身份认证系统软件
JH-DAS

产品简介 | PRODUCT INTRODUCTION

JH-DAS（建恒身份认证系统）是一套安全性极高的身份认证系统，帮助企业实现在“用户名 + 静态密码”这种传统的访问方式之上，增加二次认证，二次认证方式包括动态密码、指纹、人脸、Ukey 等，有效阻止入侵者冒用合法用户的身份访问企业资源，降低企业风险。

认证方式丰富

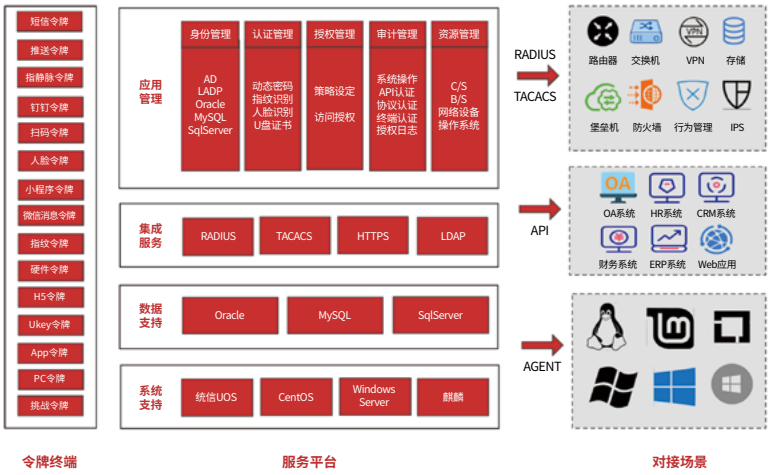
支持短信认证、邮件认证、APP 认证、小程序认证、钉钉认证、硬件令牌认证、指纹认证、人脸认证、U 盘证书认证等多种认证方式，还可以多种方式组合使用。

产品架构 | PRODUCT ARCHITECTURE

JH-DAS 身份认证系统由“服务端 + 令牌终端”组成：

服务端作为身份认证控制中心，负责用户管理、设备管理、认证管理、授权管理、审计管理等；

令牌终端作为用户信息的唯一标识，通过生成 / 接收动态密码，或采集用户信息，到服务端做校验，实现用户身份的二次验证，达到保护用户安全的目的；



产品特色 | PRODUCT FEATURES

在动态密码令牌中，安全性设计如下：

◎ 采用 SM3 国密算法生成动态密码（6 位数），每 30s/60s 变换一次（可设置），每次动态密码都有 100 万种可能，爆破难度极大；

◎ 认证系统后台可以设置错误登录次数，如 3 次，当入侵者爆破测试时，错误 3 次以后，自动锁定账户，3 分钟（可设置）以后才能再次尝试登录，此时又产生新的动态密码，之前的爆破测试失去作用。

◎ 可设置动态密码使用次数，如设置可使用 1 次时，当用户使用动态密码正常登录以后，哪怕入侵者破解动态密码，也无法使用；

◎ JH-DAS 可以选择双机部署模式。双机部署模式下，两台服务器互为主备，当一台服务器 down 机以后，另外一台正常提供认证服务，不影响客户正常业务访问；并且管理员在任何一台服务器改变数据，另外一台都会实时同步，满足日常工作需求。

令牌	提供多达 10 几种的动态令牌形式，方便用户按需组合使用，多种组合方式可以为同一客户多个应用系统或者同一应用混合使用。	**无缝**	能够与现有企业应用系统无缝集成，提供 API、SDK、源代码等多种集成方式，并提供各种开发语言的代码示例。
日志	包括接口认证日志、协议认证日志、账号锁定日志、操作日志、授权日志、审计日志等，并支持 syslog 日志上传，日志扩展和日志的自动化配置。	**登录**	登录支持操作系统的在线、离线、应急、指纹等多种认证方式。并对同一账号登录，做到自然人的一一对应，便于精准追溯。
全场景应用	支持多种应用、网络设备、操作系统的统一接入管理，具备良好的扩展性，支持国内、国际算法。内置指纹及人脸识别算法，同时支持 RADIUS、TACACS+、LDAP 等协议。	**跨平台部署**	支持跨平台部署，支持 HA、集群化部署。并支持虚拟化、国产化操作系统部署。
强大的安全机制	支持风险预警，PIN 码保护、防暴力破解、锁定风险账号、IP 黑白名单等机制，有效应对各种风险攻击。	**策略管理**	可以灵活的实现各种策略下发、管理、授权规则，并可以对特定的组、角色等进行分组、分角色进行管理。