AccessMatrix™ UAS

future proof universal authentication server

Key Benefits

- Reduce operational cost with a common authentication platform
- Simplify integration and deployment efforts
- Handle complex authentication requirements
- Cater for future authentication options
- Provide a highly scalable, open and reliable platform

Features

- Versatile Authentication Support
- Complete Token Life Cycle Management & Administration
- Embedded Vendor Agnostic Authentication Support for OTP and Biometrics
- Cloud Services Ready
- Comprehensive Support for Mobile Devices

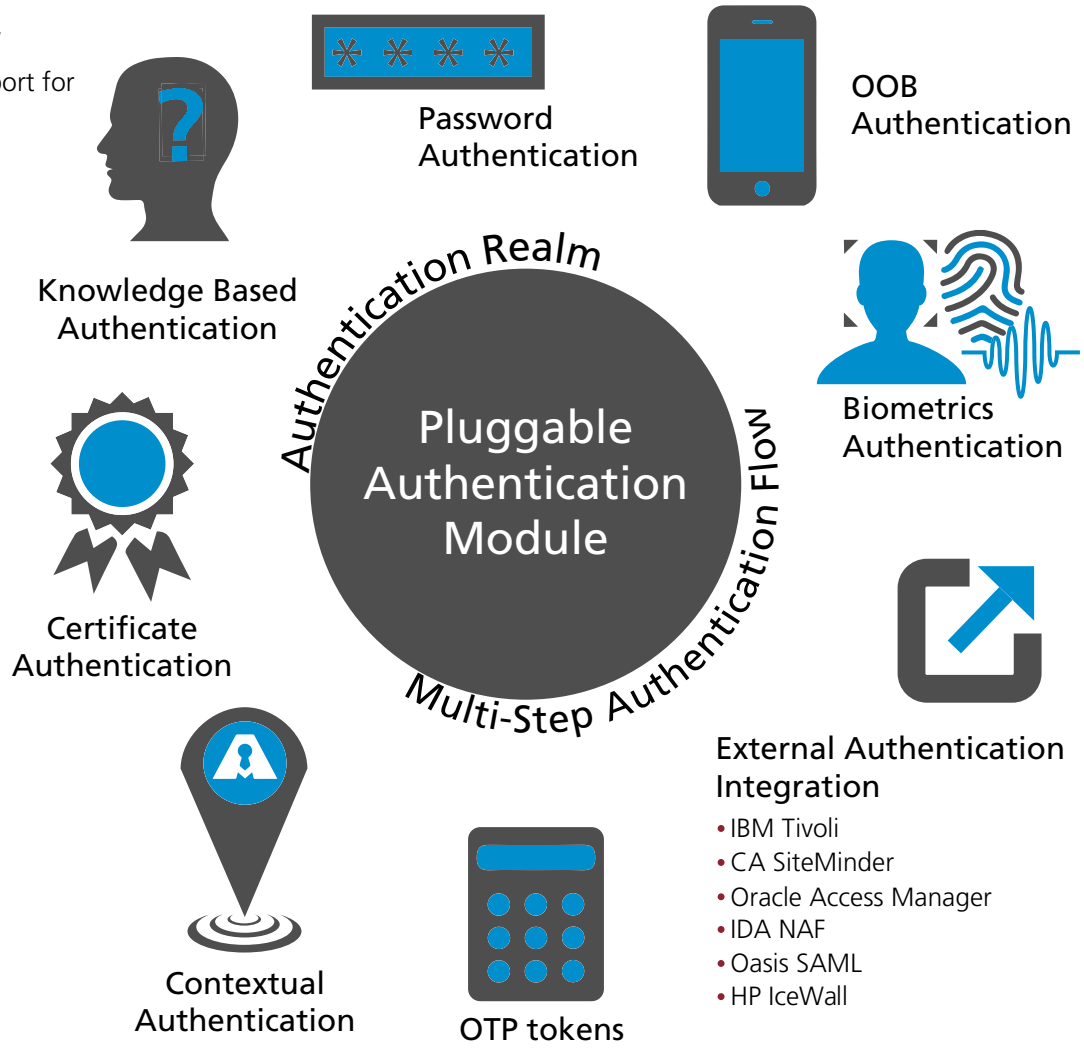
Future Proof Versatile Authentication Solution

AccessMatrix™ Universal Authentication Server (UAS) is a versatile authentication server which enables organizations to unify their different authentication mechanisms and simplify integration complexities.

UAS supports a wide range of authentication methods using a Pluggable Authentication Module (PAM) approach and new ones can be easily added to cater for evolving authentication mechanisms.

Organizations can also use the authentication workflow to chain two or more authentication methods for strong authentication and authorization requirements. The out-of-the-box end-to-end token & biometrics life cycle management module greatly streamlines the administration and reduces time-to-market.

With our patented Segmented Hierarchy-Based Security Administration and Authorization Framework, UAS allows organizations to designate security administrators at different levels of the organization. The framework can be extended to allow external organizations to manage IDs and user rights by their own security administrators. This feature has been proven to be well suited to address administration requirements for Management Security Providers or SaaS Providers.



fido CERTIFIED UAF

Modules

UAS - End to End Encryption Modules for Credential Data Protection

UAS - OTP Token Authentication and Token Life Cycle Management Module

UAS - YESsafe Mobile Token
Authentication and Token Life Cycle Management

UAS - Biometric Authentication and Life Cycle Management Module

- Fingerprint
- Facial
- Vein

UAS - 2FA for Enterprise Authentication Modules

- Windows Desktop Login using GINA & CP, Terminal Server and Citrix
- RADIUS for network devices, VPN & Unix Logins
- MS Outlook Web Access

UAS - SDK for Application Integration

UAS - 2FA Integrations for Third Party WebSSO Products

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

UAS - HSM Integration Modules

- HSM Key Manager for protection of credentials in storage
- OTP Verification inside HSM

Versatile Authentication Support

UAS provides out-of-the-box PAM modules to support various authentication mechanisms like secure passwords, OTP Tokens, PKI, Biometric Devices.

Embedded Vendor Agnostic Authentication Support for OTP and Biometrics

UAS provides out-of-the-box embedded authentication support for tokens from various vendors like Vasco, SafeNet, DynamiCode, i-Sprint YESsafe Token, Gemalto, RSA, ActivIdentity and OATH based vendors and biometric devices from CrossMatch, Futronic, NEC, etc.

Cloud Services Ready

UAS provides secure authentication integration with cloud based services using industry standard like SAML and OAuth.

Support for Multiple Form factors

UAS provides support for various Token usage modes (OTP, Challenge Response, Transaction Signing) and form factors (Hardware Tokens, Mobile Tokens, SMS Tokens, Matrix/Grid Cards, Machine Tagging Tokens, etc).

Seamless Authentication Integration with External Authentication Server(s)

UAS provides integration with third party authentication and Web SSO servers such as LDAP, Microsoft Active Directory, IBM TAM, CA SiteMinder, Oracle Access Manager, Singapore's SingPass and Assurity OneKey (RTAP), etc.

Complete Token Life Cycle Management & Administration

UAS provides an integrated solution to manage the lifecycle of OTP token devices, including issuance , Delivery, Out of Sync, Lost Token, Temporary Access, Replacement over time and other supporting functions such as PIN Mailer integration, reporting module, etc.

Comprehensive Support for Mobile Devices

UAS offers a choice of mobile token integration to meet different needs: Vasco DIGIPASS for Mobile, i-Sprint YESsafe OATH-based token and Google Authenticator.

Built in RADIUS Server

UAS has a built-in Radius Server to provide RADIUS support to offer strong authentication to firewalls, network devices, VPN servers or any server platforms and applications that support the Radius authentication protocol.

System Requirements

- Server OS: MS Windows Server 2008, IBM AIX, Oracle Linux & Oracle Solaris
- Application Server: Oracle WebLogic, IBM WebSphere and Apache Tomcat
- Java Runtime: JRE 1.7 and above
- Database for Policy Store: MS SQL Server, Oracle RDBMS, IBM DB2 and Oracle MySQL
- External User Store: Active Directory, LDAP v3 compliant directories and JDBC compatible databases
- FIPS Certified HSM: Proven integration with all the leading HSM vendors such as SafeNet, Thales-nCipher, Utimaco, etc.
- Token Vendor Specific SDKs: Vasco, SafeNet, RSA, ActivIdentity and DynamiCode

Flexible Password Policies & Quality Checks

Built-in static ID/password authentication module supports very flexible password quality policy, password expiry policy and login policy.

Login Workflow with Chained Authentication

Authentication workflow enables organizations to chain one or more authentication methods, e.g. Use Active Directory authentication plus Vasco OTP Token, during the authentication process to meet their security requirements. Dynamic authentication flow enables organizations to determine it at run-time, information such as user group, source IP-address, source targets, etc.

Native Integration with External User Stores

Security Server supports a number of user registries such as LDAP and Active Directory as external user stores via LDAP protocol or JDBC. Organizations can integrate the Security Server with their existing user registries without the need to synchronize user information.

Key Protection using HSM (Optional)

Out-of-the-box integration module for HSM products from leading vendors provides advanced protection features, using FIPS certified hardware devices, for cryptography keys

Comprehensive SDK for Integration

UAS provides comprehensive SDKs with SOAP, Java and .NET APIs to various kinds of applications to be easily integrated.

About i-Sprint Innovations

i-Sprint Innovations is the premier Identity, Credential and Access Management Solutions provider for global financial institutions and high security sensitive environments. i-Sprint maintains the highest value and reliability rankings among its clients, and is one of the most recognized names in the financial world.

i-Sprint was incorporated in Year 2000, when the company first established an office in Singapore. Singapore, being one of Asia's Top Tech cities with stable, clean and efficient government that supports a strong infocomm infrastructure and security policies, presents boundless opportunities and growth for i-Sprint. With Headquarters in Singapore, i-Sprint has expanded rapidly across Asia Pacific. We now have direct presence and active authorized partners across China (Beijing, Shanghai, GuangZhou, ShenZhen, Chengdu, Zhuhai), Hong Kong, Taiwan, Malaysia, Thailand, Japan, and the United States.

i-Sprint's Products and Solutions

i-Sprint's own unique brand of security products, intellectual properties and patents are designed to exceed global financial services regulatory requirements. In order to capitalize the fast growing Identity, Credential and Access Management (ICAM) market, i-Sprint proactively delivers innovative product features via our product offerings in **Identity Protection**, **Cloud Protection**, **Mobile Protection** and **Data Protection**.

Our world leading security solutions include a proven and secure E2E Encryption (E2EE) Authentication and Data Protection for convenient (Single Sign-On) and secure access to internet banking applications. Our solution meets Internet Banking Security Guidelines from regulatory agencies in multiple countries; overcoming the security challenges of most internet and mobile banking solutions. We deliver bank-grade versatile strong authentication (biometrics, multi-factor authentication and more) and token management platform to secure multiple application delivery environments (web, mobile and cloud) based on a common security platform.

Global Headquarters
Blk 750D Chai Chee Road
#08-01 Viva Business Park
Singapore 469004
Global: +65 6244 3900
enquiry@i-sprint.com
www.i-sprint.com

For a complete list of our offices in
United States, Malaysia, Thailand, China,
Hong Kong & Japan, please visit
www.i-sprint.com/contactus