EiPlatform

企业能力编排中心 · 统一注册与受控发布

数澄科技

产品一页纸 · v1.0 · 2026-11

让企业能力，成为 AI 的可信能力。

统一注册 · 受控发布 · 全链路审计 —— App 注册 → Skill 定义 → Workflow 编排 → Prompt 入口 → Namespace 声明 → Export 物化 → Agent 消费。

Agent 不缺工具，缺的是可信的能力供给 Why EiPlatform

- **重复对接**：每个 Agent 都要重新理解企业系统与认证。
- **凭证散落**：长期密钥被放进配置与个人机器。
- **权限模糊**：改能力的人与消费能力的人没有边界。
- **发布失控**：共享靠复制文件，改版不知谁用旧版。
- **审计缺失**：查不到谁在什么时候做了什么。

平台的核心不是“再建一个应用”，而是建立一条企业能力供应链。

企业系统只注册一次，所有 Agent 共享同一份能力定义；维护权限与消费权限分离；内容版本、声明版本、物化版本逐级引用，发布失败可重试、可回滚、可识别漂移。

三层治理模型 Skill · Namespace · Export

层	回答的问题	价值
Skill	能力是什么？谁维护？哪个版本？	唯一内容真相源；`xxx.skill.md` 标准格式，服务端强校验
Namespace	发布给谁？在哪个逻辑路径可见？	逻辑发布声明；`public / org / project / user` 四级
Export	实际交付了什么？Agent 从哪里读？	物理交付结果；对应真实 NFS 导出、ACL 与消费路径

六项核心能力 Capabilities

01 / 注册
App 注册
纳管系统元数据、API 文档、调用基址与认证描述符。

02 / 定义
Skill 定义
结构化表单与全文粘贴双入口；标准 Markdown，服务端强校验。

03 / 编排
Workflow 与 Prompt
Skill 的 DAG 组合，可版本化、可授权；Prompt 形成场景入口。

04 / 交付
双通道消费
NFS + Kerberos 服务域内 Agent；REST API + MCP 服务 HTTP Agent。

05 / 治理
权限与凭证
维护与消费权限独立；密钥不落平台，由消费端按需获取。

06 / 可信
审计与标准交付
发布、回滚、权限变更、AI 草稿全部留痕；installer / upgrader 支持回滚。

适用场景与落地路径 Fit & Roadmap

- **所有规模与行业**：按业务优先级选择首批系统与 Skill。
- **研发效能**：质量门禁、代码评审、流水线触发。
- **IT 运维**：监控、工单、发布与回滚 Runbook。
- **业务部门**：报销、采购、合同、CRM 查询。
- **数据 BI**：指标口径、取数、报表生成。
- **安全合规**：权限收敛、凭证治理、操作审计。

阶段	目标
第 1 月	安装接入；注册 3–5 个系统、5–10 个 Skill
第 2 月	单部门试点；建立提交-审批-发布；发布/回滚演练
第 3 月	扩展 3–5 个部门；固化 SLO；安全评审与推广

© 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。