Abstract

AccessMatrix suite of integrated ICAM (Identity, Credential, Access Management and Versatile Authentication solutions) enable organizations to effectively deploy versatile authentication, unified single sign-on, secure credential management services, flexible identity & role administration, externalized authorization, and provide comprehensive data analytics of access to important information assets.

This whitepaper describes the technical architecture and security features of AccessMatrix and how the AccessMatrix Suite of security solutions can effectively address the ICAM requirements.
TRADEMARK INFORMATION and DISCLAIMER

The information contained in this document represents the current view of i-Sprint Innovations Pte Ltd on the issues discussed as of the date of publication. Because i-Sprint must respond to changing market conditions, it should not be interpreted to be a commitment on the part of i-Sprint, and i-Sprint cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. i-Sprint Innovations Pte Ltd makes no warranties, expressed or implied, in this document.

The i-Sprint Innovations Pte Ltd logo, AccessMatrix, Universal Sign-On/USO, YESsafe are trademarks of i-Sprint Innovations Pte Ltd.

Product and company names mentioned herein may be the trademarks of their respective owners. All other registered or unregistered trademarks and service marks are properties of their respective companies and should be treated as such.
CONTENTS

1.  INTRODUCTION ............................................................................................................. 3

   1.1  KEY CHALLENGES IN ICAM .............................................................................. 6

        1.1.1  High Total Cost of Ownership ................................................................. 6
        1.1.2  High Risk of Information Leakage & Fraud in a Divergent World of IOT .... 6
        1.1.3  Inferior User Experiences and Cost of Helpdesk Calls ......................... 6
        1.1.4  High Cost & Complexity in Access Governance ................................ 6

   1.2  KEY BENEFITS OF ACCESSMATRIX SUITE ...................................................... 6

        1.2.1  Lower Total Cost of Ownership (TCO) ...................................................... 6
        1.2.2  Manage Risk via Traditional and Adaptive controls ............................... 7
        1.2.3  Enhance Productivity & User Experience with Unified Single-Sign-On & Biometrics ................................................................. 7
        1.2.4  Ensure Access Governance and Compliance .................................... 8

2.  ABOUT ACCESSMATRIX ............................................................................................ 9

   2.1  ACCESSMATRIX INTEGRATED SECURITY ARCHITECTURE .............................. 9
   2.2  ACCESSMATRIX SUITE OF PRODUCTS ................................................................ 10

3.  SEGMENTED HIERARCHICAL ADMINISTRATION MODEL WITH GRANULAR
    DELEGATION .................................................................................................................. 11

   3.1  FINE GRAIN ADMINISTRATION RIGHTS ................................................................ 13
   3.2  FINE GRAIN ADMINISTRATION DELEGATION .................................................. 14

4.  VERSATILE AUTHENTICATION ................................................................................. 16

   4.1  PLUGGABLE AUTHENTICATION MODULE FRAMEWORK ............................... 16
   4.2  END-TO-END ENCRYPTION ................................................................................. 17
   4.3  STRONG AUTHENTICATION AND ADVANCED END TO END TOKEN LIFE CYCLE MANAGEMENT ................................................................. 17
   4.4  DYNAMIC CHAINED AUTHENTICATION ............................................................ 18
   4.5  ADAPTIVE AUTHENTICATION & ACCESS CONTROL ........................................ 19
   4.6  AUTHENTICATION AS A SERVICE (AAAS) ........................................................... 19

5.  SESSION MANAGEMENT AND SINGLE SIGN ON ..................................................... 21

6.  IDENTITY GOVERNANCE AND ADMINISTRATION (IGA) ........................................... 23

   6.1  PROVISIONING PROCESS ..................................................................................... 23
   6.2  SELF-SERVICE REQUEST & APPROVAL PROCESS ......................................... 23
   6.3  RECONCILIATION PROCESS ................................................................................ 24
   6.4  ATTERTATION / RE-CERTIFICATION PROCESS ............................................... 24

7.  PRIVILEGED ACCOUNTS AND ACTIVITIES MANAGEMENT (PAAM) ......................... 25

   7.1  PROVISIONING PROCESS ..................................................................................... 25
   7.2  CHECKOUT REQUEST / APPROVAL PROCESS .................................................. 25
   7.3  RECONCILIATION AND ATTESTATION PROCESS ............................................. 26
   7.4  PRIVILEGED SESSION MANAGEMENT (PSM) .................................................... 26
   7.5  UCM PASSWORD CONSUMERS .......................................................................... 26

8.  EXTERNALIZED AUTHORIZATION ............................................................................. 27

9.  AUDIT TRAILS .............................................................................................................. 29

10. RELIABILITY, AVAILABILITY AND SCALABILITY ....................................................... 30
Technology Overview of AccessMatrix

10.1 RELIABILITY AND AVAILABILITY .......................................................... 30
10.2 SCALABILITY ................................................................................. 31

11. OTHER KEY FEATURES ........................................................................... 32
11.1 SECURE COMMUNICATION ................................................................. 32
11.2 KEY MANAGEMENT ................................................................. 32
11.3 EASE OF MANAGEMENT ................................................................. 32
11.4 EXTENSIBILITY & CUSTOMIZATION ................................................... 32

12. TECHNOLOGY COMPONENTS OF ACCESSMATRIX .................................. 34
12.1 DATA STORE COMPONENT .................................................................. 34
12.2 CLIENT COMPONENTS ....................................................................... 35
   12.2.1 Admin Console .......................................................................... 35
   12.2.2 Self-Service Portal ...................................................................... 35
   12.2.3 Client SDK ................................................................................. 35
12.3 SERVER COMPONENTS ....................................................................... 35
   12.3.1 Service Manager .......................................................................... 35
   12.3.2 Report Manager .......................................................................... 35
   12.3.3 Event Manager ............................................................................. 36
   12.3.4 Key Manager ............................................................................... 36
   12.3.5 Embedded RADIUS Server .......................................................... 36
   12.3.6 House Keeping Module ................................................................. 36

13. FEATURES SUMMARY ........................................................................... 37

14. CONCLUSION ....................................................................................... 41

CONTACT INFORMATION ............................................................................ 42

FIGURES
1. ACCESSMATRIX HIERARCHY-BASED ADMINISTRATION MODEL .................... 13
2. ACCESSMATRIX PAM FRAMEWORK SUPPORTS MULTIPLE AUTHENTICATION METHODS .............................................................. 17
3. TYPICAL ACCESSMATRIX DEPLOYMENT CONFIGURATION ................................................................. 30
4. ACCESSMATRIX TECHNOLOGY COMPONENTS ........................................ 34

TABLES
1. ACCESSMATRIX AUTHORIZATION MODEL ................................................... 28
2. ACCESSMATRIX AUDIT TRAIL INFORMATION ................................................. 29
1. INTRODUCTION

AccessMatrix Suite of ICAM and Versatile Authentication solutions are designed and developed based on the AccessMatrix Integrated Security Architecture (ISA) framework to enable organizations to address the access challenges through:

- **Unified Identity & Role Management**
  - Provide a common identity and role management platform to enable organizations to control identity provisioning, self-service request approval, reconciliation and attestation processes driven by consistent and flexible SoD, approval and entitlement policies.

- **Unified Authentication**
  - End-to-end encryption to prevent information leakage
  - Provide a common authentication and token management platform to enable organizations to deploy multiple advanced authentication mechanisms across multiple applications and delivery channels.

- **Unified Single Sign-On**
  - Mobile SSO via OAUTH and SAML
  - Web SSO for COTS and in-house web applications
  - Enterprise SSO for web and legacy non-web applications
  - Federated SSO via SAML to Cloud services

- **Unified Credential Management**
  - Use a compliance approach to manage the use of privileged accounts, passwords and session activities to control access to confidential information and prevent information leakage

- **Unified End Point Reporting**
  - Provide activity tracking and reporting capabilities to report admin tasks, access activities and security violations to monitor access to corporate information assets and comply with compliance reporting requirements.

The suite of AccessMatrix solutions are proven solutions and have been deployed in many regional and global financial institutions and security sensitive organizations to address most of the most stringent security requirements and challenges.

As Gartner Group has nicely summed up the capabilities of our solutions “…. Its roots are in the banking industry…. its products have been battle-tested in some demanding financial environments.”
1.1 Key Challenges in ICAM

1.1.1 High Total Cost of Ownership
Enterprises face high integration and deployment cost integrating products from different vendors. Even products from the same vendors might not work as they are acquired from different companies. Furthermore, enterprises have invested in HSMs and key management process to manage risk of data confidentiality, data integrity, authenticity and non-repudiation but not all ICAM products are designed to integrate with and leverage client’s existing HSM infrastructure.

1.1.2 High Risk of Information Leakage & Fraud in a Divergent World of IOT
Enterprises today face daunting challenges of end-to-end encryption, weak authentication and complex SSO session management due to divergent technologies e.g. Cloud, virtualization, social media, mobile devices and IoT (Internet of Things) across different communication channels. For example, the recent HeartBleed incident leaks information for years and affect almost all web services while hackers stealing passwords from database and selling them online to fraudsters.

1.1.3 Inferior User Experiences and Cost of Helpdesk Calls
Without unified SSO, employees and customers tend to complain about having to sign on to multiple services and devices at the same time. Having multiple passwords for multiple services also increase the helpdesk calls.

1.1.4 High Cost & Complexity in Access Governance
With information increasingly stored in the Cloud and demand for BYOD, enterprises face mounting challenges in ensuring compliance to security policies. Passive data collection and audits are no longer adequate to manage entitlements and access to critical resources. Data analytics and regular attestation process are preventive and active measures in managing risk.

1.2 Key Benefits of AccessMatrix Suite

1.2.1 Lower Total Cost of Ownership (TCO)
Unlike other competition, i-Sprint AccessMatrix suite of products are designed using the same platform. They are well-integrated with each other with option to share the same database and deploy into client’s existing Oracle Weblogic or IBM WebspHERE application servers as well as integrating natively to existing user directories or replica of authoritative user tables. Integration with major brands of HSMs from Safenet and Thales
are supported “out of box” so that encryption keys within AccessMatrix can be protected by client’s HSM infrastructure.

Client can start with authentication & SSO in first phase and moves to Identity Provisioning and Privileged Account Management in 2nd phase or in any order deemed appropriate to the client’s IAM strategy to minimize disruption to operation. i-Sprint and its partners offers cost effective Professional Services to assist clients in planning and phased implementation. Additional product features and modules can be activated using software license keys with ease with incurring additional infrastructure cost. No more expensive integration and deployment effort. AccessMatrix delivers a highly scalable and open authentication platform to support varying and dynamic requirements of authenticating enterprise users, channels, mobile devices and cloud services. Integration is simplified via agent-based or familiar web and EJB services using SOAP, XML RPC, REST or Message Driven Mean. This relieves clients’ developers from security component development that they might not have the core competency.

1.2.2 Manage Risk via Traditional and Adaptive controls

Beyond traditional authentication and access control mechanisms, AccessMatrix also supports adaptive access controls for step-up authentication and transaction signing for high-value transactions or by automatic trust elevation based on user’s contextual information such as correlation between known devices, geo-location and time of access. Combined with the YESsafe mobile token, Out-of-band and dual channel authentication and transaction signing are user friendly yet secure authentication mechanism. To address internal fraud and information leakage such as HeartBleed, AccessMatrix offers end-to-end encryption (E2EE) that significantly reduces the risk of leakage of important data in storage and during transit. E2EE protects sensitive information such as passwords from password cracking tools as well as rogue developers or network sniffers.

1.2.3 Enhance Productivity & User Experience with Unified Single-Sign-On & Biometrics

AccessMatrix provides Single-Sign-On capability, sign-on automation, enhancing authentication process and consistent password management policies across all web and non-web applications, mobile devices and cloud services. The SSO capabilities speed up access, improve user experiences and reduce helpdesk calls. The data analytics for the user-centric, consolidated access information provides the insights into access patterns and security violations.

Clients can also deploy many of the AccessMatrix’s built-in biometric authentication offerings to improve user experiences while ensuring authenticity e.g. passphrase-based voice authentication during helpdesk calls or face recognition at branches or ATMs.
1.2.4 Ensure Access Governance and Compliance

- **Simplify User Administration with Granular Delegation**
  Users and their privileges are defined within AccessMatrix and it offers a unique and efficient approach to manage user access to applications in the enterprise. The patented segmented hierarchy-based security administration and authorization framework enables security administrators to be appointed at every level of the organization structure. The administration rights of the local security administrators can be defined at a granular level to improve security and reduce administration costs. This innovative framework allows user IDs/passwords and privileges to be managed at the local level. This hierarchical administration model can be extended to include external organizations, i.e. customers and business partners to allow the management of IDs and user rights by their own security administrators.

AccessMatrix fine-grained security administration model can also work with existing user registries, e.g. LDAP, Microsoft NT Domain or Active Directory, etc. to further simplify user management and administration flexibility.

- **Enforce Enterprise-Wide Security Policy**
  Enterprise-wide security policies can be defined and managed by AccessMatrix in a segmented hierarchy that closely mirrors a company’s existing organization structure. Security policy can therefore be controlled and enforced from a company’s headquarters to all subsidiaries, departments and other internal and external business units.

- **Implement Best Security Practices & Principles**
  AccessMatrix supports the principles of least privilege and segregation of duties. The product clearly segregates the job function between the security administration and the system administration. Security administrators are assigned granular administration rights according to their job functions. The scope of the security administration rights is limited to the segment and subordinate segments. Unlike other products, the granularity of administration rights within AccessMatrix can be delegated within a clearly defined scope. Maker-Checker control can be used to further ensure that modification submitted by one administrator must be approved by another administrator before the proposed changes become effective. In addition, AccessMatrix can ensure that the same user will not be assigned to multiple roles that may cause conflicts of interest.
2. ABOUT ACCESSMATRIX

2.1 AccessMatrix Integrated Security Architecture

AccessMatrix Integrated Security Architecture (ISA) is an integrated identity, credential and access management framework designed from the ground up to meet the requirements of security-sensitive environments. Its unique security administration, authentication, authorization and data encryption model support new and existing applications in the enterprise for provisioning, access control, single sign-on and strong authentication requirements.

Built on JAVA technologies, open architecture, flexible integration framework and based on the Domain-Driven Design (DDD), AccessMatrix ISA has the core components to provide enterprise universal authentication, access control and security administration features.

With our patented (PCT/SG/2002/000027) Segmented Hierarchy-Based Security Administration and Authorization Framework, AccessMatrix effectively addresses the challenges in managing security for large user communities within a single organization or across multiple organizations. It provides centralized policy management services for administrators to easily and effectively manage application permissions, user privileges, and security policy throughout the entire organization. AccessMatrix is highly configurable and provides practical and powerful features to address the needs of large organizations.

AccessMatrix ISA is highly configurable and provides the following core security features to business applications:

**Flexible Security Administration Model**
- Segmented hierarchical administration model to efficiently and easily manage both internal and external users; decentralized administration through granular assignment of administration rights to security administrators at all levels of an organization.
- Built-in support for best security principles and practices. The AccessMatrix infrastructure is designed to be administered without any super-users.
- Enforcement of an enterprise security policy by applications
- Native integration with enterprise directory servers, e.g. Microsoft Active Directory, LDAP, etc, without user synchronization required.
- Common repository of application access rights

**Advanced Authentication Management**
- Pluggable authentication module to support a wide range of industrial strength authentication methods using multi-factor and multi-step approaches and provide the extensibility to incorporate new authentications easily
Technology Overview of AccessMatrix

- Powerful and flexible authorization model
- Support single sign-on to both web and desktop applications
- Comprehensive integration SDK based on web services, Java and .NET APIs
- Dynamic user defined attributes with optional encryption feature at various object levels such as applications, users, groups, etc.

These features are specifically incorporated into our AccessMatrix suite of ICAM products to meet the security and operational requirements of enterprises with high-risk business applications.

### 2.2 AccessMatrix Suite of Products

The current product offerings from i-Sprint include:

- AccessMatrix™ Universal Identity Manager (UIM),
- AccessMatrix™ Universal Authentication Server (UAS),
- AccessMatrix™ Universal Sign-On (USO),
- AccessMatrix™ Universal Access Management (UAM)
- AccessMatrix™ Universal Credential Manager (UCM)

The AccessMatrix products are engineered to meet the high standards of security sensitive environments.
AccessMatrix Universal Identity Manager (UIM)

An identity and role management solution that combines established IdM processes such as provisioning, self-service request approval, reconciliation and attestation driven by relevant enterprise policies to address productivity and security of onboarding and off-boarding of employees, partners and suppliers in an enterprise. It is designed from the ground up to fit in an SOA-based enterprise architecture and seamlessly integrate both account and role management with advanced fine-grained role scope management.

AccessMatrix Universal Authentication Server (UAS)

A versatile authentication server enables organizations to unify their different authentication mechanisms and simplify integration complexities. The out-of-the-box end-to-end token life cycle management module greatly streamlines the administration and management of token logistics.

AccessMatrix Universal Sign On (USO)

A Web Based Enterprise Single Sign-On (ESSO) solution enables organizations to achieve single sign-on to both web and non-web applications without any code change. The native integration of most leading Web Access Control solutions and strong authentication devices unify the SSO infrastructure to improve end point security and end user experience.
AccessMatrix Universal Credential Manager

A Web Based Privileged Account management solution with multi-level access approval process empowers organizations to manage the use of privileged accounts and session activities where policy-driven automatic password management ensures compliance.

AccessMatrix Universal Access Manager

A web service based integration platform with 4As security components and agent technologies enable organizations to strengthen application security and enforce fine grained access control policy to manage users in accessing confidential information and critical business transactions.
3. SEGMENTED HIERARCHICAL ADMINISTRATION MODEL WITH GRANULAR DELEGATION

The AccessMatrix architecture is based on our patented segmented hierarchy model, which allows granular delegation of system and user administration tasks based on our clients’ operation requirements. AccessMatrix provides powerful administration services for security administrators to easily and effectively manage application permissions, user privileges and security policies throughout the entire organization.

Our unique Patented Segmented Hierarchy-based Administration and Authorization Framework enables highly scalable security and user administration to reduce on-going operational costs by delegating user administration tasks to departments within an organization and external customers without reducing security control and accountability. Security / User administrators can be assigned at each level of the organization and they could be assigned the minimum privileges required for their job functions within a clearly defined scope. The security administration tasks and system administration tasks can be assigned based on the current job assignment.

3.1 Fine Grain Administration Rights

AccessMatrix supports a segmented hierarchy-based access management model as illustrated in the following figure:

![Segmented Hierarchy-based Policy-driven Model Granular delegation](image)

**Figure 1 – AccessMatrix Hierarchy-Based Administration Model**
For example, three administrative roles can be defined to perform the administrative functions:

- **Policy Admin**: Administrators who are responsible for defining system or region wide security policy such as authentication method, security registry for authentication
- **Application Admin**: Administrators who are responsible for maintaining applications information and features
- **Security Admin**: Administrators who are responsible for maintaining user profiles and user’s access rights for access specific applications

From the security administration perspective, each business division, department or unit within an organization can be represented by segments. Segments are linked to form a segment hierarchy, which can be used to represent an organization’s existing structure. This technique can be extended so that the segments could represent related external organizations, such as business partners.

Within each segment, principal, group and application nodes can be created to represent users, groups of users, and applications/objects within the business respectively. This in turn allows the security policy to be defined at the segments level or inherited from its parent segment.

Security administrators can be created at segment level to manage security within their respective segments and sub-segments. In addition, multiple security administration roles or functions e.g. policy officers, security auditors, application, principal and segment administrators can be created at each segment. By allowing the administration rights for each security administrator to be tightly controlled, administrators are prevented from either accidentally, or intentionally, interfering with the security policy of the business, or access privileges of individuals in other segments.

### 3.2 Fine Grain Administration Delegation

AccessMatrix can also leverage existing enterprise directory as segment hierarchy. If customers already have a complex OU trees in Active Directory, AccessMatrix can be configured to point to Active Directory as its data source of segment hierarchy.

The granular administration delegation in the AccessMatrix system is highly flexible and it can meet most the administration requirements for most complex organizations.

The following delegation options are available:

- **Own Only**
  
  The administrator has the respective role, but does not have the delegation power to assign the role to another administrator.

- **Own + Delegate**
The administrator has the respective role, as well as the delegation power to assign the role to another administrator.

- **1 Level Delegate Only**
  The administrator does not have the respective role, but has one level delegation power to assign the role to another administrator. One level delegation power means can delegate “Own Only” option.

- **Delegate Only**
  The administrator does not have the respective role, but has the delegation power to assign the role to another administrator.

- **Own + 1 Level Delegate**
  The administrator has the respective role, as well as one level delegation power to assign the role to another administrator.

In high security environments, AccessMatrix can be configured to provide a security feature called *dual* control. This control feature requires at least two security administrators – one *maker* and the other a *checker* or *authorizer* to be involved before a sensitive administration task is completed. Dual control can be configured to be turned on or off for a specific administrative operation for a certain group of administrators.
4. VERSATILE AUTHENTICATION

Authentication is an important security service because everything depends on the identity of the user to ensure proper authorization, audit trail and accountabilities. In order to grant and control access to critical resources and services, organizations must develop a strategy to provide the proper mechanisms to identify and authenticate users. If not, organizations cannot attest that access to resources and services is being properly controlled.

A one-size-fits-all authentication approach cannot address the security challenges in today’s business operating environments. Organizations must be able to deploy various authentication mechanisms to address different risk level associated with business activities for all users across all systems and yet be able to manage the deployment and operation aspects of the authentication solutions effectively.

4.1 Pluggable Authentication Module Framework

AccessMatrix has implemented a Pluggable Authentication Module framework to enable organizations to support various authentication mechanisms. With the PAM framework, AccessMatrix has the built-in features to support many industrial strength authentication mechanisms to address the authentication requirements of the organizations. New authentication methods can be easily integrated into the AccessMatrix with the PAM interface. This future proof design provides much flexibility to cater for the changing landscape of the authentication requirements and available technologies.

Some of the out-of-the-box supported authentication mechanisms include:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Static passwords</td>
<td>e.g. default, E2EE, Microsoft Active Directory, LDAP, etc.</td>
</tr>
<tr>
<td>2. Dynamic passwords</td>
<td>e.g. Vasco DigiPass, RSA Secure ID, ActivCard Token, OATH mobile tokens such as Google Authenticator and YESsafe etc.</td>
</tr>
<tr>
<td>3. Certificates</td>
<td>e.g. X.509 based certificate</td>
</tr>
<tr>
<td>4. Trust-based authentication</td>
<td>e.g. Windows Integration Authentication (NTLM), Kerberos, SAML, etc.</td>
</tr>
</tbody>
</table>
5. Knowledge Based Authentication  e.g. Questions & Answers
6. Out-Of-Band Authentication  e.g. SMS, email, IVR, Two Channels
7. Biometrics  e.g. voice, fingerprint, face, palm vein
8. Integration with leading authentication server  e.g. IBM Tivoli Access Manager, CA SiteMinder, and Sun Java Access Manager

Customer specific PAMs can be easily developed to support existing or new authentication methods e.g. biometric authentication, End to End Encryption

![AccessMatrix PAM Framework Supports Multiple Authentication Methods](image)

Figure 2 – AccessMatrix PAM Framework Supports Multiple Authentication Methods

Other than using the programmatic interface, AccessMatrix supports declarative policy to allow security administrators to specify the authentication method required for users to access business applications without modification of the application source code. In addition, AccessMatrix also supports re-authentication of the user at the object/method level when a stronger authentication mechanism is required for some types of business transactions.

### 4.2 End-to-End Encryption

UAS E2EE is one of the bestselling UAS authentication modules as it is mandated by both Monetary Authority of Singapore as well as the Hong Kong Monetary Authority (HKMA). Clients can implement an E2EE lite version without server and HSM to first secure the internet channel followed by a full scale server/HSM-backed solution that also covers encrypted passwords within the RDBMS. The solution also comes with advanced pin mailer option for direct printing from the HSM as well as remote printing advanced
options that support generating pin in one office and pin mailers collected in another office.

UAS E2EE can prevent information leakage such as HeartBleed as well as insider frauds by application developers, 3rd party software and DBA.

For more information on how UAS E2EE can prevent HeartBleed information leakage, please visit: http://www.i-sprint.com/press/how-to-avoid-heartbleed-or-similar-ssl-related-vulnerabilities/

4.3 Strong Authentication and Advanced End to End Token Life Cycle Management

AccessMatrix PAM framework allows for rapid deployment of multi-factor 2FA solutions with minimal disruption to existing production environment while catering to complex operational deployment and maintenance scenarios. This is achieved by providing various application integration interfaces via APIs and/or Web Services and a comprehensive token management framework.

AccessMatrix provides a vendor-neutral One Time Password Token Management Framework to support co-existence of industrial-strength event-based or time-based tokens. End to End Token Life Cycle Management Functions supported include:

- Token import
- Token resynchronization & auto resynchronization
- Token assignment & un-assignment
- Change token status
- Reset token static pin
- OTP verification (Response Only or Challenge Response-based tokens)
- Token batch for tracking battery/manufacturing batch
- Token group for access control and allocation
- Token inventory report
4.4 Dynamic Chained Authentication

Another unique built-in feature of AccessMatrix is the support of chained authentication via Authentication Realm.

**Authentication Realm** allows authentication modules to be grouped, ordered and chained together as an authentication realm to meet regulatory or complex authentication requirements e.g. a static password module followed by a Vasco OTP module. The composition of the Authentication Realm can also be specified on the fly to change the behavior and the authentication process via the Admin Console or programmatically.

By leveraging the dynamic feature of the Authentication Realm, Rules based authentication can be implemented easily using application data such as User attributes, Group information, access location, etc. or external data sources such as rule based engine to determine the authentication methods.

This much needed flexibility and dynamic capability empowers organizations to take control of their authentication policy and to address the security requirements for the changing business environments.

4.5 Adaptive Authentication & Access Control

AAC (Adaptive Access control) is a useful risk management tool based on contextual or pre-assigned user information such as geo-location, group-based risk ranking and time-based access patterns. Such contextual information is then combined into a risk scoring engine to give the risk score for a particular login or access. Beyond a certain score, AccessMatrix UAS or UAM can perform a step-up authentication or trust elevation. Alternatively passive measures such as increased log level, sending warnings via out of band SMS can be used to help the real user to detect a fraud.

4.6 Authentication As A Service (AaaS)

AccessMatrix UAS Cloud Edition enables an authentication operator to run authentication as a service (AaaS) in a public or private Cloud. Such authentication service is a natural fit for SMEs and mid-size enterprises seeking to leverage a Cloud infrastructure to lower total cost of ownership and enjoy the versatile authentication offerings of i-Sprint UAS E2EE, SMS OTP, mobile tokens etc with a flexible charging model per usage or per month per user. Logistics, deployment and integration cost are much lower compared to a more traditional way of investing upfront for a dedicated on-premise authentication infrastructure. The secure, flexible and scalable multi-tenancy
Technology Overview of AccessMatrix

model of UAS Cloud Edition brings the best of YESsafe and AccessMatrix platform authentication and SSO services to enterprises in internet speed!!!
5. SESSION MANAGEMENT AND SINGLE SIGN ON

AccessMatrix provides a strong and flexible Session Lifecycle Management feature to manage user sessions. After a user has successfully authenticated to an AccessMatrix server, a random session ID will be generated. The session information is securely stored as encrypted cookie in the user browser’s memory using NIST approved authenticated encryption algorithm AES GCM to ensure authenticity, data confidentiality and integrity, which can be used to identify the user and his/her login session. A user’s login session ends when the user logs out, or is forced logout, or the session time out for the user is activated. Separate E2EE session tracking is available to prevent session replay attack.

When the user tries to access the same or other web server, the web server verifies the session cookie with the Access Manager. The user does not have to sign on again if the verification is successful. WSA ensures that SSO session cookie value changed on each new access to protected web resource, greatly reduce the risk of replay attack.

AccessMatrix provides foundation to simply the application development process and the building blocks for our Enterprise, Federated SSO and Web SSO SDK solution via:

- **Session Life Cycle Management**
  SSO session token (encrypted with MAC) can be securely passed around (e.g. as cookie) to manage SSO lifecycle (creation, idle timeout, expiry, logout). There is also option to enable persistent sessions with configurable limit on number of sessions per user.

- **Web Security Agent (WSA)**
  WSA is an interceptor at the target web/application server to transparently protect and manage Web SSO for target application. It can also push user profile information via HTTP header for ease of integration with the target application.

- **User application entitlement association with secondary accounts**
  Store what applications a user can access with secondary account id mapping to automatically translate between primary SSO user id and secondary account login id within each application.

- **ESSO information for Target applications**
  Store ESSO information e.g. the user id and encrypted password for a target application of a particular user.

- **Configurable HTTP request header and SAML assertion payload for Federated SSO / Cloud SSO**
  User response information such as login id, group memberships, application roles are configurable to be returned to application or SAML service provider upon a successful access to resource or SAML authentication request.
- **Mobile SSO via OAuth 2.0**
  AccessMatrix also provides the OAuth 2.0 server component and mobile client SDK for developers to enable organizations to implement the Mobile SSO features on mobile devices.
6. IDENTITY GOVERNANCE AND ADMINISTRATION (IGA)

According to Gartner Group, Identity governance and administration (IGA) is a set of processes to manage identity and access information across systems. It includes management of the identity life cycle that creates, maintains and retires identities as needed, as well as governing the access request process, including approval, certification, risk scoring and segregation of duties (SOD) enforcement. Core functionality includes identity life cycle processes, automated provisioning of accounts among heterogeneous systems, access requests (including self-service) and governance over user access to critical systems via workflows for policy enforcement, as well as for access certification processes. AccessMatrix UIM includes advanced role management, role-based entitlements rules, identity analytics and reporting.

6.1 Provisioning Process

UIM not only addresses provisioning of individual accounts in each resource, also shared account in account store shared by multiple resources/applications as well as shared account by multiple users. UIM also serves to maintain user properties mapping to resource account properties such that authoritative user data from HR is auto replicated to the corresponding account property within the target resources.

In the 1st stage, user entitlements can be automatically derived from a set of entitlement rules by combining multiple conditions such as user’s business role and organizational unit. The result is straight-through automatic role-based provisioning to create accounts in target resources via connectors which greatly improve efficiency of the user onboarding process. As part of the provisioning process, UIM is also designed to provide optional authentication device binding to each user e.g. binding virtual staff card such YESsafe ID, mobile token such as YESsafe token or Vasco hardware token to each user.

The second stage of provisioning involves assigning IT roles or user groups within the resource/application. If necessary, further IT role constraints (aka role scope) can be defined to further restrict what an IT role can do.

6.2 Self-Service Request & Approval Process

The objective of self-service request (SSF) is to improve productivity and cut down helpdesk costs. It could be self-service password reset via SMS OTP by employee or raising ad-hoc access requests. UIM ships with an embedded Apache Activiti BPM product with a default request-template based approval system. A request form per each self-service request type and associated approvers is managed via a request template object. The first stage of approval process is named as a template-level approval. For
example, enterprise can define two forms one for full time employee and another for part-time employee, these two forms might require different HR persons to approve.

Depending on the number of access requests and the approval process, requests might need to be split into multiple execution paths that require approvals from different application/data owners in the organization determined by the operational policy. The decisions from multiple approvers for each access are then merged by UIM before the actual provisioning process takes place.

If the default approval process does not meet complex project requirement, client can use an external workflow/ticketing system to perform request/approval and integrate it into UIM.

6.3 Reconciliation Process

Enterprise usually has authoritative data source for employees stored at the HR database. The reconciliation with the authoritative data source can be performed with incremental event-based approach or periodic full snapshot approach where discrepancies between the HR and downstream resource accounts are detected. A reconciliation rule can result in manual task assigned to administrator or an automatic attempt to reconcile the discrepancies detected. For example, if the email address of an employee is changed at HR, this change is automatically propagated to corresponding accounts in resources.

6.4 Attestation / Re-certification Process

Attestation process can be event-based or scheduled.

Certain critical actions e.g. change of employee’s business role might trigger an attestation task assigned to the line manager of the employee. The manager will be required to review the employee’s existing entitlements so redundant access can be removed. Employee will be given a grace period to make appeal to the line manager to retain such access.

Scheduled attestation is useful for a group of critical resources e.g. Finance/HR database system. An attestation policy might require the Finance and HR heads to re-certify all access to Finance/HR databases every 3 months. UIM will automatically start an attestation task assigned to them and monitor the progress accordingly. The result action is such that the certifiers can choose to accept, reject or allow exceptions for employees having access to the resources.
7. PRIVILEGED ACCOUNTS AND ACTIVITIES MANAGEMENT (PAAM)

Privileged accounts are special accounts such as Unix root or Windows administrators and Cisco router power users. AccessMatrix UCM offers PAAM capabilities on top of UIM so that enterprise could enhance risk management of such privileged accounts and their session activities.

7.1 Provisioning Process

Privileged accounts and passwords can be provisioned by UIM or another IDM product. Administrators can also choose to use CSV import for initial account bulk loading. UCM allows privileged accounts to be placed in a virtual Safe where password policies are defined. *Automatic password change* can be turned on so that UCM will automatically change the privileged account password upon each check-in or upon password expiry as configured. The UCM connector is equipped with “backoff threshold algorithm”, if a change password action failed to take place, a retry will be performed in increasingly longer period until a threshold is reached. Thereafter, an email alert will be sent to administrator to manually investigate the situation.

Passwords are automatically backed up to a passphrase protected PDF files for each privileged account with multiple versions of passwords upon each successful change. In the unlikely event that UCM is offline, such PDF files can be opened by authorized personnel for manual sign on to target resource.

7.2 Checkout Request / Approval Process

Privileged account users can submit checkout request via a standard multi-level approval process. An access policy automatically grants the rights to check out by user group and resource target type or password virtual *Safe* container of the privileged account. The approvers can be manually assigned per privileged account or determined by using an approval policy e.g. based on reporting line manager or resource owner.

A checkout request can be submitted with reservation time. If a privileged account is flagged as “allow exclusive checkout”, a reservation placed on it in a future time will exclude another checkout at the same time. A checkout request has a checkout expiry time where system might perform an automatic force check-in to terminate the checkout session in case the administrator does not check-in manually.
7.3 Reconciliation and Attestation Process

If privileged account and password goes out of sync between target resource and UCM, it should be automatically detected and administrator can manually reconcile the account password. If another reconciliation account is predefined, this account can be used to automatically reconcile the detected problematic account.

Periodically, attestation tasks can be created and assigned to application/data owners to review default access to critical target resources. User with many default accesses to many resources can be flagged as high risk by UCM within the attestation task. The certifiers can then choose to allow, remove or raise exception for the user.

7.4 Privileged Session Management (PSM)

Privileged session management starts after a successful checkout of a privileged account by user. It consists of:

1. Automatic or manual login – UCM will display password in clear for manual login or perform an automatic login on behalf of the user. There are automatic login launchers for well-known software such as putty (SSH/telnet) and Toad (db client). UCM also allows partners or PS to write custom launchers in standard MS .NET languages.

2. For session activities that require session video recording, a special Windows terminal service gateway is required. Logging into TS can be automatically performed via Kerberos.

3. Session video recording is streamed to UCM server in real time and automatically saved either to RDBMS or file system. A review of session video recording can be performed once the video conversion to MP4 process is completed.

4. Automatic keystroke captured and audited for the session

7.5 UCM password consumers

UCM password consumers are scripting batch files, JNDI data source or custom database password property file where clear database passwords pose compliance challenges. UCM password consumers are special programs that remove the need to hardcode clear database id / passwords. For scripting batch files, the batch file password consumer performs macro replacement of database password before executing it. For JNDI data source, a wrapper JDBC driver password consumer performs database login on behalf on the actual JDBC driver. It is also possible for applications to call the password consumer web service API for direct integration to retrieve database user id and password from UCM.
8. EXTERNALIZED AUTHORIZATION

For advanced requirements to externalize certain part of fine-grained access control within enterprise & channel applications, UAM offers flexible externalized authorization capabilities. Coupled with UAM’s server plugin and web service extension architecture, domain-specific data can be stored as extension table in UAM where access control information can be managed within UAM and domain specific web service API calls can be presented to the application developers.

AccessMatrix protects an application by setting required access permission for each resource of the application in terms of who can access which operation under what conditions. The general format for access permission is:

<role, resource, operation, constraints>

Within AccessMatrix, resources are logical units of an application and operations are access interfaces to business applications. The authorization model also allows the definition of various required access constraints.

AccessMatrix provides the following access constraints checking:

- Location – checking whether user logins via ip address or range of ip address (e.g. from ATM)
- Time – checking user logins within specified time range (e.g. office hours)
- Dynamic roles – Everyone, authenticated users
- User Group – restrict the viewing of users by administrator to certain groups only
- Segment – restrict the viewing of users by administrator to certain segments only
- Token Group – restrict the viewing of tokens by administrator to certain token groups only
- Contextual evaluation – combined user’s profile and domain data macro variables where the value can be determined upon actual access control check request.
- Authentication level – allow access only if user authenticated to a sufficiently high value of authentication level

On the other hand, roles in AccessMatrix represent the users or job functions of the application. Roles are application-specific. AccessMatrix controls user privileges by assigning the user to the role of the application, or by assigning a group to the role of the application and joining the user to the group.

Example: An application Banking may include an object account. Administrators can define a role teller and specify the following access permission for the application.
<teller, account, debit, certificate, office-hours, teller-machine, "amount < 1000">

Assigning user Bob to the teller role means that he is able to access this application’s account object using debit method, as teller role provided the following conditions are satisfied:

1. the user was authenticated with a digital certificate
2. the transaction is performed during office hours, 9:00 am to 6:00 pm
3. the request must be from the teller machine with IP address 10.20.30.40.
4. the transaction amount must be less than $1000

| Table 1 – AccessMatrix Authorization Model |

The AccessMatrix authorization model provides coarse-grain, medium-grain and fine-grain access control. Users within AccessMatrix are assigned to resources at 3 different levels – applications they are allowed to access, business functions they are allowed to access and custom server-plugin interface or contextual evaluation for domain data centric specific access control.

This unique model combines the strengths of the traditional Capability authorization model and the Access Control List (ACL) model. The availability of an authorization service that is intuitive and flexible will reduce application maintenance costs as application logic could be separated from security-related logic within an application.
9. AUDIT TRAILS

AccessMatrix provides detailed audit trails for activities performed by normal users and administrators. In high security environments, AccessMatrix can be configured for the audit trails to be digitally signed and sent to an independent audit log server.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description &amp; Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Audit Events</td>
<td>AccessMatrix logs the activities performed by normal users and administrators. The activities logged include actions such as login, change password, access to application &amp; object, and security administration activities and also event result such as success and failure. Administrators can be notified of specific events via emails or SMS.</td>
</tr>
<tr>
<td>Online &amp; Offline Audit Reports</td>
<td>AccessMatrix provides the online &amp; offline audit reports with support for templating &amp; internationalization</td>
</tr>
</tbody>
</table>

Table 2 – AccessMatrix Audit Trail Information
10. RELIABILITY, AVAILABILITY AND SCALABILITY

Multiple servers can be installed to provide a HA configuration to ensure reliability, availability and scalability.

- All AccessMatrix .NET and Java SDK have automatic fail over, retry features in case of fail over. The fail-over does not require any additional hardware or software and is provided as out-of-the-box features.
- AccessMatrix can be implemented using horizontal and/or vertical Scaling to address the fail over and scalability requirements by leveraging the platform agnostic feature.

10.1 Reliability and Availability

The AccessMatrix ISA framework has support for high availability using automatic failover and load balancing using external load balancer. Multiple instances of AccessMatrix security server can be deployed to support high availability.

Multiple AccessMatrix servers can be installed to provide redundancy at each level. All components have automatic fail over, retry features in case of fail over and load balancing. It is recommended to use database’s clustering features for HA.

![Figure 3 – Typical AccessMatrix Deployment Configuration](image-url)

The above diagram shows a sample AccessMatrix deployment configuration. For example, WebApp Server1 can point to AccessMatrix Server1 as primary server and AccessMatrix Server2 as secondary server. If AccessMatrix Server1 goes down, the system will automatically fail-over to AccessMatrix Server2. It will periodically check for the availability of AccessMatrix Server1 and will automatically switch back to using AccessMatrix Server1 once it is available.
If the database connection is down, AccessMatrix Server1 and AccessMatrix Server2 will automatically keep on retrying until connection is available.

The AccessMatrix server has been certified to work with the leading fault-tolerant server providers such as Stratus to ensure maximum up time of our server components to cater for mission critical environments.

10.2 Scalability

AccessMatrix can be implemented using horizontal and/or vertical Scaling to address the fail over and scalability requirements.

For vertical scaling, AccessMatrix Security Server is platform independent by leveraging Java technology and it can be deployed and executed in a wide range of operating systems and enterprise server platforms from major hardware and OS vendors: IBM AIX, HP-UX, Sun Solaris, Linux and various Microsoft Operating systems such as Windows 2008, Windows 2012.

For horizontal scaling, AccessMatrix security server can be scaled by running multiple copies of the server components across multiple enterprise servers to achieve load balancing and fail over with active-active configuration.

Because of the high availability design of the AccessMatrix server, it is important to note that the AccessMatrix server can be upgraded to higher capability servers without disrupting the services in the Production environment.
11. OTHER KEY FEATURES

11.1 Secure Communication

All connections among components of the AccessMatrix security system are secured using standard HTTPS protocol, which provides PKI-based mutual authentication, message confidentiality and integrity for all messages exchanged between AccessMatrix security components.

11.2 Key Management

AccessMatrix is designed to allow the selection of various encryption strengths and JCE provider. The default cryptographic library is the default JCE provider shipped in the JRE. All encrypted data are salted and encrypted AES algorithm. Key hierarchy can be set up so that the domain master key can be protected by an HSM via standard protocol like PKCS11. Key Change Process is also available as part of the key management features.

11.3 Ease of management

AccessMatrix can be managed just like any other Java web application using features provided by the application server. There are many commercial monitoring and profiling tools available for commercial application servers.

AccessMatrix has a built-in scheduler so that background tasks like housekeeping, monitoring, statistics collection tasks can be run and tracked. Specific events can be sent out as alerts to administrators via email or sms.

11.4 Extensibility & Customization

AccessMatrix is highly extensible with its pluggable authentication, token management modules and data stores. The web admin console is highly configurable e.g. to hide certain form field or change certain label for a certain view can be easily done.

The AccessMatrix has been UNICODE and double-byte enabled to support most native languages etc for screen display, user input and data storage. New languages can be easily added using language templates.

The languages supported today apart from English are:

- Thai,
- Japanese,
- Simplified Chinese,
Technology Overview of AccessMatrix

- Traditional Chinese,
- Arabic
- French.
12. TECHNOLOGY COMPONENTS OF ACCESSMATRIX

AccessMatrix consists of the following major components:

12.1 Data Store Component

There are a few logical data stores, each with different content:

- **Default Store**
  Default Store refers to the primary JDBC database used by AccessMatrix for storing data.

- **User Store**
  User store contains credential information about principals, such as user/group and user attributes such as email address or hand phone number. This may be part of the default store, or an external user store such as the LDAP server or proprietary user database accessible via JDBC.

- **Token Store**
  Token Store contains the 2FA tokens. This is typically the same as the default store but could also point to an LDAP server or external JDBC database.

- **Segment Store**
Segment Store contains the segment hierarchy. This is typically either the default store or Microsoft Active Directory.

12.2 Client components

12.2.1 Admin Console
This is the web based user profile management and security administration GUI tool. It allows administrators to create users, assign user privileges/attributes, define applications, access control permissions and manage security policy.

12.2.2 Self-Service Portal
This is the user self-service portal to enable the following functions:
- Self-service password reset (Microsoft Active Directory) – user must be authenticated via a set of questions & answers
- Self-service ESSO application enrollment (for ESSO only)
- Self-service ESSO password retrieval (for ESSO only)

12.2.3 Client SDK
The AccessMatrix SDK can be used to access AccessMatrix from a web application or thick client:
- Web Service APIs
  This is based on the popular XML RPC protocol. Built-in pooling, fail-over and timeout are available for .NET and Java clients. SOAP web services are also supported.
- RADIUS
  AccessMatrix authentication service is accessible via standard RADIUS protocol.

12.3 Server Components

12.3.1 Service Manager
System administrators can deploy, configure, start/stop, monitor and tune the AccessMatrix just like any other web applications via the standard console provided by the underlying Java application server platform.

12.3.2 Report Manager
The Report Manager is used by auditors to access to a comprehensive set of audit reports. Access to the audit reports is also restricted based on administrative rights. Audit reports are generated offline or online with internationalization.
support. Custom reports can also be supported via SQL views or Jasper Report Server.

### 12.3.3 Event Manager

The Event Manager collects audit log information from various components to log all administrative activities and user access activities. The activities logged include actions such as login, change password, and security administration activities and also event result such as success and failure. It can be configured to collect selective events for auditing purposes or channel certain audit events to flat file. Standard event notification is supported via sending out specific events via MQ, email or SMS.

### 12.3.4 Key Manager

The Key Manager is a standard interface to integrate with Hardware Security Module (HSM) from major HSM providers such as SafeNet, nCipher, IBM etc to provide encryption key management and meet the higher security requirements for some organizations. The interface is based on PKCS#11 or HSM specific APIs to provide the maximum integration flexibility.

### 12.3.5 Embedded RADIUS Server

The Embedded RADIUS server enables access via standard RADIUS protocol (Challenge Response is also supported). This is most useful for integration with network security devices such as VPN/Firewalls/Routers.

### 12.3.6 House Keeping Module

AccessMatrix provides standard House Keeping facility to assist on the operational requirements such as automatic rollover to system log files for easy of backup and archiving, disable and reporting of expired accounts, archiving of audit log records, etc.
13. FEATURES SUMMARY

<table>
<thead>
<tr>
<th><strong>Authentication and Single Sign-On</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single Sign-On</strong></td>
<td>Single Sign-On support for non-webSSO applications and webSSO applications without modifying the applications and enable the users to enjoy login automation for different types of application. The SSO features can be extended to Cloud based applications and mobile applications on mobile devices.</td>
</tr>
<tr>
<td><strong>Pluggable Authentication Module</strong></td>
<td>Enable AccessMatrix deploy a wide variety of authentication methods to address the business requirements for strong authentication and evolving authentication mechanisms, through a single, unified framework; new methods can be easily added to cater for evolving authentication mechanisms. Each user can be assigned different authentication methods e.g. static passwords, certificates, etc. depending on the risk level.</td>
</tr>
<tr>
<td><strong>Authentication Realm</strong></td>
<td>Linking of multiple authentication methods into one logical authentication process. AccessMatrix supports authentication workflow which enables organizations to chain two or more authentication methods, e.g. Use Active Directory Authentication plus Vasco OTP Token, during the authentication process to meet their security requirements and simplify integration efforts.</td>
</tr>
<tr>
<td><strong>Pluggable Token management module</strong></td>
<td>Support for token batch to track battery expiry or other batch related information e.g. color, country of origin, etc. Support for token group so that different group of administrators can manage different groups of tokens. Different tokens from different vendors can be integrated into the AccessMatrix token-agnostic management platform.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Password Management</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Password Safe</strong></td>
<td>A virtual password safe deposit box with strong encryption (AES) using HSM devices to store confidential information. ACL can be applied to each Password to ensure that only authorized personnel can access the confidential information. Detail audit reports are available to provide.</td>
</tr>
</tbody>
</table>
## Technology Overview of AccessMatrix

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flexible Password Policies And Quality Checks</strong></td>
<td>- Flexible password quality policy, password expiry policy and login policy</td>
</tr>
<tr>
<td><strong>Multi-Level Approval Workflow</strong></td>
<td>- Use of the configurable multi-level approval flow to provide additional controls to ensure accountabilities</td>
</tr>
<tr>
<td><strong>Audit Trail Information</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Authorization

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fine grained access controls</td>
<td>- Access control down to applications, objects, methods and parameters</td>
</tr>
<tr>
<td>Time, location and user group restrictions</td>
<td>- Access control based on time and location and user group</td>
</tr>
<tr>
<td>Business rule on parameters</td>
<td>- Access control based on parameters of the request at run-time</td>
</tr>
<tr>
<td>Application specific roles</td>
<td>- Roles are application specific, for example, the Supervisor role in application A may have different meaning in application B.</td>
</tr>
</tbody>
</table>

### Integration Flexibility

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexible Integration &amp; Customization</td>
<td>- Comprehensive and open API set for ease of integration and code re-use</td>
</tr>
<tr>
<td></td>
<td>- API sets are available for virtually all languages that support web services using XMLRPC</td>
</tr>
<tr>
<td></td>
<td>- Use built-in Radius Server and Radius Client to integrate with Radius ready devices and applications</td>
</tr>
<tr>
<td>Customized Web Interface</td>
<td>- The web interface of AccessMatrix can be customized for each application to present different views of security-related information to the end user.</td>
</tr>
<tr>
<td>Personalization</td>
<td>- Business and security-related attributes which have been defined within AccessMatrix can be utilized by applications to provide flexible and powerful personalization features via API calls</td>
</tr>
<tr>
<td>Integrity protection of audit logs</td>
<td>- Audit trials are digitally signed and may be sent to a dedicated server</td>
</tr>
<tr>
<td>Secure communications</td>
<td>- All communications between components of AccessMatrix are secured using SSL</td>
</tr>
<tr>
<td>Key Protection using HSM</td>
<td>- Out-of-the-box integration module for HSM products from leading vendors to provide advanced key management</td>
</tr>
</tbody>
</table>

### Manageability

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segmented hierarchy</td>
<td>- Security policy, applications and users are defined in a central security server based on a segmented hierarchy model</td>
</tr>
<tr>
<td>Granular administration rights</td>
<td>- Security administrators are assigned with</td>
</tr>
</tbody>
</table>
### Technology Overview of AccessMatrix

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>with flexible delegation</td>
<td>Granular administration rights and scope</td>
</tr>
<tr>
<td>Maker-Checker control</td>
<td>- AccessMatrix can be configured to ensure that certain administration modifications submitted by one administrator (maker) must be approved by another administrator (checker) before the change takes effect</td>
</tr>
<tr>
<td>Delegation</td>
<td>- Administrators can be given the option to delegate part or all their administration rights to other administrators within a clearly defined scope</td>
</tr>
<tr>
<td>Policy driven</td>
<td>- The security policy can be synchronized and enforced automatically throughout the enterprise in real time</td>
</tr>
</tbody>
</table>
| Easy management               | - The management of the user credentials, privileges and other attributes of a large user population can be easily managed via a graphical user interface of the Policy Manager  
                              |   - All components of AccessMatrix can be easily configured and managed via the web-based AccessMatrix Admin Console                          |

### Scalability and High Availability

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy deployment</td>
<td>- AccessMatrix can be quickly deployed using the standard Java web application deployment process</td>
</tr>
<tr>
<td>High availability</td>
<td>- The fail-over and high availability features can be achieved by running multiple instances of the AccessMatrix server components across multiple machines</td>
</tr>
</tbody>
</table>
## Multi-Platform Supported

| OS                  | Any operating systems with JRE 1.6 and above  
|                     | The AccessMatrix suites of security solutions have been certified to run on the following platforms:  
|                     | IBM AIX, IBM zLinux, Oracle Solaris, HP HP-UX, Linux  
|                     | Microsoft 2008 and 2012  
| Web server          | IBM Websphere Application Server, Oracle BEA Weblogic, Apache Tomcat  
| Policy Store RDBMS  | IBM DB2, Oracle RDBMS, Microsoft SQL Server, MySQL or any other JDBC compliant RDBMS  
| User Directories    | Microsoft Active Directory, Open LDAP, IBM LDAP or any LDAP / JDBC compliant user directories  |
14. CONCLUSION

i-Sprint delivers a suite of integrated enterprise-class solutions to enable organizations to effectively deploy flexible administration delegation, fine grained authorization, versatile authentication, unified single sign-on, secure credential management services and provide comprehensive audit trails of access to important information assets.

The proven AccessMatrix suite of ICAM and Versatile Authentication solutions has been deployed by large enterprises and major global and regional banks. This common security platform helps organizations unify their authentication methods by providing a common authentication and token management platform; and enhance authentication to provide single sign-on features to non webSSO applications, webSSO enabled applications, Cloud based applications and Mobile applications. This empowers the users to enjoy the benefits of Single Sign-On to different types of application; Its flexibility in managing the use of privileged User IDs and Passwords to access confidential information has helped organizations to comply with some stringent security policies; It also ensures compliance by providing user-centric activity tracking and powerful reporting capabilities to report user activities and security violations.

Built on JAVA technologies, open architecture, flexible integration framework and component based approach, AccessMatrix offers unique security administration and authorization model to address the access control, single sign-on and strong authentication requirements for the enterprise. AccessMatrix provides flexible user administration with granular delegation services for security administrators to easily and effectively manage roles, permissions, user privileges and security policies throughout the entire organization. This unique patented technology enables highly scalable security and user administration and reduces on-going operational costs by delegating user administration tasks at the various locations or organization levels (if required) without reducing accountability.

Based on our AccessMatrix framework, we offer a suite of integrated security solutions to help organization address their access control, single sign-on and strong authentication requirements. Our current product offerings, AccessMatrix™ Universal Identity Manager (UIM), AccessMatrix™ Universal Authentication Server (UAS), AccessMatrix™ Universal Sign-On (USO), AccessMatrix Universal Credential Manager (UCM) and AccessMatrix™ Universal Access Management (UAM), are engineered to meet the high standards of security sensitive environments.
CONTACT INFORMATION

Further details about i-Sprint's products are available at www.i-sprint.com. To reach us, please email us at enquiry@i-sprint.com.

About i-Sprint

i-Sprint Innovations specializes in ICAM solutions for global financial institutions and high security sensitive environments. Our mission is to deliver a suite of bank-grade, integrated enterprise class ICAM solutions to address identity management, Access Control, Single Sign-on and Strong Authentication requirements. i-Sprint's own unique brand of security products, intellectual properties and patents are designed to exceed global financial services regulatory requirements. Our Client list includes leading global and regional financial institutions, MNCs and government agencies.

©2002-2014 i-Sprint Innovations Pte Ltd. All rights reserved. i-Sprint Innovations Pte Ltd, i-Sprint, i-Sprint Innovations, enterprise services manager are registered trademarks of i-Sprint Innovations Pte Ltd in Singapore. AccessMatrix™, Universal Sign On™, Enterprise AdminGuard™ are worldwide trademarks of i-Sprint Innovations Pte Ltd. A Hierarchy Model is patent of i-Sprint Innovations Pte Ltd. All other trademarks are for identification purposes only and are the 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.