AuthCahn

全域信任根 · 统一身份与细粒度授权

数澄科技

产品一页纸 · v1.0 · 2026-11

认证归身份源，授权归权限中心。

让每一次访问都有依据、可审批、可回收、可审计 —— 面向 4A 的账号、认证、授权、审计与统一单点登录。auth（身份目录 + 统一认证）承载身份与认证，cahn（授权决策引擎 + 治理面）承载授权与治理，独立部署；身份源、授权引擎与存储均可替换，接口以标准协议与稳定契约为界。

认证与授权解耦 · 统一身份底座 · 独立部署 / 独立升级 · 两个管理面

一条可审计的授权链 Architecture

身份源（OIDC / SAML / Kerberos） → 业务系统（JWT） → 授权判定 / 列表查询 → 授权决策引擎

管理面 → 同步服务（校验 / 幂等 / 重试 / 审计） → 授权决策引擎 | 申请审批 → 同步服务写入

查询与写入分离：业务系统只做两件事 —— 用 OIDC 登录拿 JWT，用 `/authorize/check` 或 `/list-objects` 问权限；权限写入必须经同步服务，**严禁直连授权引擎写入**。

六项核心能力 Capabilities

01 / 身份

统一身份与强认证

目录用户/组/部门 + 外部身份源联邦；OIDC / SAML / Kerberos；口令、OTP、WebAuthn、X.509。

02 / 授权

ReBAC 细粒度授权

26 类对象覆盖身份/资源/权限/管控；组织继承 + 角色 + 项目；条件支持有效期、同租户、IP 段。

03 / 写入

统一元组写入通道

同步服务统一校验、幂等、重试、审计、批量与删除；敏感关系需审批。

04 / 审批

申请、审批与回收

申请 → 审批 → 通过后写入元组；支持到期回收、定期复核与超期预警。

05 / 治理

治理与审计闭环

生命周期、组织同步、认证事件汇聚、按角色/部门报表、从账号、HR/AD 连接器。

06 / 接入

接入与运行

Node SDK（验签 / 授权判定 / 列表查询）；Token、OIDC、mTLS；离线部署、VIP 与数据库主从。

主体分层、适用场景与交付 Model & Delivery

主体	承载与标识
员工	企业内部身份源，`user:<uid>`
外部用户	外部身份源联邦；临时账号带有效期
机器 / 服务	服务账号 / 目录服务主体，`service:<clientId>`

适用：所有规模与行业的企业。典型场景包括 4A 平台建设、多业务系统统一身份与权限治理、外包与临时人员管理、机器/服务身份纳管，以及需要申请审批与审计证据链的组织。

交付：auth 与 cahn 两产品独立打包、独立安装与升级，支持离线交付；提供安装部署、初始化与验收工具，并支持生产级高可用与容灾部署。

边界：auth 负责登录与认证，cahn 只做授权与治理；资源注册与业务门户归资源方。权限项/权限集、多租户隔离、外部审计库/SIEM、国密 SM2、Java SDK/代填仍在推进；Hypernet / EiPlatform 实质接入待完成。

© 2026 北京数澄科技有限公司 版权所有

保留所有权利。未经本公司书面许可，不得复制、转载或用于商业用途。