AccessMatrix™ UAM

common security platform for enterprise applications

Web Access Management, Federated SSO & Externalized Authorization Management

Key Benefits

- Ease up integration and deployment efforts with native integration with existing LDAP, AD and JDBC directories, i.e. no schema changes or no information written to the external user stores
- Provide a highly scalable, open and reliable platform to support demanding operational requirements such as automatic failover, horizontal & vertical scaling and 24x7 operations
- Provide security management and enforcement of 4As, including authentication policies, authentication methods, user stores and administration delegation, as well as audit compliance reporting
- Lower integration and operational costs with a common set of IAM services for custom enterprise and internet applications to access

AccessMatrix™ Universal Access Management (UAM) is a comprehensive web single sign-on (SSO), web access management, federated single sign-on (SSO), social network login, externalized authorization management, and hierarchy-based delegated administration system. Leveraging the AccessMatrix™ technology, UAM fulfills the most rigorous form of application security by providing secure Administration, Authentication, Authorization, and Audit services (4As) to business applications within your organization. Built on the regulatory requirements and standards in banking & finance sector, UAM enables custom enterprise/ internet applications to access a common set of IAM (Identity & Access Management) services and lowers the integration cost.

Web Access Management/ Web SSO enables SSO for customizable web-based applications that offering the option of tightly integrated web access management approach. Alternatively, Cloud-based applications, especially in distributed locations, can adopt the loosely-coupled federated SSO and it enables SSO based on standards like SAML 2.0 and OpenID Connect.

With the use of Web Security Agents (WSA) to intercept web requests, UAM provides URL based access control and Session Management for web applications.

Suitable for Cloud-based/ distributed/ Single Page App (SPA) Applications and microservices using OpenID Connect and JSON Web Token (JWT) that support for Microservices and API Gateway authentication.

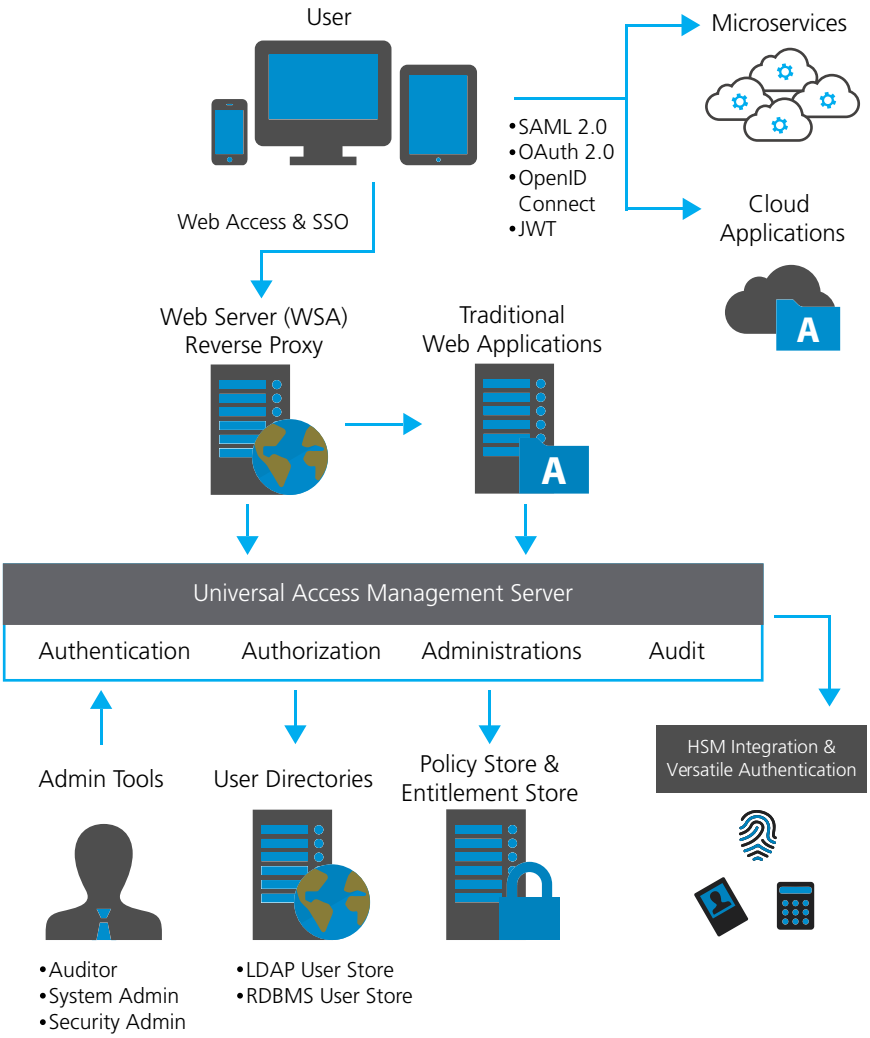
For simpler integration with Social Network Login Module, it allows social authentication/ sign-on, registration, identity mapping to existing user, and on-the-fly identity provisioning. UAM supports Facebook, Google, LINE, and WeChat.

It increases productivity and reduces cost by relieving the business application developers from having to learn, design and implement complex security/ audit/ regulatory requirements.

With our patented Segmented Hierarchy-Based Security Administration and Authorization Framework, UAM has been proven to be well suited to address administration requirements for multi-region/ department applications, B2C/ B2B banking applications, and SaaS Providers.

Key Features

- Embedded Strong Authentication, Web SSO, Federated SSO and Enterprise SSO on the same backend
- Extensible Pluggable Authentication Modules support strong authentication requirements using SMS, hardware and software tokens
- Flexible and open APIs are provided for ease of integration and code re-use for security 4As services
- Support SAML, OAuth and OpenID Connect
- Tamper-evident Audit Trail
- Scalable



Application Integration

- UAM provides REST APIs for ease of integration and code re-use for security 4As services.
- Web Security Agent Reverse Proxy enable UAM to support URL level access control for web applications with ability to transparently push user information via standard HTTP request headers to assist your web applications in establishing the user identities and aggregate information from multiple directories.
- Native Integration with External User Stores, such as LDAP and Active Directory as external User Stores via LDAP protocol or JDBC, enable organizations using their existing user registries without the need to synchronize user information. UAM server can access the external user store(s) directory to simplify the integration efforts.

Scalability

Design for Reliability and Scalability, UAM leverages commercial grade java application servers such as IBM Websphere, Oracle WebLogic to support high availability, horizontal & vertical scaling and 24x7 operations. UAM has production sites with up to 10 million accounts.

Authentication

- Flexible Password Policies and Quality Checks are supported by the built-in proprietary static passwords and LDAP authentication module. Enhanced end-to-end encrypted passwords with HSMs are also supported.
- Extensible Pluggable Authentication Modules support strong authentication requirements using SMS, FIDO UAF, hardware and software tokens. Some of the token vendors include OneSpan (Vasco), Gemalto, OATH, V-Key, etc.

Externalized Authorization

- Built-in Role-Based Access Control (RBAC) model grants applications specific roles to both users and groups. Upon successful authentication, user role information can be passed to applications transparently via HTTP header or via web service integration.
- User Authorization Mapping of user IDs in different applications to a unique SSO IDs is useful for co-existence strategy when existing applications wish to migrate to the UAM SSO system. Such user information can again be transparently passed to applications protected by WSA or via web service integration.

Administration

- Delegation & Administrative Scope can be defined by the web-based Admin Console. Security administration functions can be restricted to an OU/ segment within a particular user store e.g. Active Directory. Administrative rights can be delegated from root administrators to another administrator down the reporting hierarchy to decentralize administration and ensure a high level of accountability. The framework can be extended to allow external organizations to manage IDs and user rights by their own security administrators with a custom admin interface.
- The Best Security Practices such as key management with established HSMs (Hardware Security Modules) enabled UAM to enforce principles like dual control workflow, the least privilege, and segregation of duties effective for the change of security policies and other critical operations via our admin console.

Audit

- Tamper Evident Audit Trail addresses administration, access and transaction audit requirements. Other than the standard audit trail logging, UAM audit APIs can be used to generate application specific audit trail information.
- Ready Module for Audit Reports offer a standard set of user-centric reporting capabilities to both administration and access activities.

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

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