



APUSIC
固若长城
睿比世界

产品白皮书

金蝶Apusic统一身份管理

版权所有 © 深圳市金蝶天燕云计算股份有限公司2026。保留所有权利。

版权声明

本文档所涉及的软件著作权、版权等知识产权已依法进行了注册，由金蝶天燕云计算股份有限公司合法拥有。受《中华人民共和国著作权法》《计算机软件保护条例》《知识产权保护条例》和相关国际版权条约、法律、法规以及其它知识产权法律和条约的保护。未经授权许可，不得非法使用。

免责声明

本文档包含的版权信息由金蝶天燕云计算股份有限公司合法拥有，受法律的保护，金蝶天燕云计算股份有限公司对本文档可能涉及到的非金蝶天燕云计算股份有限公司的信息不承担任何责任。在法律允许的范围内，您可以查阅并仅能够在《中华人民共和国著作权法》规定的合法范围内复制和打印本文档。任何单位和个人未经金蝶天燕云计算股份有限公司书面授权许可，不得使用、修改、再发布本文档的任何部分和内容，否则将被视为侵权，金蝶天燕云计算股份有限公司有依法追究其责任的权利。

本文档如有更新，不另行通知。对本文档中的问题您可向金蝶天燕云计算股份有限公司告知或查询。未经本公司明确授予的任何权利均予保留。

商标声明

 是深圳市金蝶天燕云计算股份有限公司向中华人民共和国国家商标局申请注册的注册商标，注册商标专用权由金蝶天燕合法拥有，受法律保护。未经金蝶天燕的书面许可，任何单位及个人不得以任何方式或理由对该商标的任何部分进行使用、复制、修改、传播、抄录或与其它产品捆绑使用销售。凡侵犯金蝶天燕商标权的，金蝶天燕将依法追究其法律责任。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

目录

1 背景

2 产品介绍

• 2.1 产品定位

• 2.2 产品受众

3 核心能力

4 产品能力

• 4.1 单点登录

• 4.1.1 标准协议

• 4.1.2 应用管理

• 4.1.3 访问授权

• 4.2 人员账户

• 4.2.1 组织管理

• 4.2.2 用户管理

• 4.2.3 分组管理

• 4.3 应用授权

• 4.3.1 资源管理

• 4.3.2 角色管理

• 4.3.3 授权管理

• 4.4 企业门户

• 4.4.1 用户门户

• 4.4.2 管理员门户

• 4.5 用户中心

• 4.5.1 个人资料

• 4.5.2 账号安全

• 4.5.3 操作记录

5 部署方案

1 背景

产业互联网进行到下半场，企业在数字化转型的大背景下，通过互联网信息技术构建了自己的业务系统。如有面向企业内部沟通的IM系统，有面向企业效率管理的ERP系统，有管理供应链的CRM系统，等等。随着后续国家对数字城市、数字企业的大力支持，可以预见未来的企业数字资产一定是企业的核心竞争力之一。那么作为互联网企业方案提供商，如何保证数字资产的安全性、扩展性、追溯性、灵活性，是互联网下半场的议题。

从现实情况来看，企业面临降本增效的目标。数字化不仅仅是将原有的线下业务搬到线上来，数字化是帮助企业突破自身的生产瓶颈，让企业通过统一标准，统一流程去规范化自己的生产行为，从而实现增效的目标。但是数字化的最大问题就是这些系统的运维成本的增加，如何统一的管理这些系统是企业现在面临的难题。当前企业主要面临以下几个问题：

1. 安全风险：多个系统，多套数据，登录密钥容易丢失
2. 管理风险：维护成本较高，人员离职后存在僵尸账号
3. 体验风险：多系统，多账号，多密码，用户使用繁琐

2 产品介绍

2.1 产品定位

金蝶天燕APUSIC 统一身份管理认证系统（简称AIDM）是一款企业身份管理产品，通过给企业提供应用认证、资源权限、用户管理、权限分配、审计日志等一系列的功能，构建统一的身份认证平台，帮助企业打通不同系统间的信息孤岛，同时AIDM也可以打通上下游数据同步，把AIDM做为一个用户数据中心。实现在用户侧、企业侧、运维侧的数据治理。

2.2 产品受众

- 管理员

管理员对系统内的各种基础信息、系统资源做配置化管理，包括单点登录用户、角色、权限及基础安全配置。同时对系统的访问日志和操作日志具备审计功能。

- 企业用户

企业用户主要是可以使用对应用单点登录的操作和对自己的个人信息修改、操作日志的记录、子账号的绑定。

- 运营人员

企业用户需要申请账号、申请单点登录应用并由运营人员进行成员入职和授权。只有授权、入职企业用户才能进行使用，运营人员同事需要维护组织机构的架构根据企业的组织机构实际情况变动。

3 核心能力

针对企业的上述痛点，AIDM统一身份认证管理系统通过提供应用认证、资源权限、用户管理、权限分配、审计日志等一系列的功能，搭建标准的身份管理平台，帮助企业打通不同系统间的信息孤岛，构建统一的身份管理体系。其中：

应用认证：通过提供单点登录（SSO）或第三方认证的功能，优化用户的登录体验，解决一人多户的困扰。

资源管理：统一整理接入系统的资源，通过统一的授权出口，对登录系统进行不同颗粒度的资源管理，包括登录入口等粗颗粒度的管理和页面按钮等细颗粒度的管理。

用户管理：通过对所有系统的使用人员回收，由AIDM统一为用户分配使用权限，解决不同系统间管理混乱、人员变动后需要在多个系统间进行权限回收的问题。

权限分配：通过对回收的系统资源进行统一分配，解决运维人员管理多人多账号成本过高的问题。

审计管理：通过记录用户和管理员的使用操作，监控用户的高危行为，从而实现对用户行为的审计，做到权责分明，安全可溯。

企业门户：支持打造企业门户中心，集应用访问、通知中心、自助申请、待办事项等多场景办公于一体

4 产品能力

4.1 单点登录

4.1.1 标准协议

AIDM系统支持多种认证协议的接入，能兼容主流认证协议，如OAuth认证、SAML认证、OIDC认证，以及表单代填的接入方式，来集成应用适合各种场景，同时AIDM的表单代填在基本协议的基础上做出了扩展，使用浏览器插件来使集成应用更加便捷，单点登录配置也不在繁琐。

4.1.2 应用管理

应用管理主要是管理根据标准协议创建的应用进行一个列表展示，可以根据切换样式变成表格展示全部的应用列表，可对应用进行停用，启用，编辑，删除，配置等操作。

4.1.3 访问授权

AIDM可以通过用户、分组、组织机构、角色4种纬度出发实现不同场景的授权模式，配合上授权授权黑名单功能能够更加灵活配置用户访问授权。达到企业内复杂的现实场景。

4.2 人员账户

4.2.1 组织管理

管理员登录AIDM系统后，在用户管理-组织管理页面下可以完成组织架构的新增、上下级组织的新增、移动、删除等。同时可以查看不同组织下的用户。主要实现对于企业组织架构的管理和对组织部门的人员入职、移动管理。

4.2.2 用户管理

管理员在人员账户列表可以对当前企业中的所有人员进行操作，通过用户名、姓名、手机号搜索可以快速定位用户。同时可以对用户状态进行筛选，用户状态包括启用、停用两种；过期状态包括正常和已过期两种状态。用户信息展示字段包括用户名、姓名、电话、最后登录时间、过期状态、启用状态、操作。主要实现是对用户的全生命周期进行管理

4.2.3 分组管理

分组管理列表主要是将用户可以不局限于组织机构的限制，把AIDM用户纳入一个分组的集合可以进行授权。分组管理主要包含分组名称、备注、组内成员（位）、创建时间、查看、修改、删除、新增操作。主要是实现将用户以一个新的

纬度来进行授权管理。

4.3 应用授权

4.3.1 资源管理

资源管理主要是对当前应用的菜单资源、按钮资源、API资源、数据资源进行管理的页面。资源管理主要包括资源列表、创建资源、资源列表、资源名称、上级菜单、类型、描述、创建时间、查看、编辑、删除操作。主要是实现对于当前应用下的资源进行增删改查管理

4.3.2 角色管理

角色管理是对应用下所有角色的预览。角色管理主要包括角色列表、角色名称、用户数量（位）、创建时间、状态、查看、编辑、删除、新增操作。支持角色授权给用户、授权给组织机构两种纬度，同时可以对当前角色下的资源进行一个管理。

4.3.3 授权管理

授权管理是用户对角色、用户两种对象授权资源的权限操作的功能。授权管理主要包括创建授权、授权列表、被授权主体、主体类型、查看详情、删除操作。主要是实现于可以通过用户和角色两种纬度来进行资源的授权，让不同用户拥有不同的应用权限。

4.4 企业门户

4.4.1 用户门户

用户可以在此查看到自己拥有的全部单点登录应用，可以进行单点登录操作。会展示一个常用应用的环形图、最近七天的最新动态、最近一个月的登录热点图。

4.4.2 管理员门户

管理员实时监控用户总数据和用户登录次数前5名、应用总数和应用登录次数前5名还可以通过预设快捷入口进行快速入门操作。管理员可以看到用户今日新增用户人数和前七天的数据环比、本周新增用户数和对比前七周的数据环比、本周登录用户数和对比前七周数据环比。还可以根据用户总数新增的趋势图来分析当前企业的一个趋势情况，同时可以监控最近实时登录的前5名。还会展示当前月份全部用户的登录热点图。

4.5 用户中心

4.5.1 个人资料

用户可以此查看、修改自己的个人信息。

4.5.2 账号安全

用户在此可以设置、修改账号密码，绑定手机号、修改手机号，绑定邮箱、修改邮箱操作。

4.5.3 操作记录

用户可以在此查看自定义日期内的操作记录。

5 部署方案

部署方式	硬件要求	说明
单节点部署	8 cpu+64G内存+512G硬盘 物理机集群上高可用部署	以上所有组件均已容器化单实例的方式运行；通过docker-compose+ 的方式打包集成容器镜像，方便的在docker环境中一键部署，在中小微企业项目中可以采用此方式
双机热备	2+ 服务器 8 cpu+64G内存+512G硬盘	数据库和缓存采用主从方式部署
集群部署	3+服务器 8 cpu+64G内存+512G硬盘	数据库和缓存采用cluster模式部署

全国统一服务热线
4008-555-800



金蝶天燕云计算股份有限公司(简称“金蝶天燕云”)成立于2000年,前身为“金蝶中间件公司”,是金蝶集团旗下新一代软件基础云平台服务商,云计算国家标准制定企业,国家信创产业核心软件企业。金蝶天燕是国家863重点研发计划与核高基重大专项承接企业,也是“两网一站四库十二金”国家重点工程的基础平台提供商,产品广泛应用于政府、军工、金融、能源等关键行业,累计服务客户总数超过10万家。

Apusic
金蝶天燕

云计算国家标准制定企业
金蝶集团旗下基础软件企业
信息技术应用创新核心企业
官网: www.apusic.com

