



Future-Proof Versatile Multi-Factor Authentication Platform

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.

Key Features



Versatile Authentication Solution – Unifies Methods, Simplifies Integration Complexity



Complete Token Life Cycle Management & Administration



Embedded Vendor-Agnostic Authentication
Support for OTP, PKI, and Biometrics



Comprehensive Support for Mobile Device-Based Authentication
Including OATH Tokens, FIDO2, DID, and PKI



Future-Proof Solution Eases Integration of New Authentication Methods



Extensible to SSO on the Same Platform With Standard Protocols
Including OIDC, SAML and more



Out-of-Band
Authentication



Password
Authentication



Biometric
Authentication



OTP Token
(Hard / Soft Token)



Contextual
Authentication



Knowledge Based
Authentication



FIDO2
Certified



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

Available Modules



UAS End-to-End Encryption Module

For mutual authentication between clients and servers, and protecting 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 Module (E2FA)



UAS SDK for Application Integration



UAS HSM Integration Modules

HSM Key Manager for secure credential storage
OTP and Password Verification inside HSM

System Requirements

Server OS:

Windows Server 2022 (Version 21H2), Red Hat Enterprise Linux Server 8/9

Java Runtime:

JRE 17/21 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 leading HSM vendors, including nCipher, Thales, Utimaco, and more

Token Vendor Specific SDKs:

OneSpan (Vasco), Thales

Global Headquarters

Blk 750D Chai Chee Road #08-01
ESR BizPark@Chai Chee (Lobby 1)
Singapore 469004
+65 6244 3900
enquiry@i-sprint.com

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

©2000-2026 i-Sprint Innovations Pte Ltd. All rights reserved.

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.



www.i-sprint.com



[iSprintInnov](#)



[iSprintInnov](#)



[company/i-sprint-innovations](#)



Scan for more
information

i-Sprint
Trust without Boundaries