Apusic 金蝶天燕

生成时间：2026-05-19

技术白皮书

金蝶Apusic统一身份管理

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

Apusic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 AIDM技术白皮书

1.1 业务需求

1.1.1 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。

1.1.2 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。

1.1.3 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。

1.1.4 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。

1.1.5 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。

1.1.6 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

1.2 整体架构

1.2.1 产品逻辑结构

AIDM集成企业内各种业务系统的用户账户信息，面向普通用户提供统一身份认证门户，面向企业内管理员提供跨应用的用户账户管理统一视图。

用户可以通过多种方式登入AIDM，AIDM对用户进行身份认证后，通过各种身份认证协议登入对应业务系统。


AIDM产品逻辑结构

1.2.2 AIDM与其他系统集成路径

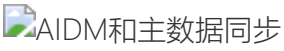
根据当前企业内是否存在主数据系统或其他对用户信息统一管控的系统，以及企业之前是否有类似LDAP这类对用户目录服务，将AIDM和企业内其他应用系统集成架构分为三种情况：

1.企业之前没有主数据系统或其他用户统一管控的系统，也没有LDAP系统。


AIDM为主

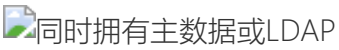
这种情况，有AIDM通过各种应用系统支持的标准身份认证协议与各个业务应用进行集成，或使用表单代填来完成单点登录。之后管理员统一在AIDM中管控不同人员的账户信息变动。

2.企业已经有主数据或用户统一管控系统，没有LDAP等系统。或者已有LDAP系统，使用AIDM对LDAP进行替代。


AIDM和主数据同步

这种情况，AIDM系统和企业内部主数据或其他用户统一管控系统通过ESB进行用户数据的同步，AIDM通过各种身份认证协议和其他内部各业务应用集成。管理员可以通过主数据系统管控用户信息。

3.企业已经有主数据或用户统一管控系统，并且有LDAP系统，希望同时使用AIDM和LDAP保持对用户统一登录认证进行管控。


同时拥有主数据或LDAP

企业内已有主数据，同时通过LDAP服务实现了对一些系统的认证集成的情况，AIDM通过ESB保证和主数据或上游系统的数据同步，同时AIDM内部提供和LDAP服务的数据同步，保证AIDM和LDAP服务中的数据一致。AIDM使用各种协议和应用系统进行认证集成，也可以保留企业内LDAP对各应用系统的认证能力。

1.3 技术架构

1.3.1 产品架构

AIDM产品自上而下可分为四层，依次为交互层、负载均衡层、内部服务层、数据持久化层。如下图所示。

1.3.1.1 交互层

交互层包括了面向普通用户的用户门户，面向管理员的管理员门户，供其他系统调用的身份认证API接口和SDK。

用户门户向用户提供用户登录功能和用户可访问的应用列表，用户个人信息编辑，最近登录信息等一些常用信息。

管理员门户提供了对应用、用户、组织机构、资源、权限、安全配置、日志等方面的管理功能，让管理员可以根据需求配置用户对各种应用的访问权限和策略。

身份认证API和SDK，提供给其他应用调用。应用通过API或SDK和AIDM进行集成，获得授权后可以获取用户在本系统中的应用权限信息，通过这种方式可以实现AIDM对应用系统内部权限的统一控制，除了单点登录以外也可以实现权限的统一管控和审计，进一步提高企业内部信息集成水平。

1.3.1.2 负载均衡层

负载均衡层接受交互层的请求，对请求进行分流或限流，将请求转发到不同服务节点上，可以实现AIDM服务的横向扩展及高可用。如果AIDM服务节点中有节点暂时不可用，负载均衡层保证AIDM服务整体对用户依然可用。

1.3.1.3 内部服务层

AIDM内部服务层整体又可以分为管理服务、协议认证服务、系统支撑服务等三部分。

管理服务负责对用户、组织、应用、资源、权限、系统证书等信息的管理。

协议认证服务提供了包括OAuth 2.0，SAML2.0，OIDC，CAS，LDAP，表单代填等认证协议的支持，负责对接各种外部业务应用，用户登录AIDM平台经过认证后，登录第三方业务应用时，该服务负责通过认证协议与第三方应用进行相互认证。

系统支撑服务包括身份验证服务、权限验证服务、日志归档服务等。身份验证服务提供了用户通过用户名密码、云之家扫码、短信验证码等各种身份认证方式认证到AIDM中的功能。权限验证服务提供了对用户访问某资源时是否拥有对应权限进行校验的功能。日志及归档服务提供了用户登录第三方应用日志记录，管理员对各种数据进行修改及日志查询的服务。

1.3.1.4 数据持久层

数据持久层封装了对数据库的操作，将对Mysql，Postgresql，以及各种国产化数据库的访问及修改操作进行封装。


产品架构

2 主要功能

2.1 多协议支持

支持多种主流认证协议，如OAuth2.0、SAML、LDAP、JWT、OPEDID、FormBased

2.2 支持多种权限控制模型

支持RBAC、ABAC权限控制模型、

2.3 多系统集成

支持AMDC、AMP、ADMQ系统集成

2.4 可扩展性

支持数据库、协议、中间件容器等组件的插件化开发

2.5 支持多种部署方式

支持容器化，私有化部署，在系统设计初期就保留对后续产品SaaS化的支持

2.6 组件国产化

系统核心框架与内部组件采用国产化设计，从系统层面保障数据信息安全， 真正意义上做到独立自主，确保企业的正常运转。

3 技术特性

3.0.1 支持多种登录认证方式

AIDM除了支持常规用户名/密码登录方式以外，还支持扫码登录，手机、短信验证码登录，指纹识别，面容识别，动态口令等，提供了更安全灵活的登录可选方案。

3.0.2 支持灵活的权限校验方式

AIDM系统除了提供传统RBAC权限管理方案，还支持按照组织、分组、个人分配对应用的登录权限，支持企业矩阵化管理，可以适应企业内各种对权限管理的模式。

3.0.3 支持多种身份认证协议

支持OAuth2.0，SAML，OIDC，表单代填等常用的身份认证协议，方便与各种应用进行快速集成。

3.0.4 稳定可靠

AIDM在部署时采用多节点部署，保证系统稳定可靠，在单节点发生故障时依然可以提供系统服务。数据存储进行主从复制，在数据库故障时可以进行快速恢复，防止数据丢失。

4 运行环境

AIDM支持容器化部署、安装包部署模式，根据部署方式不同提供不同的安装包。以下为最低规格的要求。

部署模式	操作系统	安装内容	硬件规格 (CPU/内存/硬盘)	服务器台数
容器化部署	Linux，银河麒麟	docker-compose,AIDM服务相关容器	4核/16G/100G	2
安装包部署	Linux，银河麒麟	AIDM服务，AIDM依赖服务	4核/16G/100G	2

5 总结

5.1 产品优势

5.1.1 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、OICD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。

5.1.2 单点登录

用户仅登录一次即可访问企业内具有访问权限的应用系统，不再需要重新登录验证。同理用户在一个应用系统注销会话，同时终止该用户在多个应用系统中会话的机制。

5.1.3 权限配置

目前系统权限模型基于角色的访问控制（RBAC），通过用户、角色这两种对象实现RBAC权限模型的授权。同时为了满足大型系统中的复杂组织架构设计需求，将资源、角色、授权合并在一个应用权限分组中。

5.1.4 用户管理

AIDM系统作为用户身份管理软件，需要对企业中的各个组织进行管理满足用户全生命周期的管理，如对某一个组织进行授权，某一个部门中的人员的职位变动，因业务需要对不同组织的人进行统一管理等。针对企业中人员管理的需求，AIDM提供了组织管理、用户管理，分组管理来满足各种企业间的不同需求。

5.1.5 审计日志

审计日志主要是将全部的AIDM系统账户操作日志集中记录管理和分析帮助用户对账户行为进行监控并且通过集中的审计数据进行数据挖掘，以便于事后的安全事故责任认定，所有操作行为都可以通过审计日志归档

5.2 应用价值

5.2.1 提高账户管理水平

信息安全三分技术，七分管理。企业内部众多的信息系统各自的用户认证体系，增加了管理成本，让信息管理过程中产生了更多风险点。AIDM提供了对用户账户和登录权限统一管控的平台，提供更灵活丰富的授权方式，简化了账户管控

过程，提供账户操作日志记录，帮助企业提高账户管理水平。

5.2.2 打通信息孤岛

AIDM为企业内部提供统一用户管理，用户不需要在针对每个系统记录一个单独账号，实现企业内部用户整合。

5.2.3 更安全的认证方式

随着技术进步，用户认证的方案越来越多。传统的用户名/密码登录方式一旦发生密码泄露，则会导致数据泄露无法管控。手机验证码、指纹识别、动态口令等技术为增加账户安全提供了解决方案。企业内部很多信息系统，设计之初没有考虑对新的认证方式的支持，使用AIDM，提供了多种安全性更高的认证方式，助力企业信息安全防护提升。

5.2.4 拥抱变化

传统系统中权限管理方式较为单一，经常无法适应企业内业务或管理结构调整而带来的权限管理方式变革。AIDM提供了多维度多层次的权限管理方式，可以根据不同应用场景灵活配置用户对应用的权限，适应企业业务调整时对员工权限管理的变化。

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