# AccessMatrix™ UAS

新一代的通用认证服务器

## 关键优势

- 以通用的认证平台来减少成本
- 简化集成和部署工作
- 处理复杂的认证需求
- 提供面向未来的认证选择
- 提供可高度扩展且值得信赖的平台

## 特点

- 支持多种身份认证
- 完整的令牌生命周期管理
- 基于PAM框架实现身份认证
- 支持 OTP 和指纹生物识别技术
- 提供云服务
- 全面支持移动设备

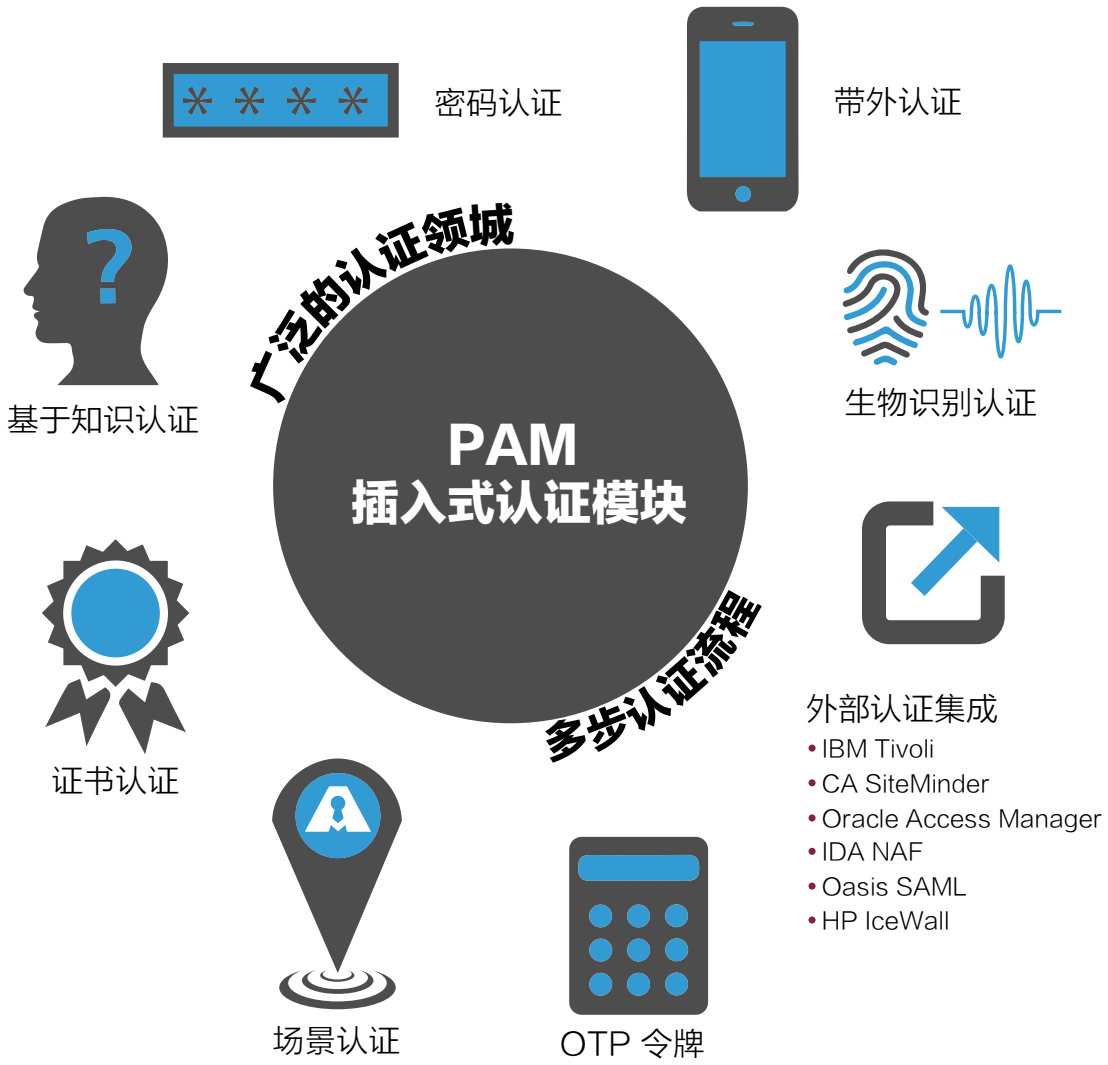
## 新一代的通用认证解决方案

AccessMatrix™ UAS（Universal Authentication Server）是新一代通用认证服务器，可以统一不同的身份验证机制,简化集成的复杂性。

UAS 采用可插拔的认证模块技术 (Pluggable Authentication Moule，PAM) 支持集成广泛的认证方法，便捷地添加新的身份验证机制。

企业还可以灵活配置认证工作流，从而满足强大的身份验证和授权需求。开箱即用的端到端令牌和生物识别技术生命周期管理平台大大降低了企业的管理成本，并缩短投放市场的时间。

UAS 基于分层分区的安全管理与授权框架，允许组织指定各级安全管理员，其可扩展性可支持外部组织管理企业的安全管理员 ID 和用户权限，且满足管理安全提供商或 SaaS 提供商提出的管理需求。



**模块组成**

UAS – E2EE 凭证数据保护模块

UAS – OTP令牌认证与令牌生命周期管理模块

UAS – YESsafe手机令牌认证与令牌生命周期管理模块

UAS – 生物识别认证与生命周期管理模块

UAS – 双因素加密认证模块

- Window桌面登陆使用 GINA & CP、终端服务器、Citrix
- RADIUS用于网络备、VPN、Unix登陆
- MS Outlook Web 访问

UAS – 应用集成的 SDK

UAS – 双因素加密认证模块

- IBM TAM 的 EAI
- CA SiteMinder 的 CAS
- Oracle Access Manager 的 CAS

UAS – HSM 集成模块

- 为保护凭证存储，以软件方式提供HSM 的密钥管理
- 内置HSM支持OTP 认证

**支持多种认证机制**

安全的密码、OTP令牌、PKI证书、生物识别技术 (指纹 、掌纹、指静脉 、面部 、声音 、虹膜)。

**支持多种形式的认证因素**

UAS 提供支持多种令牌的使用模式(OTP、挑战响应、交易签名)和多种令牌的形式因素（硬件令牌、手机令牌、短信令牌、矩阵或网格卡、机器标签令牌等）。

**插入式模块支持灵活的外部认证方式扩展**

UAS 提供可插拔的认证模块，支持集成各种供应商的令牌，如 Vaco、SafeNet、 DynamiCode、Gemalto、RSA、ActivIdentity、YESsafe（安讯奔）和基于 OATH 的供应商和生物识别设备，如 Sensetime，Face++，博宏，CrossMatch、Futronic、NEC 等。

**支持云服务**

UAS 采用行业标准（如SAML和 OAuth）实现基于云服务的安全认证集成。

**与外部认证服务器无缝集成**

UAS 支持与第三方认证和Web单点登录（SSO）服务器的无缝集成，如 LDAP 目录、Microsoft 的 AD 目录、IBM的TAM、CA SiteMinder、Oracle 的 Access Manager、新加坡的 SingPass 和 Assurity OneKey (RTAP)等。

**完整令牌的生命周期管理**

- USA 提供整个令牌生命周期管理的集成解决方案，包括：核发、交付、启用、不同步令牌丢失、不同步和逾时替换声音
- 定制化的用户界面，方便服务台工作人员使用
- 支持令牌管理功能
- 提供详细的审计跟踪信息和灵活的报告
- 可通过服务台接口实现令牌管理
- 重置和其他支持功能，如PIN Mailer集成等

**全面支持移动设备**

UAS 提供满足不同需求的手机令牌集成：如移动设备的 Vasco DIGIPASS、基于 OATH 的安讯奔 YESsafe 令牌和谷歌令牌。

**内置RADIUS服务器**

UAS 内置 Radius 服务器，可对防火墙、网络设备、VPN 服务器或任何服务器平台和支持 Radius 认证协议的应用程序等提供强大的身份认证 。

### 灵活的密码策略和质量检查

内置的静态ID与密码身份认证模块支持非常灵活的密码质量策略、密码过期策略和登录策略。

### 灵活配置验证工作流

支持企业将多个身份认证方法串连起来例如，在认证过程中使用AD身份认证加上 Vasco OTP 令牌, 以满足企业的安全需求。其灵活配置的特点，使企业能够灵活适应不同业务场景下对于认证模式的需求，如用户组、源 IP 地址、源目标等，灵活制定认证方式。

### 无缝集成外部用户存储

安全服务器支持大量用户注册 如 AD 目录 LDAP 目录等通过 LDAP 协议或 JDBC 存储的外部用户。企业可以集成现有用户注册的安全服务器，而不需要同步用户信息。

### 采用 HSM (可选)的密钥保护

开箱即用的集成模块使用 FIPS 认证的硬件设备加密密钥,为主要供应商的 HSM 产品提供先进的保护功能。

### 全面的 SDK 集成

UAS 采用 SOAP、Java 和 .NET 等 API，为各种应用提供全面的 SDK，便于集成。

### 系统要求

- 服务器OS：MS Windows Server 2008、IBM AIX、Oracle Linux、Oracle Solaris
- 应用服务器：Oracle WebLogic、IBM WebSphere 和 Apache Tomcat
- Java 运行环境：JRE 1.6 及以上
- 数据库存储：MS SQL Server、Oracle RDBMS、IBM DB2 和 Oracle MySQL
- 外部用户存储：AD目录、LDAP v3 兼容目录 and JDBC 兼容数据库
- 经 FIPS 认证的 HSM: 可集成所有的主要 HSM 供应商的产品，如 Thales-nCipher、SafeNet、Utimaco 等
- 令牌提供商的专业SDK: Vasco、SafeNet、 RSA、ActivIdentity 和 DynamiCode

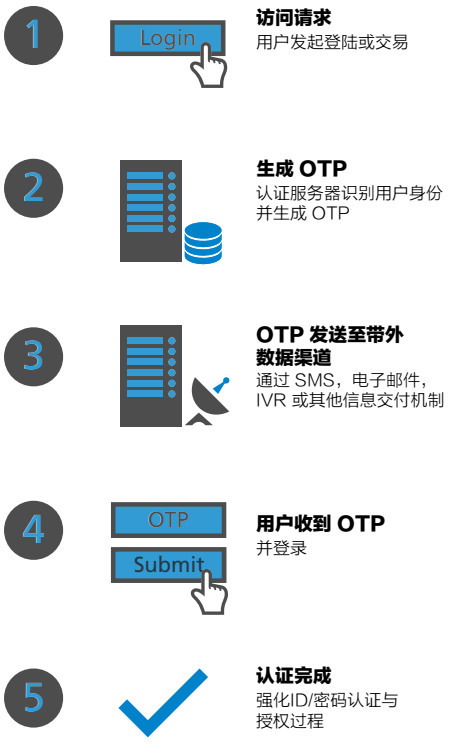
# UAS 带外认证

## 关键优势

- 通过 AccessMatrix™ UAS 灵活集成架构和细粒安全策略可实现强 OTP 身份认证解决方案的快速部署
- 通过 OOB 身份认证增强安全性，以缓解钓鱼软件的攻击
- 利用 HSM 硬件提供预先的 OTP 生成和对比选项
- 通过部署已验证的安全解决方案，降低实施成本和项目风险，最大限度地提高投资回报率
- 强大的报告能力，确保按照合规性要求报告用户活动和安全违规信息

## 特点

- 灵活的 OTP 策略
- 审计跟踪
- 多种交付机制
- 灵活的集成 SDK
- 内置 RADIUS 服务器
- 无缝集成




## 新一代多用途认证解决方案

AccessMatrix™ 带外数据（OOB）一次性密码（OTP）模块，使用两个独立渠道来认证用户身份，提供高安全的强认证解决方案。OOB 解决方案通过 GSM 短信服务（SMS）、邮件、IVR 或其他信息交付途径（不用于用户和应用系统交互渠道）来发送 OTP 给用户。当用户访问网站时，一次性密码将通过 SMS 或邮件（由用户事先设定）被发送到用户的移动电话，移动设备现在成为了安全令牌，用于接收一次性密码，这将强化现有ID与密码的认证和授权过程。

## 灵活的 OTP 策略

- 有效期
- OTP 格式 (长度、数字、字母、字母数字)
- 发送信息模板
- 一次性使用和多次使用
- 限制重置次数
- 个人认证代码改善用户体验

## 审计跟踪

AccessMatrix™ UAS – OOB OTP 提供全面的防篡改的审计日志跟踪，用来跟踪 OTP 的使用和满足交易审计要求。它提供了灵活的报告功能，可以管理用户活动和安全违规。

## 多重交付机制

UAS 通过基于 API 的 SMTP、SMPP、HTTP/S POST/GET、Web 服务，来支持 OOB OTP 的交付。

## 灵活的集成 SDK

UAS 提供全面的 SDK、SOAP、JAVA 和 .NET 的 API，各种应用程序便于集成。

## 内置 RADIUS 服务器

内置的 RADIUS 服务器，为防火墙、网络设备、VPN 服务器或任何支持 RADIUS 认证协议的服务器平台和应用程序提供强认证。

## 无缝集成

- 安全服务器支持大量的用户注册表，如 LDAP 和 AD 目录以及通过 LDAP 协议或 JDBC 的外部用户存储。
- 企业可以将安全服务器与现有的用户注册表集成，而不需同步用户信息。
- AccessMatrix™ UAS 可以访问外部用户存储目录以简化集成工作，无需写入外部用户存储，也不需更改用户信息。

## 密钥管理和加密处理

AccessMatrix™ UAS 已被证明可与HSM设备集成保护主密钥，并为高安全需求提供在HSM中的 OTP 生成与比对服务。

## 运营标准

AccessMatrix™ UAS 提供可扩展性和可靠性的功能，以满足大规模部署对服务水平和操作的严格要求。