ICS 35.240.01
CCS L 70

SCIE

智慧城市产业生态圈联盟标准

SCIE 6.1—2021

统一身份管理与访问控制平台 第1部分：总体要求

Unified identity management and access control platform—Part 1: General requirements

2021－10－17 发布　　2021－10－17 实施

智慧城市产业生态圈　　发 布

目　　次

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。

本文件由智慧城市产业生态圈提出并归口。

本文件主要起草单位：深圳竹云科技有限公司、西安电子科技大学、华为技术有限公司、深圳市标准技术研究院、山东省计算中心（国家超级计算济南中心）

本文件主要起草人：赵静谧、史晓婧、徐曲莎、张涛、张志为、黄敏、胡露、侯义荣、杨叶、史丛丛

统一身份管理与访问控制平台　第1部分：总体要求

1　范围

本文件规定了统一身份管理与访问控制平台的总体框架、功能建设、平台规范建设要求、平台运维管理要求、平台安全管理要求。

本文件适用于统一身份管理与访问控制平台项目的规划与建设参考。

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 22239-2019　信息安全技术 信息系统安全等级保护基本要求

GB/T 28827.1　信息技术服务 运行维护 第1部分：通用要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

统一身份管理与访问控制平台　Unified identity management and access control platform

是管理自然人及应用系统的平台，通过对人员所属的组织、角色、岗位、身份、账号、权限、身份认证等进行统一的管理，将不同维度的人员纳入统一的安全管控体系，合理控制自然人访问应用系统资源的权限，并对异常访问行为进行有效防范。

3.2

弱口令　weak password

容易被他人猜测到或被破解工具破解的口令为弱口令。

4　缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

B/S：浏览器/服务器模式(Browser/Server)

C/S：客户端/服务器模式(Client/Server)

OAuth：开放授权(Open Authorization)

Radius：远程用户拨号认证服务 (Remote Authentication Dial In User Service)

RESTFUL：一种网络应用程序的设计风格和开发方式（Representational State Transfer）

SSO：单点登录（Single Sign On）

SAML：安全断言标记语言（Security Assertion Markup Language)

SQL：结构化查询语言（Structured Query Language）

XML：可扩展置标语言（Extensible Markup Language）

5　总体框架

统一身份管理与访问控制平台包括统一身份、统一权限、统一访问、审计分析四大功能模块。统一身份管理与访问控制平台总体架构见图1。

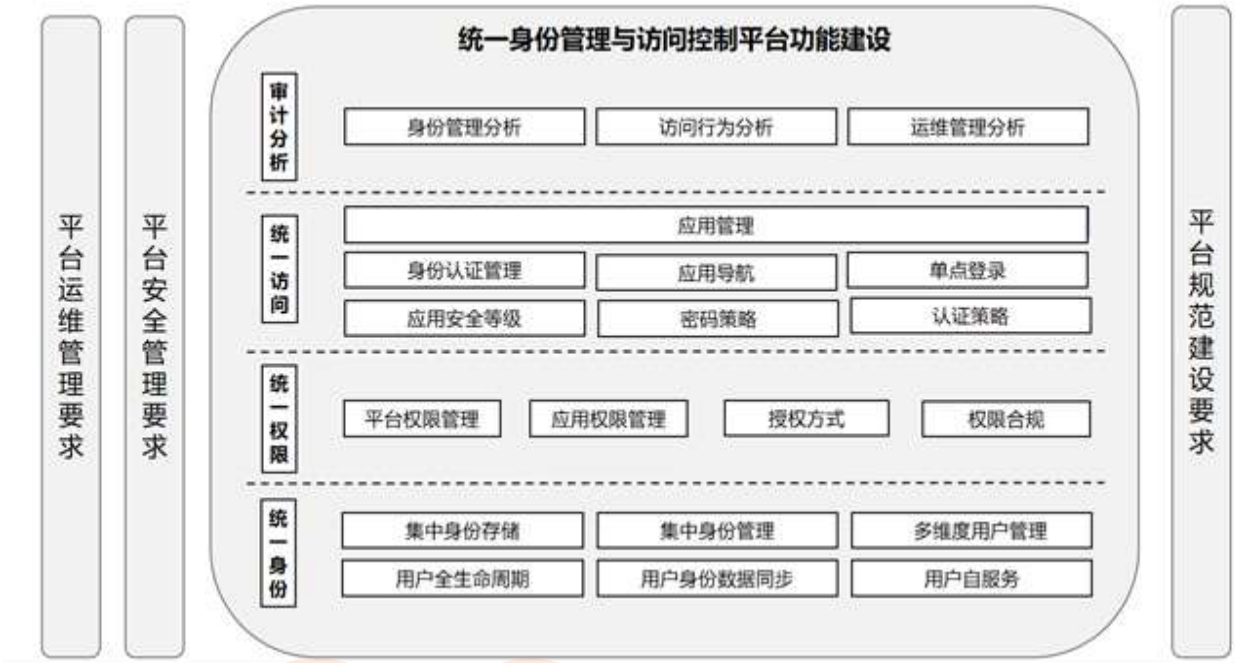

图1　统一身份管理与访问控制平台总体架构

统一身份管理与访问控制平台各部分描述如下：

a) 统一身份：对各维度人员的组织机构、用户、账号、角色、岗位等进行全生命周期管理。
b) 统一权限：基于角色访问控制原则，提供平台级、应用级、核心级管理。
c) 统一访问：统一门户、一个账号、一次登录，访问所有可信并且有权限的应用系统并针对高安全级别应用提供多因素身份认证。
d) 审计分析：对用户的账号（违建、僵尸、孤儿等）、用户权限、登录行为、访问行为以及操作行为等进行可视化审计。
e) 平台规范建设要求:包含用户管理规范及应用对接规范,用户管理规范可规范化用户身份管理、授权管理、口令管理等管理工作；应用对接规范可提供应用进行用户数据同步及统一访问管理对接标准流程。
f) 平台运维管理要求：规定运行维护服务组织在人员、资源、技术和过程方面应具备的条件和能力，统一身份管理与访问控制平台应满足 GB/T 22239 中的相关要求。
g) 平台安全管理要求：规定统一身份管理与访问控制平台自身应满足安全保护。

6　功能建设

6.1　统一身份

6.1.1　集中身份中心

集中身份存储由集中身份存储、身份数据汇集、身份数据供给三部分功能组成，各部分功能应符合以下要求：

a) 集中身份存储：满足用户身份信息与账号信息的集中存储；
b) 身份数据汇集：支持各类用户库，汇集用户身份与账号信息，形成身份数据中心；
c) 身份数据供给：为信息系统集中供给统一的身份信息。

6.1.2　集中身份管理

集中身份管理由统一身份管理、身份管理可视化、多维身份管理三部分功能组成，各部分功能应符合以下要求：

a) 统一身份管理：满足不同维度的身份管理体系统一管理，并建立相对应身份管理规范；
b) 身份管理可视化：提供可视化、人性化的身份管理图形界面；
c) 多维身份管理：提供用户管理、机构管理、应用管理、账号管理、权限管理、审计管理等功能。

6.1.3 多维度用户管理

多维度用户管理由内外部用户管理机制、各类账号管理两部分功能组成，各部分功能应符合以下要求：

a) 内外部用户管理机制：建立敏捷的身份生命周期管理机制，满足对内部、外部等不同身份的管理；
b) 各类账号管理：针对不同的用户体系提供完整账号有效期管理机制。

6.1.4 用户全生命周期

用户全生命周期由用户唯一标识、用户全生命周期管理两部分功能组成，各部分功能应符合以下要求：

a) 用户唯一标识：确保用户身份整个全生命周期内用户标识的唯一性；
b) 用户全生命周期管理：实现用户身份全生命周期闭环管理（涵盖用户入职、离职、转岗、调岗等不同的业务场景），统一身份数据贯穿整个应用域，确保身份体系协同一致。

6.1.5 用户身份数据同步

用户身份数据同步由上下游数据同步、多源身份聚合两部分功能组成，各部分功能应符合以下要求：

a) 上下游数据同步：包含平台的用户、机构、账号、权限等身份数据与各应用系统的数据同步；包括从上游应用系统回收数据和从平台往下游应用系统的供应数据；
b) 多源身份聚合：支持从一个身份数据源回收身份数据（含用户、机构数据），也支持将分散在多个应用系统中的身份数据回收并聚合为权威身份数据。

6.1.6 用户自服务

用户自服务由个人信息维护、口令信息维护、权限信息维护、待办任务、安全中心五部分功能组成，各部分功能应符合以下要求：

a) 个人信息维护：可查看或修改（授权允许其修改的）个人属性；
b) 口令信息维护：提供忘记口令（忘记口令时通过邮件、短信、密保问题等自助重置或找回口令）、自助修改口令功能；
c) 权限信息维护：提供应用权限查看、账号权限委托、应用权限申请等功能；
d) 待办任务：查看和审批平台工作流待办任务（包括申请账号、自注册等）；
e) 安全中心：检查用户账号安全性（包括口令安全等级、口令到期时间）、密保工具设置等。

6.2 统一权限

6.2.1 平台权限管理

平台权限管理由菜单角色管理、菜单权限管理、不同维度授权管理三部分功能组成，各部分功能应符合以下要求：

a) 菜单角色管理：支持自定义平台管理角色，包括身份管理员、系统管理员、审计管理员等角色；

b） 菜单权限管理：管理不同管理角色查看、访问不同的平台菜单及数据范围，并允许将相关的管理权限再分配；
c） 不同维度授权管理：可按用户维度、组维度、机构维度、应用维度等进行权限的授予。

6.2.2 应用权限管理

应用权限管理由应用账号级权限、角色级权限两部分功能组成，各部分功能应符合以下要求：
a） 应用账号级权限：平台集中为用户分配应用账号，可以实现应用账号的集中统一管理；
b） 角色级权限：平台集中为用户分配应用角色级权限，包括机构、角色、群组、岗位等与用户关联的权限；

6.2.3 授权方式

授权方式由管理员手工授权、用户属性授权、角色/组授权、工作流授权四部分功能组成，各部分功能应符合以下要求：
a） 管理员手工授权：管理员手工为用户分配或移除权限，支持从用户、应用两个维度授权；
b） 用户属性授权：基于用户属性的自动授权，设置规则为满足条件的用户自动授予权限；
示例：财务部用户自动授予财务系统权限、正式员工自动开通邮箱权限等。
c） 角色/组授权：基于角色/组的自动授权，当用户加入角色/组时自动授予权限，当用户从角色/组中移除时自动回收用户权限；
d） 工作流授权：基于工作流的自动授权，用户自助申请权限，在领导或应用管理员审批通过后自动为用户开通权限。

6.2.4 权限合规

权限合规由合规规则、互斥规则、规则扫描、用户/应用合规情况查看四部分功能组成，各部分功能应符合以下要求：
a） 合规规则：配置基于岗位的应用系统权限规则；
示例：开发经理岗位能授予项目管理系统的权限；
b） 互斥规则：配置权限互斥规则，支持应用互斥、应用内角色互斥、应用间角色互斥；
示例：应用互斥，可定义同一个人不能同时授予财务系统及项目管理系统权限；
应用内角色互斥，可定义财务系统中，同一个人不能同时授予会计和出纳两类角色；
应用间角色互斥，可定义项目管理系统-项目经理角色及财务系统-会计角色不能同时授予同一个人。
c） 规则扫描：平台根据已配置的合规规则、互斥规则扫描检查所有授权数据；
d） 用户/应用合规情况查看：查看违反合规规则的用户授权/应用授权情况。

6.3 统一访问

6.3.1 应用管理

应用管理由应用信息管理、应用注册、应用模板管理三部分功能组成，各部分功能应符合以下要求：
a） 应用信息管理：包含应用列表、应用查看、应用修改、应用删除、应用查询等；
b） 应用注册：支持按照模板或自定义方式注册应用，并配置应用的基本信息、集成配置、连接器配置、对象建模、映射定义、过程定义、事件定义、回收及其他设置；
c） 应用模板管理：支持常用应用注册配置标准化。

6.3.2 身份认证管理

身份认证管理由统一身份认证服务、外部身份认证源、多因素身份认证支持、互信身份认证四部分功能组成，各部分功能应符合以下要求：

a） 统一身份认证服务：统一身份管理与访问控制平台可作为身份认证源对外提供统一身份认证服务或统一身份认证集成接口，支持 Restful、SAML、OAuth、Radius 等身份认证集成接口；
b） 外部身份认证源：支持服务器身份认证源、办公类身份认证源、社交类身份认证源及第三方身份认证源；
c） 多因素身份认证支持：可提供包括账号口令、数字证书、手势、指纹、人脸、声纹等具有相应安全强度的两种或两种以上的身份认证方式组合机制进行用户身份鉴别（人脸、声纹、指静脉等 AI 身份认证以及数字证书、邮箱、短信等身份认证均需要第三方提供算法或者服务）；
d） 互信身份认证：若企业已有身份认证平台，统一身份管理与访问控制平台可与已有身份认证平台（包括企业自建身份认证平台及商用身份认证平台等）作身份认证互信，包括单方互信和双方互信，互信可能涉及双方的定制开发。

6.3.3 应用导航

应用导航由统一应用入口、多语言支持、界面自定义三部分功能组成，各部分功能应符合以下要求：
a） 统一应用入口：应用集中的访问入口，支持收藏应用、所有应用、最近访问、应用分类等显示方式；
b） 多语言支持：支持中文和英语两种语言；
c） 界面自定义：支持入口及应用列表界面配置图标、背景图片、系统名称等内容。

6.3.4 单点登录

单点登录由一站式访问、跨模式应用集成两部分功能组成，各部分功能应符合以下要求：
a） 一站式访问：用户通过一次身份认证，展示有权限访问的应用系统列表；
b） 跨模式应用集成：支持 B/S、C/S 应用的单点登录。

6.3.5 应用安全等级

应用安全等级由应用安全等级管理、身份认证级别管理两部分功能组成，各部分功能应符合以下要求：
a） 应用安全等级管理：对应用系统进行风险安全级别的划分，可根据不同安全级别配置不同的身份鉴别方式；
b） 身份认证级别管理：若访问应用时判断当前身份认证安全级别低于应用安全等级时，强制要求用户作二次身份认证。

6.3.6 口令策略

口令策略由初始口令策略、口令校验策略、弱口令管理、过期策略四部分功能组成，各部分功能应符合以下要求：
a） 初始口令策略：支持用户创建或重置口令时的初始口令策略；支持固定口令、随机数字、随机字母+数字、定义随机规则；
b） 口令校验策略：支持口令复杂度管理和口令检查策略；

注：口令校验策略包含：最小长度、最大长度、最少字母数、最少数字数、最少特殊字符数、最少大写字母数、最少小写字母数、最多重复数、必须以字母开头，允许使用的字母、数字、特殊字符，是否开启历史口令检查，是否允许用户名作为口令，是否开启弱口令检查等。

c） 弱口令管理：支持自定义弱口令数据；支持弱口令数据的导入导出；
d） 过期策略：支持口令到期提醒、到期强制修改口令等。

6.3.7 身份认证策略

身份认证策略由失败次数锁定、口令到期提醒、强制修改口令、认证顺序管理四部分功能组成，各部分功能应符合以下要求：

a) 失败次数锁定：用户登录失败次数达到预先设置数值可自动锁定，可设置失败次数、锁定时长、自动解锁等；
b) 口令到期提醒：可设置提前提醒用户修改口令天数；
c) 强制修改口令：可设置到期后强制用户修改口令；
d) 认证顺序管理：可设置应用系统认证顺序。

示例： 可配置财务系统首次使用用户名+口令认证，二次认证使用手势，三次认证使用人脸或者声纹。

6.4 审计分析

6.4.1 身份管理分析

身份管理分析由重复账号统计分析、僵尸账号统计分析、孤儿账号统计分析三部分功能组成，各部分功能应符合以下要求：

a) 重复账号统计分析：检测并处理重复账号；

注： 重复账号是指一个人在一个应用中有多个账号；消除无效重复账号，有效重复账号需和自然人进行绑定。

b) 僵尸账号统计分析：检测并消除僵尸账号；

注： 僵尸账号是指长期无人使用的应用账号；长期无人使用账号，可定义时间期限为半年或者一年。

c) 孤儿账号统计分析：检测并消除孤儿账号；

注： 孤儿账号是指对应不到自然人的应用账号。

d) 公共账号统计分析：指定使用者和责任人并进行身份认证审计。

注： 公共账号是指多人使用同一个应用账号登录应用系统。

6.4.2 访问行为分析

访问行为分析由身份认证统计、账号使用情况统计两部分功能组成，各部分功能应符合以下要求：

a) 身份认证统计：统计统一用户登录/登出应用系统身份认证数量及统计时间段内应用系统访问量；
b) 账号使用情况统计：时间段内活跃用户/非活跃用户统计排行。

6.4.3 日志管理分析

日志管理分析由操作日志、同步日志、身份认证日志、接口日志四部分功能组成，各部分功能应符合以下要求：

a) 操作日志：平台管理员进行用户管理时，提供操作记录、操作内容监控；
b) 同步日志：平台与应用集成时，提供身份数据同步监控；
c) 身份认证日志：用户访问各应用系统资源时，对用户身份认证情况进行监控；
d) 接口日志：外部应用调用统一身份管理与访问控制平台接口时，对平台各接口使用情况进行监控。

7 平台规范建设要求

统一身份管理与访问控制平台规范建设要求应包括用户管理要求和应用对接要求。

8 平台运维管理要求

统一身份管理与访问控制平台的运维管理应满足GB/T 28827.1的要求。

9 平台安全管理要求

统一身份管理与访问控制平台的安全管理平台应满足GB/T 22239-2019中的相关要求。