AccessMatrix™ UAS
future proof universal authentication server

UAS Out-of-Band One Time Password is designed for easy integration with existing applications without having to synchronize user information

Key Benefits

- Rapid deployment of strong OTP authentication solution via the AccessMatrix™ UAS flexible integration framework and granular security policies

- Enhance security with OOB authentication to mitigate phishing attacks

- Leverage HSM hardware to provide the advance OTP generation and comparison options

- Maximize ROI by reducing implementation costs and project risks by deploying a proven security solution with solid track records

- Ensure compliance with powerful reporting capabilities to report user activities and security violations

Features

- Flexible OTP policies
- Audit Trail
- Multiple Delivery Mechanisms
- Flexible integration SDKs
- Built-In RADIUS Server
- Native Integration
- Key Management & Crypto Processing
- Operational Standard - Meet the most stringent service level and operational requirements for large-scale deployments.

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 by providing off-the-shelf strong authentication modules for common applications.

AccessMatrix™ Out-of-Band (OOB) One Time Password (OTP) Module provides a secure authentication solution by using two separate channels to authenticate a user. This solution delivers an OTP to users via GSM Short Message Service (SMS), email, IVR or any message delivery mechanism which is different from the channel that the users interact with the applications. When a user tries to access a website, an OTP will be sent to his mobile phone via SMS or email which has been determined by the user in advance. Mobile devices can now become security tokens to receive OTPs that will strengthen the existing ID/ Password authentication and authorization process.

The complexity (length and format) and expiration of the generated OTP can be configured to comply with security policies of the organization.

1 **Access Request**
User initiates a login or transaction

2 **OTP Generated**
User identified by authentication server and OTP generated

3 **OTP Sent to OOB Channels**
via SMS, email, IVR call or other message delivery mechanism

4 **User receives OTP**
and can login

5 **Authentication Complete**
ID / password authentication and authorization process strengthened

System Requirements

- Server OS: MS Windows 2012 R2, 2016 and 2019, Redhat Enterprise Linux 7.x and 8.x, Ubuntu Server 18.04.
- Java Runtime: JRE 11 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

Flexible OTP Policies

- Expiry time
- OTP format (length, number, alpha, alphanumeric)
- Outgoing message template
- One-time use vs Multi-use
- Restriction to number of retries
- Personal Authentication Code to improve user experience

Audit Trail

AccessMatrix™ UAS - OOB OTP provides comprehensive tamper-evident audit trail information to track the usage of OTP and address the transaction audit requirements. It offers flexible reporting capabilities for administration, user activities and security violations.

Multiple Delivery Mechanisms

UAS supports delivery of OOB OTP via SMTP, SMPP, HTTP/S POST/ GET, Web Services based APIs.

Flexible Integration SDKs

UAS provides comprehensive SDKs with REST APIs to various kinds of applications to be easily integrated.

Built-In RADIUS Server

Built-in server offers RADIUS Server for strong authentication to firewalls, network devices, VPN servers or any server platforms and applications that support the RADIUS authentication protocol.

Native Integration

- 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
- AccessMatrix™ UAS can access the external user store(s) directory to simplify the integration efforts. No schema change is required and no information needs to be written to the external user stores

Key Management & Crypto Processing

AccessMatrix™ UAS has proven integration with HSM devices to protect the master key and support for OTP generation and comparison inside the HSM for high security needs.

Operational Standard

AccessMatrix™ UAS provides proven scalability and reliability features to meet the most stringent service level and operational requirements for large scale deployments.

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.

20211011