戳 1970-1-1 到签发时的秒数
	过期时间（exp）	过期时间。时间戳 1970-1-1 到过期时间的秒数
	唯一标识（jti）	TOKEN 的唯一标识
签名（Signature）		用算法（如 SM2）对编码后的 Header 和 Payload 生成签名，用于校验 Token 完整性

```
代码示例如下：
Token =
base64UrlEncode(Header) + . + base64UrlEncode(Payload) + . + base64UrlEncode(Signature)
Header: {
  typ:authToken
  alg:SM2
}

Payload: {
  iss: XXX,  // 签发方
  sub: YYY,  // TOKEN持有者
  auth: ZZZ,  // 被授权可与之交互的节点
  exp: 1311282970,  // 过期时间。时间戳1970-1-1到过期时间的秒数
  iat: 1311280970,  // 签发时间。时间戳1970-1-1到签发时的秒数
  jti: 1234567890123456  // TOKEN的唯一标识
}

Signature = SM2(
base64UrlEncode(header) + . +
base64UrlEncode(payload))
```

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》
-