

### Key Benefits

- Reduce operational cost with a common authentication platform
- No vendor lock-in
- 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
- Comprehensive Support for Mobile Device based authentication
- Extensible to SSO on the same platform

### The Ultimate Platform For All Your Authentication Needs

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.



Knowledge Based Authentication



Password Authentication



OOB Authentication (SMS/ OTP/ Email)



FIDO UAF Certified



Biometric Authentication (Face and Fingerprint)



Contextual Authentication



External Authentication Integration and PIN-less Authentication/ Zero-Login



OTP Tokens (Hard or Soft Token)

## Modules

UAS - End to End Encryption Modules for Authentication and Data in Transit

UAS - Hardware OTP and Token Authentication and Token Life Cycle Management

UAS - Biometric Authentication and Life Cycle Management Module

UAS - 2FA for Enterprise Authentication Modules

- RADIUS for network devices and VPN
- Microsoft ADFS Plugin

UAS - SDK for Application Integration

UAS - HSM Integration Modules

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



## Versatile Authentication Support

UAS provides out-of-the-box PAM modules to support various authentication mechanisms like secure passwords, OTP Tokens, FIDO and 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 OneSpan (Vasco), DynamiCode, i-Sprint YESsafe Token, Gemalto, V-Key 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 and OpenID Connect.

## 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, Social Network Login, 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: OneSpan (Vasco) DIGIPASS for Mobile, i-Sprint YESsafe OATH-based token and Google Authenticator. UAS also provides self-service soft token activation portal for OneSpan (Vasco) DIGIPASS for Mobile.

## 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 2012/ 2016 and Red Hat Enterprise Linux 7
- Application Server: Oracle WebLogic, IBM WebSphere, Apache Tomcat and JBoss Web Server
- Java Runtime: JRE 1.8 and JRE LTS
- Database for Policy Store: MS SQL Server, Oracle RDBMS 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 Gemalto, Thales-nCipher, Utimaco, etc.
- Token Vendor Specific SDKs: OneSpan (Vasco), Gemalto, V-Key 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 OneSpan (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 REST APIs to various kinds of applications to be easily integrated.



## About i-Sprint Innovations

i-Sprint Innovations, established in the year 2000, is a premier identity, credential and access management solutions provider that enables individuals, organizations, and societies to build trust and identity assurance for powering productivity gain through digital identity and identity of things (IDoT).

i-Sprint's unique brand of security products, intellectual properties, and patents are designed to exceed regulatory requirements such as global financial services. By incorporating the latest mobility/ biometrics/ cloud/ identification technologies, i-Sprint provides solutions that ensure secure access and protection of data, transaction and assets. i-Sprint delivers trusty, versatile and strong authentication, and identity management platform to secure multiple application delivery environments based on a common security platform.

i-Sprint's digital identity product offerings include adaptive authentication (biometrics, multifactor authentication and more), single sign-on services, end-to-end encryption (E2EE) authentication and data protection for transaction data and to secure access to the web, mobile, and cloud-based applications. i-Sprint's IDoT product offerings provide the next-gen anti-counterfeiting, track and trace, and interactive consumer engagement that aims to help business in building consumer trust, improve brand protection, personalize consumer engagement and provide business intelligence.

i-Sprint's clients include leading global and regional financial service institutions, government agencies, telecommunications, public utilities, manufacturing, healthcare, education, multi-national corporations and others. Currently, i-Sprint has a direct presence and active authorized partners across Singapore, China, Hong Kong, Taiwan, Malaysia, Thailand, Japan and the United States.

### 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

China, Hong Kong, Japan, Malaysia,  
Thailand & United States, please visit  
[www.i-sprint.com/contactus](http://www.i-sprint.com/contactus)

©2000-18 i-Sprint Innovations Pte Ltd. All rights reserved.

A Hierarchy Model is a patent of i-Sprint Innovations Pte Ltd. i-Sprint, i-Sprint logo, AccessMatrix, AccessMatrix logo are registered trademarks of i-Sprint Innovations Pte Ltd. All other trademarks and registered trademarks are property of their respective owners. i-Sprint reserves the right to make changes to the specifications or other product information at any time and without prior notice.

