Non-Intrusive Enterprise Single Sign-On Solution – Universal Sign-On

Feb 2011

Abstract

This paper is intended for Technical or Security Architects who need to assess and evaluate Enterprise SSO solutions for their organization.

This paper provides an overview of the Enterprise Single Sign-On technology and explains the concept of non-intrusive Enterprise SSO approach that addresses the SSO requirements for a wide range of application types: Web, Windows, Terminal Server/Citrix, terminal emulator/host, and Java applications and applets based applications.

This paper highlights the unique features of I-Sprint's Universal Sign-On (USO) solution for Enterprise SSO and discusses how it can provide a non-intrusive approach to help organizations to address the challenges with increasing number of Ids and passwords that are required by the users. This evaluator guide also highlights the key considerations in selecting an Enterprise Single Sign-On solution.

.

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, eoCentral, AccessMatrix, Universal Sign-On/USO, Enterprise Admin Guard and Enterprise Services Manager (ESM) are pending 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

FIGURES

TABLES

1. INTRODUCTION

1.1 Overview of Single Sign-On (SSO)

In a typical SSO environment, a user logs in just once, then is transparently granted access to a variety of permitted systems with no further login being required until after the user logs out. This user-friendly SSO approach enables an organization to manage authentication consistently across applications, but has the disadvantage of requiring all systems to trust the same authentication service. This implies that the applications must be modified in order to trust the same authentication service. This tight integration approach may be good for certain applications and environment. For this document, we would like to explore a non-intrusive approach to address the Single Sign-on requirements.

In most organizations today, users of IT services are often required to remember many IDs and passwords in order to perform their various job functions. By deploying our enterprise single sign-on solution, our clients will improve staff and client satisfaction, resulting in improved productivity and reduced administration costs.

1.2 Defining Enterprise Single Sign-On (ESSO)

An Enterprise SSO product enables a user to access multiple systems (Web, Windows, Terminal Server/Citrix, terminal emulator/host, and Java applications and applets-based applications) after being authenticated just one time and without any source code change of the target applications. With just one primary login which could be with a password, PKI smart card, USB token, biometric scan, proximity card or combination of supported methods, users can achieve single sign-on to all of the business systems they are authorized to use.

In today's environment, most organizations have many legacy applications and tradition approach of modifying applications may not be possible due to resources, time and unavailability of source code. Therefore, organizations are exploring different alternatives to achieve SSO keeping modification of the applications as the last resort.

For Enterprise SSO solution, the user first authenticates to the ESSO product. When the user attempts to log in to a SSO-enabled business application, the ESSO product retrieves the user's name and password for that application from the SSO database and performs the login to the target system. Behind the scenes in this "authenticate once, log in everywhere" model, the system maintains a separate credential mapping (user id, password and other optional attributes) for each target application.

2. ACCESSMATRIX UNIVERSAL SIGN-ON (USO)

2.1 Overview

AccessMatrix USO is one of the product offerings from our AccessMatrix integrated suite of Credential Management solutions. All our products share the same core technology components and were designed and architected by ex-global banking security professionals in 2000, to satisfy the demanding needs of the global Banking e-security market.

AccessMatrix Universal Sign-On (USO) is a non-intrusive Enterprise Single Sign-On (SSO) solution. The USO loose integration approach complements the Plugin/API based tight integration approach of AccessMatrix Universal Access Manager (UAM). Both these solutions leverage the robust, flexible and scalable AccessMatrix security infrastructure providing a comprehensive application security solution to meet the access control challenges of most organizations.

USO was developed to support web, client-server, host based, java and thin client (Citrix/Microsoft Terminal Services) applications. With our unique approach for passing credentials into the target applications, USO supports the non-intrusive approach to SSO and it does not require any source code modification in order to achieve the SSO requirements. We have experienced varying Use-Case deployments of USO in many Banks, world-wide and have, since then, evolved the product to fully comply with the stringent internal compliance policies of such banks where they have been deployed.

Designed and built to support a large number of users, USO has many built-in features to address the deployment and implementation requirements for large organizations. The USO server-based single sign-on technology simplifies the deployment and implementation challenges for large enterprises. Our unique solution has eliminated the need for manual software installation on client workstations and minimized the on-going desktop software maintenance requirements. USO also offers automatic software configuration and upgrade to address first time deployment and future software upgrade challenges without the need to have any administrator rights on the client OS. USO provides a self-service facility to enable users to manage their IDs and Passwords for the target applications themselves, which greatly simplifies the implementation efforts.

AccessMatrix USO has been reviewed by the Gartner Group since 2006 and was featured in the Gartner Magic Quadrant for E-SSO solutions in 2007, 2008, 2009 and again in Sep 2010. All End-User references provided in such reviews have been rigorously and individually vetted and interviewed by Gartner Group accordingly.

2.2 User Experience

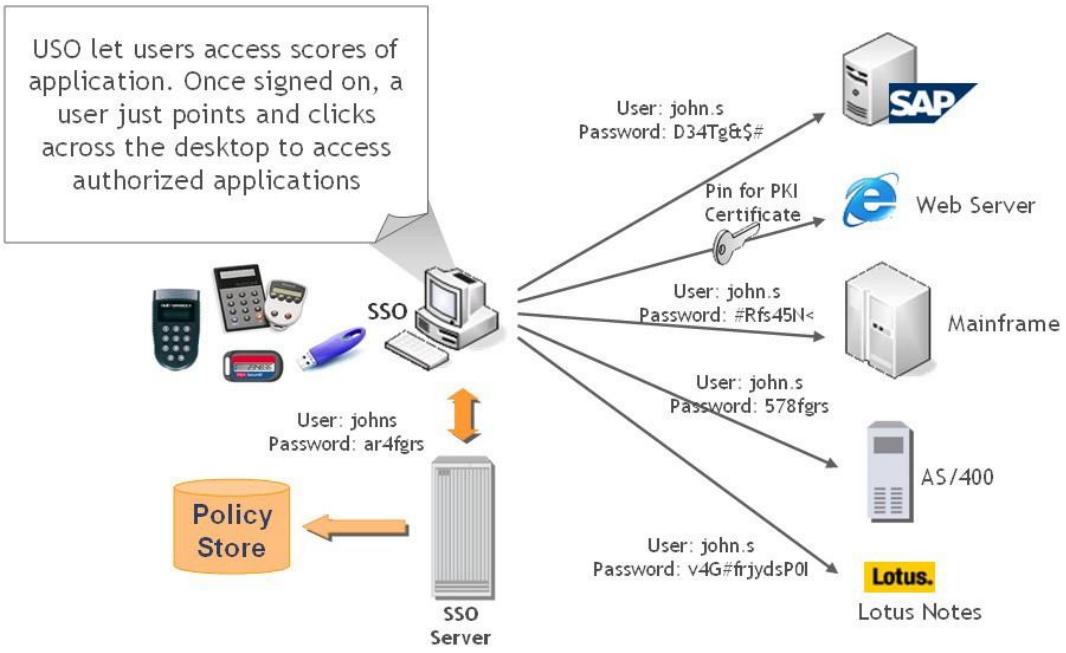

Figure 1 – Enterprise SSO Operating Model

The figure above shows the action sequence of the SSO solution:

1. User performs a "primary" authentication to the SSO server using one of the assigned login methods based on the login policy which can be static ID & password, hardware tokens, biometrics etc. Also, the USO Login can also be integrated with the Window Desktop Active Directory login i.e. after a user has successfully login to the desktop, the login to the USO server will be done transparently based on the desktop login information.
2. After the User has successfully login to the SSO server, it returns the login credential information and script or screen identification attributes of the target applications based on the application assignments.
3. Then, when the user accesses a target application, the USO Client software intercepts the standard login dialogue and replays the login credential to the application via the login dialogue to automate the login process.
4. The solution also handles the change password sequence of the application either by prompting the user to provide the new password or automatically generating a new password as per the policy.

2.3 Application Integration Process

The figure below shows the high level flow how USO works with existing applications to achieve the SSO functions for the End Users.

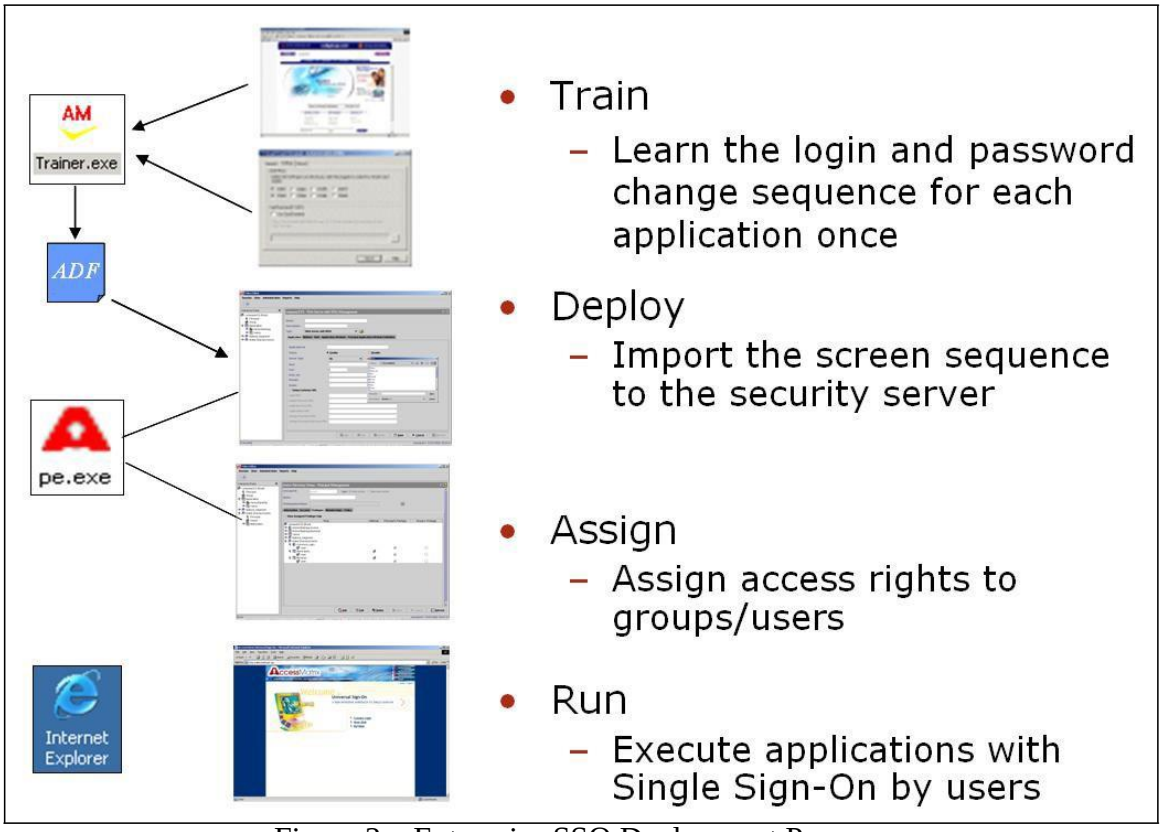

Figure 2 – Enterprise SSO Deployment Process

Typically, a typically application will be integrated with USO via the following process:

Process	Performed by	Activities	Output
Train Application for SSO and Change Password	Developer or System-Administrator	Use the USO Trainer Software to record the properties such as URL, Window Title, Field Names, etc for one or more screens for the login process and Password Change process. The screen properties information will be recorded in a Application Definition File (ADF) which is a XML file.	Application Definition File (ADF)
Deploy Applications for	Application Administrator	Use the Policy Editor/Admin Console to import the ADF file into the central repository	Application Definition
Assign Application	Security Administrator	Use the Policy Editor/Admin Console to assignment application	Application Entitlement

Access		entitlement to users or groups of users	
Run Application with SSO enabled features	End User	Use the USO WebAgent or USO Client software to login to the USO Server to retrieve the application entitlement information, the screen properties information and login credential (if available) for each application Use the USO Client to store the initial or the updated login credential information for each application Use the USO Client to replay the login information to the target application when the application screen can be recognized by the USO Client based on the screen properties information	Successful Login to target application using the SSO feature

2.4 Putting It Together

When a user logins successfully to the AccessMatrix USO server, a random session ID is generated for this login session. The session information is securely stored as cookie in the user browser's memory, which can identify the user and his/her login session. A user's login session ends when the user logs out, or force logout, or the session times out.

After a successful login, the user will be presented with a welcome page. The following sequence of events then happen simultaneously:

1) Check for USO Client Software Status
During the first time login, the USO client will be downloaded and configured automatically. For subsequent login, the download of the USO client will only occur when there is an upgrade of the software.

2) Download Target Application Information and Credential Information
The target application list, application attributes for identification and credential information are pushed from the server the USO clients. The communication between the USO client and the USO agent can be configured over SSL to ensure confidentiality and the downloaded information remains encrypted in the memory of the desktop environment.

3) Display a list of applications that the user is granted to access
The personalized target application list will be presented to the user to enable the user achieve SSO to the applications.

When the user launches an application that has been trained with the USO trainer software, the USO client software will locate the application's login page or screen. It will automatically fill in the required login ID and password, and then sign-on to the application on behalf of the user.

3. TECHNOLOGY ARCHITECTURE

AccessMatrix USO leverages on i-Sprint's patented **AccessMatrix™** technology (PCT/SG02/00027), Pluggable Authentication Module (PAM) and access control capabilities to enable our clients to enforce security policy and the flexibility to provide various authentication methods to meet the business and technical requirements.

Built on the open architecture, flexible framework and latest technology, AccessMatrix provides a common security infrastructure to offer complete enterprise security solution for various applications: web or non-web, new or existing, in-house developed or commercial package, with or without source code. AccessMatrix is the only security product family specifically designed to meet the security *administration, authentication, authorization* and *audit* requirements of banks and other security sensitive environments.

The USO product can be combined with our other complementary products - Universal Access Management and Universal Authentication Server Products, which provide a security framework to enable our clients to tightly integrate any web based and client/server applications to a centralized application security infrastructure and to support different authentication mechanisms. This will facilitate our clients to consolidate all the new and existing applications in to the same security infrastructure and provide a centralized user administration environment to reduce the administration cost and increase operation efficiency.

The benefits of leveraging AccessMatrix USO to our cliens in providing the SSO solution are as follows:

- This common security infrastructure will enable our clients to achieve single sign-on to applications for internal users without any source code changes.

- With our server based implementation approach, our clients can easily deploy the USO solution across their environment.

- USO provides a single and consolidated view of user privileges in the entire organization: how many applications a user can access.

- USO can ensure the compliance of application passwords to corporate security policy and enhance the authentication process.

- USO has a unique feature that allows administrators to set the policy to allow users to leverage the SSO feature either from any "authorized workstations" or restricting to specific workstations. No configuration change is required on the workstations.

- USO provides powerful administration services for security administrators to easily and effectively manage application entitlements and security policies throughout the entire organization. This unique technology enables highly scalable security and user administration to reduce on-going operational costs by delegating user administration tasks to departments within the organization.

3.1 Technology Components

The diagram below shows the technical architecture and key components of AccessMatrix USO.

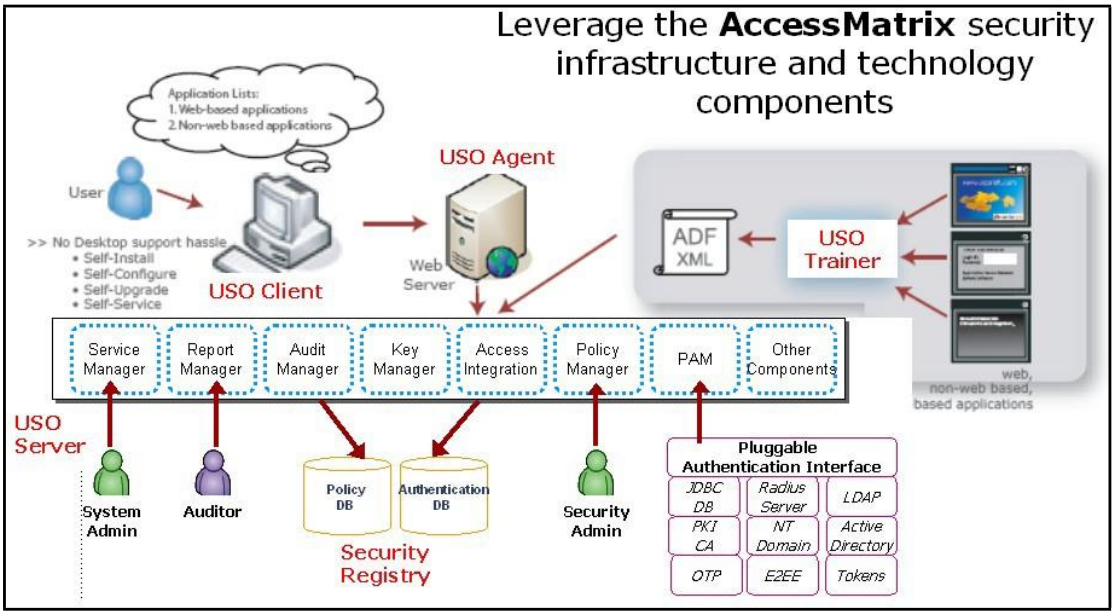

Figure 3 – Conceptual View of AccessMatrix USO

The AccessMatrix USO system consists of the following major components. All components can be installed into one physical server or in separate computer systems depending on the workload, fail-over and network configurations requirements.

3.1.1 Security Registry Components

The Security Registry is the core security database of AccessMatrix. The database can be a JDBC-compliant relational database e.g. DB2, Oracle, MS SQL Server.

Policy Registry contains the security policy, the principals' privileges and the application's access control permissions. This is the default security registry. The policy registry database is determined during installation stage.

Authentication Registry contains credential information about principals, such as passwords. This may be part of the default security registry, or an external registry such as the LDAP server or NT domain database. The authentication registry database is defined at each segment level.

There are two logical security registries, each with different content:

- Policy Registry
  Policy Registry contains the security policy, the principals' privileges and the application's access control permissions. This is the default security registry. The policy registry database is determined during installation stage.

- Authentication Registry
  Authentication Registry contains credential information about principals, such as passwords. This may be part of the default security registry, or an external registry such as the LDAP server or NT/AD domain database. The authentication registry database is defined at each segment level.

3.1.2 Security Server Components

- **Service Manager (SM)**
  The Service Manager is used by system administrators to configure, start and monitor the critical servers and components of the AccessMatrix Security System.

- **Audit Manager (AU)**
  The Audit Manager is the module to collect 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 only to collect selective events for auditing purposes.

- **Report Manager (RM)**
  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.

- **Key Manager (KM)**
  The Key Manager is a standard interface to integrate with Hardware Security Module (HSM) from major HSM providers such as SafeNet, nCipher etc to provide encryption key management and meet the higher security requirements for some organizations.

- **Access Manager (AM)**
  The AM server is the main security server of the AccessMatrix system. It manages the access control by providing the following security services:

  - **Authentication Services**
    It supports multiple authentication mechanisms, for example, static passwords, digital certificates, dynamic passwords, etc. for user authentication. The AccessMatrix authentication service is implemented according to the Pluggable Authentication Module (PAM) standard.

  - **Administration Services**
    The AM server also allows the security administrators to manage the security policy, principals, and applications of the entire organization. Granular administration rights can be assigned to the administrators to control the tasks they can perform via the admin interfaces.

- **Web Policy Editor/Admin Console**
  This is the 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.

  The AccessMatrix architecture is based on our patented segmented hierarchy model, which allows:
  - The segmented hierarchy allows an organization's structure to be defined within the security database
  - Security/user administrators are assigned at each level of the organization could be assigned the minimum privileges required for their job functions within a clearly defined scope.
  - Security policies governing authentication e.g. password rules, etc. could be defined at the root segment e.g. corporate headquarters propagated to all lower level segments. This allows easy enforcement of security policies in applications throughout the organization.
  - External authentication databases can be defined at each segment. This allows different users defined at different segments to authenticated using different authentication servers, e.g. Microsoft AD and iPlanet Directory Servers.
  - Other unique features include dual-control and separation of duties. Our solutions are built from the ground up not to require a super-user for all administration activities.

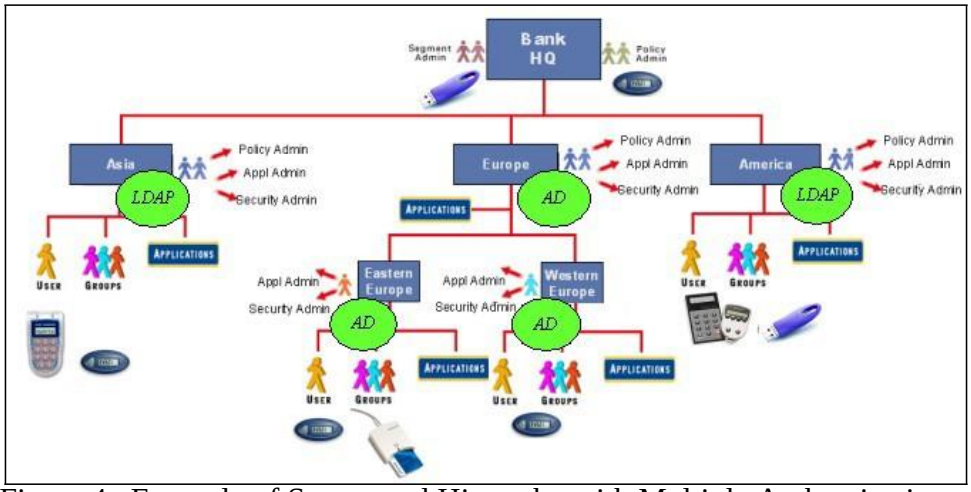

Figure 4– Example of Segmented Hierarchy with Multiple Authentication Registries and Multiple Authentication Mechanisms

3.1.3 Other Supporting Components

- **Services API Toolkit**
  The AccessMatrix USO Services API Toolkit is an add-on API sets to address the customization requirements and the comprehensive APIs set can be categorized into three categories:
  - **Application Security APIs**
    This is a set of APIs to provide common security services such as Single Sign-On, Authorization and User information retrieval, etc.
  - **Administration APIs**
    This is a set of APIs to provide administration functions to enable organization to tailor their unique user administration requirements and integration to provisioning software.
  - **Audit APIs**
    This is a set of APIs to provide a common audit function for applications to log audit events to a common audit log registry.
- **Import / Export Utilities**
  AccessMatrix provides a XML and CSV based standard UIX utility to import and export users, groups, group membership, application and entitlement information.
- **House Keeping Utilities**
  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.

- **Portal Server Integration Module**
  AccessMatrix USO integrates with leading Portal servers based on JSR 168 specifications. AccessMatrix USO can be easily integrated with portal environment in form of a portlet, which allows the users to access all types of application from the portal: web-based, client-server based, java-based, and host-based. At the same time, it complements the portal server to provide a common access point to applications without porting all applications to portlets. Currently, the following portal servers have been integrated and certified:
  - BEA WebLogic Portal Server
  - IBM Websphere Portal Server
  - SUN ONE Portal Server
  - Vignette Portal Server

3.1.4 USO Specific components

There are three USO specific components: USO Trainer, USO Client and USO Agent.

- **USO Trainer**
  - The trainer component is used to learn the login & password change sequence of each target application.
  - The trainer records the attributes about screen identification and field mappings so that the appropriate login information will be automatically passed to the application during run time.
  - The trainer also includes the default application level security policy for login behavior and password change.
  - The trainer provides a testing option to test the login and password change sequence captured by the trainer.
  - The trainer can export the information learnt by the trainer to an application definition file (ADF).
  - Administrators can then use PE to import the application information into the AccessMatrix security server. Administrators can change or set the application level security policy if necessary using PE.

- **USO Client**
  - The USO client component resides on the client desktop. It will communicate with the USO Agent to get the application login and the information.
  - The USO client monitors the desktop environment and examines program execution and screen flows. If it finds a match based on the pre-defined

information, it will pass on the login information to the screen input fields of the target applications.
- The USO client agent is installed automatically and no manual desktop installation is required.
- If required (optional feature), the USO client uses the 3DES key stored PTD (Personal Trust Device) such as SmartCard to decrypt the information stored in the PSE (Personal Secure Environment) such as login user id and password.

- **USO Agent**
  - The USO agent is one of the server component is resided on the web server. It serves as a gateway between the USO client agent and the AccessMatrix security server in the online SSO mode.
  - The USO agent maintains secure connections to the AccessMatrix security server via ASA.
  - Users primarily sign on to the AccessMatrix security server by accessing the USO login page.
  - The USO agent then retrieves the application list that the logged-in user is allowed to access and pass to the USO client.

3.2 Delegated Administration

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

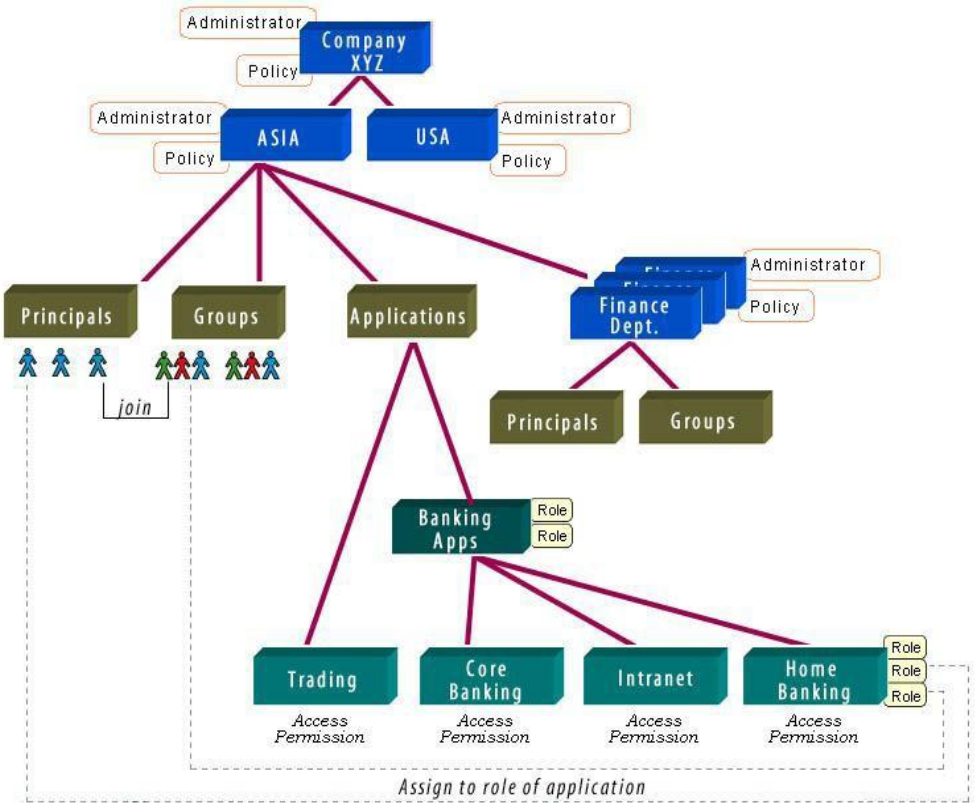

Figure 5 – AccessMatrix Hierarchy-Based Administration Model

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 segment 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.

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 at segment level.

3.3 Support for Multiple Authentication Methods

AccessMatrix implements the Pluggable Authentication Module framework to support for various different authentication mechanisms, e.g.: Static passwords, X.509 digital certificates, Dynamic or one-time passwords from RSA, Vasco, ActivCard, USB Tokens, etc.

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

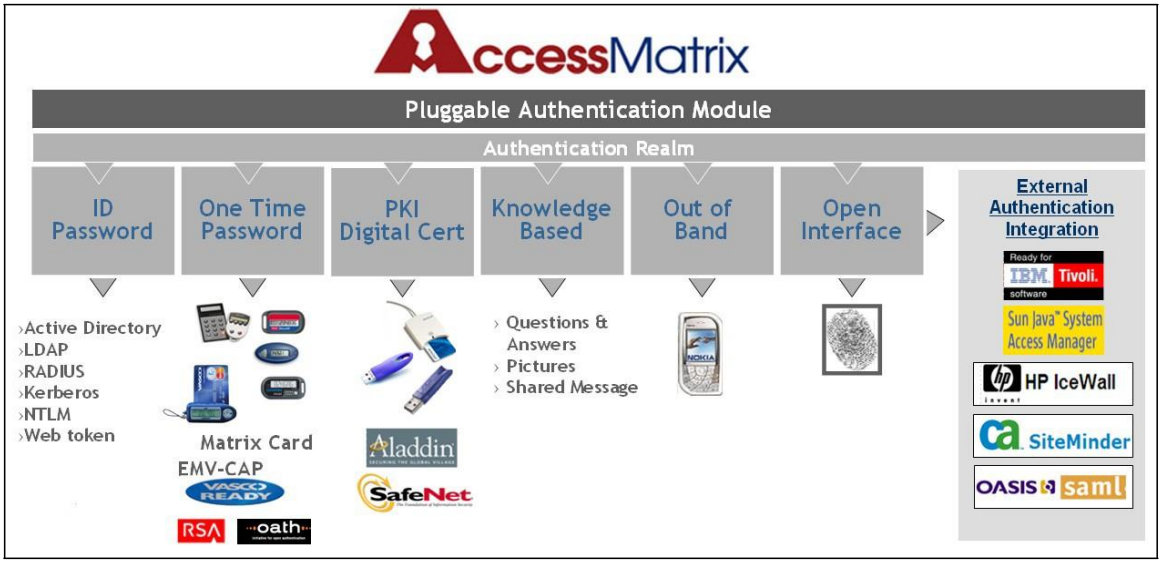

Figure 6 – AccessMatrix PAM Framework

AccessMatrix also provides standard PAM modules for leading Authentication server such as IBM Tivoli Access Manager, CA SiteMinder, and Sun Java Access Manager. This will enable AccessMatrix USO to integrate with existing authentication infrastructure, which will greatly reduce the deployment effort.

3.4 USO Unique Features

- **Secure Connections**
  All connections among components of the AccessMatrix security system are secured using standard SSL protocol, which provides PKI-based mutual

authentication, message confidentiality and integrity for all messages exchanged between AccessMatrix security components.

AccessMatrix is designed to allow the selection of various encryption strengths and cryptographic library. The default cryptographic library is the SUN's JCE.

- **Reliability, Availability and Scalability**
  Multiple USO servers can be installed to provide a HA configuration to ensure reliability, availability and scalability.
  - All AccessMatrix USO components have automatic fail over, retry features in case of fail over. The fail-over features do not require any additional hardware or software and are provided as out-of-the-box features.
  - AccessMatrix USO can be implemented using horizontal and/or vertical Scaling to address the fail over and scalability requirements by leveraging the platform agnostic feature.

- **Location Restriction**
  AccessMatrix USO has a unique feature that allows administrators to set the policy to allow users to leverage the SSO feature either from any "authorized workstations" or restricting to specific workstations based on IP Address. No configuration change is required on the workstations.

- **State-Aware Implementation**
  AccessMatrix USO has a unique technology to detect the various states during the login process so that it can handle very complex login process of the target application for single sign-on and provide a user a very seamless interface.

State	Definition
`NotRunning`	No application instances are running.
`BeforeLogin`	The application instance (indicated by process id) has been detected and not yet logged in. USO will fill in the login information when the logic screen is matched.
`AfterLogin`	USOClient has successfully filled in the login information to the application and login process succeeded.
`AfterLogout`	USOClient has detected that user has logged from the application
`Disabled`	The application has been disabled in USO Client.

This technology has overcome many challenges during the single sign-on process by knowing the target application status. This has enabled our USO solution to address unique sign on and screen navigation requirements.

- **Follow on Automation**
  AccessMatrix USO can provide follow-on automation for various application types like web, non-web, client /server, terminal emulator based applications, etc. The follow-on automation can be used for various scenarios like navigation of screens and menus, transaction automation, etc.

- **Concurrent Session Control and Session Idle Timeout**
  AccessMatrix USO enables organizations to concurrent session control and idle session timeout based on security policy on the server side. No configuration change is required on the workstations.

- **Desktop Screen Lock Activation**
  Screen Lock activation on the desktop can be enforced by the USO Server policy even if the user turns off the screen saver feature.

- **Single Sign Off**
  AccessMatrix USO supports single sign-off feature which can be applied only to selective applications based on security policy to support shared desktops and kiosk applications.

4. DEPLOYMENT OVERVIEW

4.1 Reliability, Availability and Scalability

4.1.1 Reliability and Availability

The AccessMatrix USO security architecture has support for high availability using automatic fail-over. Multiple instances of AccessMatrix USO security server can be deployed to support automatic fail-over.

Multiple USO servers can be installed to provide redundancy at each level. All the components have automatic fail-over; retry features in case of fail over. The fail-over features do not require any additional hardware or software and are provided as out-of-the-box features. It is recommended to use database's clustering features for HA.

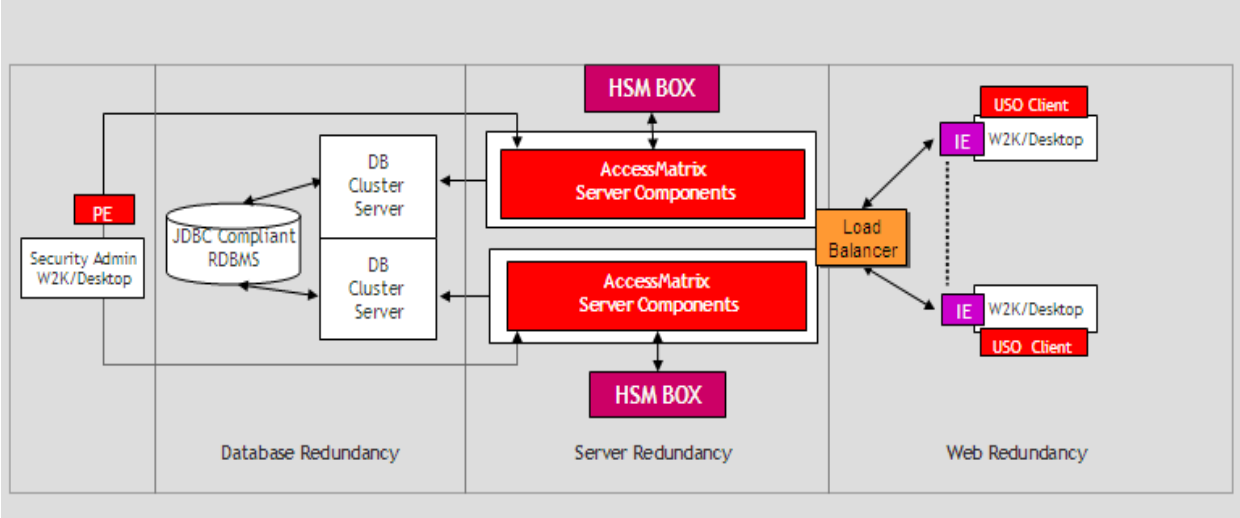

Figure 7 – Typical USO Deployment with external Load Balancer

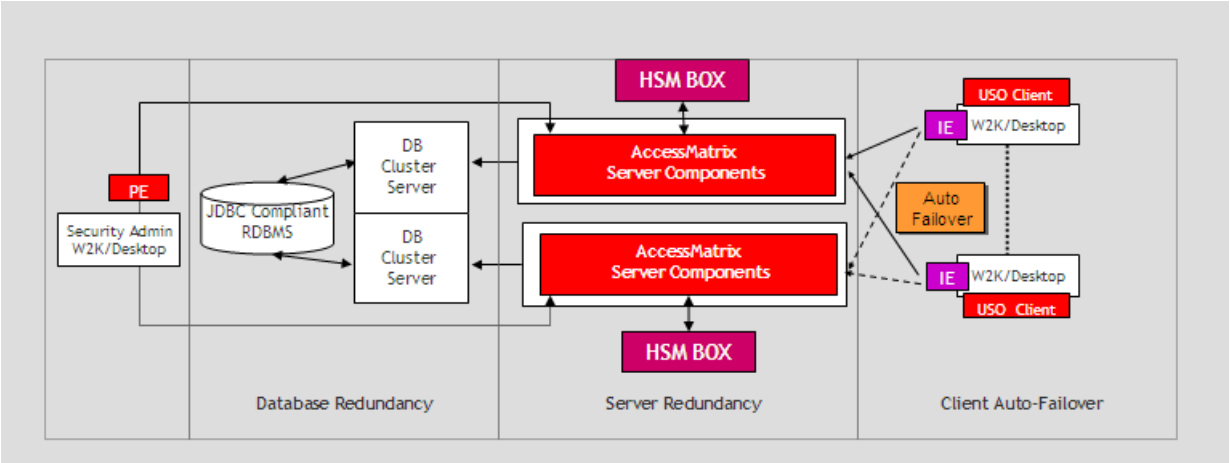

Figure 8 – Typical USO Deployment with USO Client Auto Failover features

The above diagram shows a sample USO deployment configuration. For example, USO Clients can point to AM USO Server1 as primary server and AM USO Server2 as secondary server. If AM USO Server1 goes down, the client will automatically fail-over to AM USO Server2. It will periodically check for the availability of AM USO Server1 and will automatically switch back to using AM USO Server1 once it is available.

If the database connection is down, AM1 AM USO Server1 and AM USO Server2 will automatically keep on retrying until connection is available.

The USO 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.

4.1.2 Scalability

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

For vertical scaling, USO 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 Windows 2003/2008.

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

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

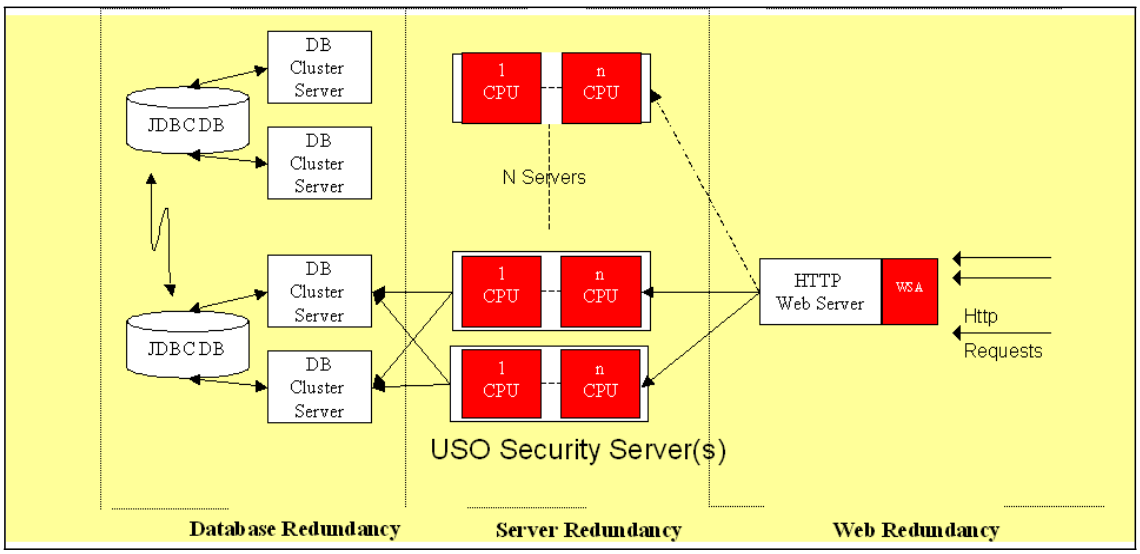

Figure 9 – Vertical and Horizontal Scaling for USO Deployment

4.2 Use of Hardware Security Module

The HSMs is a specialized tamper resistant hardware box protect the encryption keys and to perform the encryption and decryption of the users' application passwords in the USO implementation context. The USO server thus securely offloads all key management and cryptographic processing to the hardware security module.

Hardware security modules (HSMs) can be installed on every AccessMatrix USO security server to secure the encryption keys of passwords that are stored in the security database.

USO supports Hardware Security Module (HSM) from major HSM providers such as nCipher, SafeNet, etc to provide encryption key management and meet the higher security requirements for some organizations. The usage of HSM for USO is optional but it demonstrates the security design of the product.

For example, USO can leverage the HSM device to protect the user's encrypted application password information which is securely stored at USO Server database (Policy Database).

4.3 Design for Continuity of Business or Disaster Recovery

In the USO product design, there is strong emphasis to address the Continuity of Business or Disaster recovery requirements. In our implementation, there is no configuration change required on the desktop environment to switch to the backup/COB/DR servers even though there is a location or IP address change of the USO security server. This same rule will apply during "normalization" or "go home" after the main USO servers have been recovered. This unique design has greatly simplified the operation support during DR drills and actual unplanned prolong service disruptions.

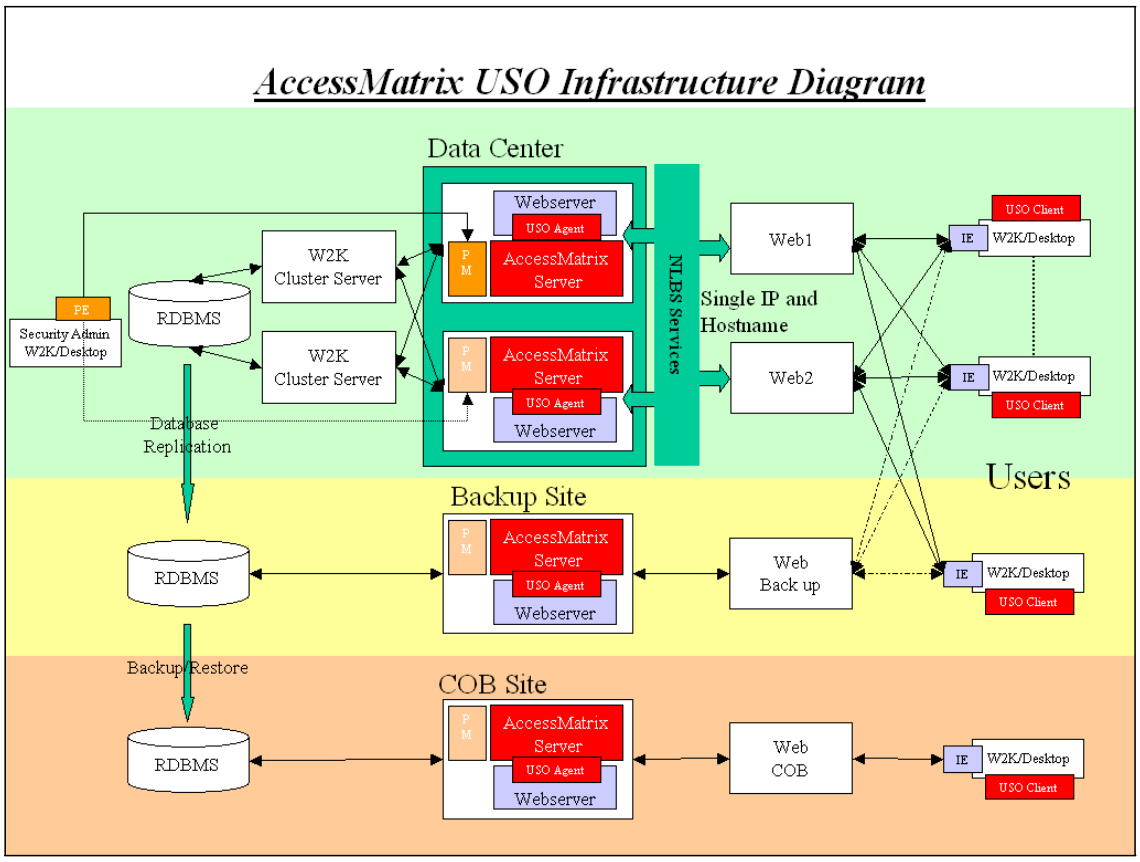

Figure 10 – Design for COB and DR Requirements

4.4 Daily Operation Considerations

4.4.1 User & System Administration

The AccessMatrix USO architecture is based on our patented segmented hierarchy model, which allows granular delegation of system and user administration tasks based on our clients' operating environment. 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. 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 for single sign-on
- **Security Admin**: Administrators who are responsible for maintaining user profiles and user's access rights for access SSO enabled applications

There are other roles can be defined in the USO system such as Auditors. These admin roles can be assigned at various organization hierarchies depending on where the administration tasks and span of control should be executed. For example, the "Security Admin" in the Asia region can only administer the user in Asia region while "Application admin" can only administer applications for the Asia region.

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

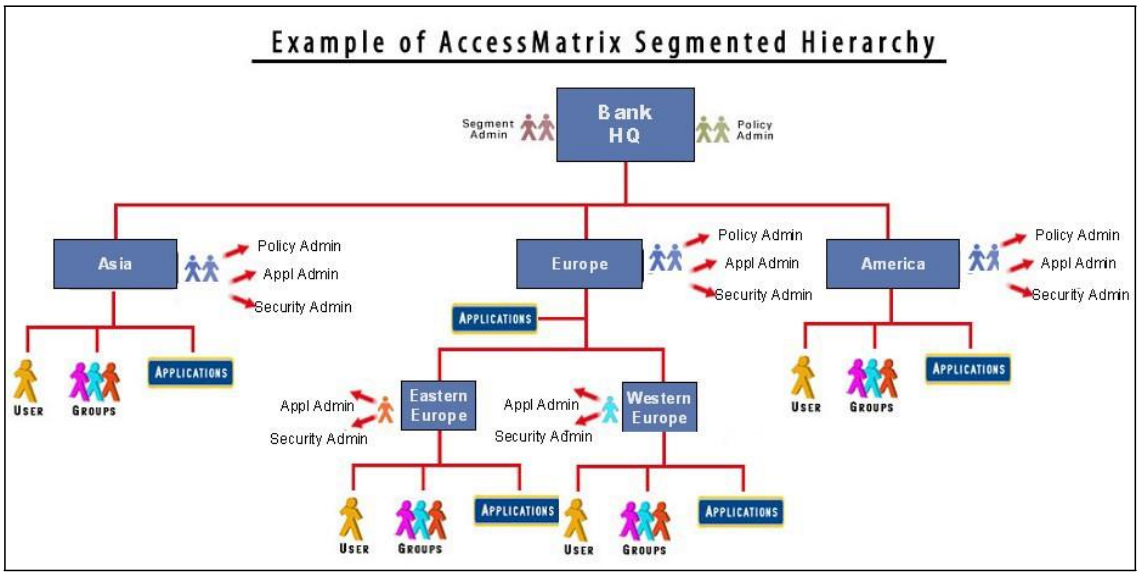

Figure 11 – Sample Segmented Hierarchy

If required, our clients can enable the dual-control features to enforce the maker / check process for critical administration tasks. This illustrates that the USO product is built from the ground up not to require a super-user for all administration activities.

4.4.2 Single View of User Entitlement

USO provides a single view of user entitlement of all applications for a given user. This is a very powerful feature to enable organizations to consolidate user entitlement information across in-country, regional and global applications. This will greatly simplify the task of tracking user entitlement information. This is another major benefit for deploying the USO solution.

4.4.3 Monitoring and Alerting Capabilities

USO provides extensive system log information to enable our clients to leverage their existing System Management tools such as IBM Tivoli, BMC Patrol, CA Unicenter, to monitor for critical error messages and alert the management console.

4.4.4 Data Import & Export

USO can synchronize user information from standard user registries such as Microsoft Active Directory, LDAP, databases or other electronic formats. This will address the requirements that most organizations have existing user information that resides in their existing user registries. Therefore, it will simplify the user creation process

At the same time, USO also provides a flexibility data migration tool to migrate data across multiple environments (DEV, SIT, UAT, PROD). This will greatly reduce the effort to perform user registration and administration process.

4.4.5 Operational Requirements

To address the house keeping requirements such as clean up of audit log information, unused account suspension etc, USO provides a House Keeping Utility which can be scheduled in a batch processing environment. These are designed to ensure no impact to online access.

For backup requirements, there is no specific operational requirement for the USO environment. The security registry (RDMBS) is the only key component which requires backup and recovery consideration. In terms of back and recovery strategy, it will follow the standard operating procedure in our clients' environment.

4.4.6 Multi-Language Support

The USO product has been UNICODE and double-byte enabled to support most Asian languages such as Japanese, Simplified Chinese, Traditional Chinese, etc for screen display, user input and data storage. New languages can be easily added using language templates.

4.5 Recommended System Configuration

Supported Server Operating Systems:

- AIX
- Sun Solaris
- Linux
- Windows 2003
- ZLinux

Supported RDBMS for Policy Store:

- DB2
- MS SQL Server
- Oracle

Supported WebAppServer:

- Weblogic
- Websphere / Express
- Sun One App Server
- Apache Tomcat

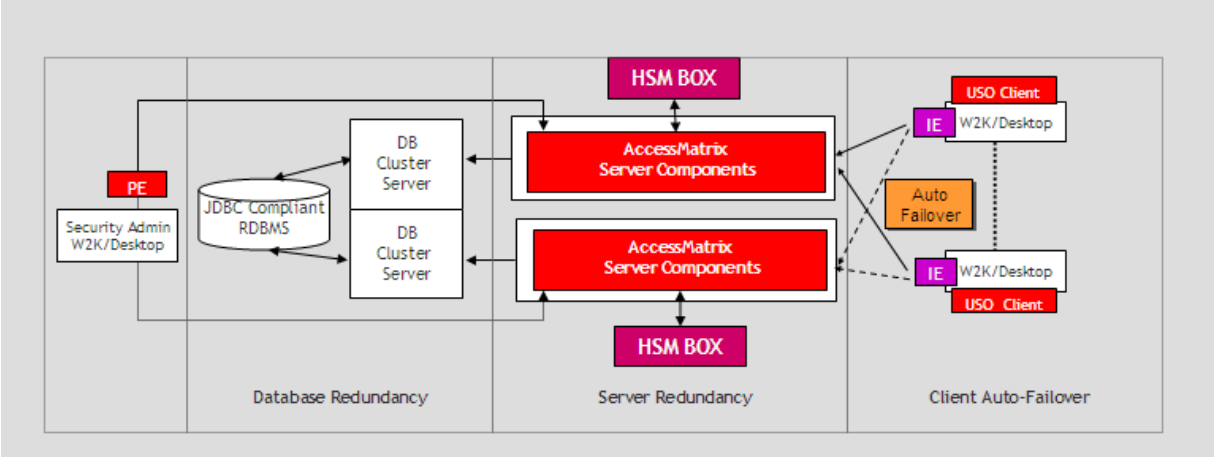

Figure 12 – Typical USO Deployment

Our Clients can select their preferred deployment platform to house the USO server environment.

5. SUMMARY OF KEY STAND ARD USO FEATURES

5.1 Architecture

Feature	Description & Benefits
Built-in Support for Best Security Practices and Principles	AccessMatrix is designed as an enterprise security system for mission-critical and security sensitive environments like banks and governments. AccessMatrix provides built-in support for best security practices and principles: least privilege, no super user, dual-control, and segregation of duties.
Integrated Complete Security Solutions	All AccessMatrix products are built on the same AccessMatrix security infrastructure, which provides complete integrated security services (administration, authentication, authorization and audit) for all enterprise applications (web or non-web, new or existing, with or without source code).
Platform Independence	AccessMatrix security infrastructure is built using Java technology and standards and therefore can be deployed in any platform that supports the Java Run-time Environment.
Secure Communication	All communication channels between AccessMatrix components are secured using standard SSL protocol.
Secure Key Management	AccessMatrix makes use of standard cryptographic functions. Cryptographic keys can be properly protected using HSMs.
Internationalization	AccessMatrix supports multiple languages: English, Chinese, Japanese, Malay, and Arabic.
Easy Deployment	AccessMatrix USO is designed to achieve SSO to multiple application types, which could be client-server based, java-based, web-based or host-based. AccessMatrix USO can be easily deployed without changing application source codes.
Easy Services	The client component of AccessMatrix USO can be self-installed, self-configured, and self-upgraded. AccessMatrix USO also provides self-service for users to initialize/reset their own application login information if allowed by the policy setting.
Easy Portal Integration	The organization's portal can be easily integrated with AccessMatrix USO, which allows the users to access all applications from the portal: web-based, client-server based, java-based, and host-based.

Shared Workstation and Kiosk Support	AccessMatrix USO provides support for shared workstations and kiosks using the Native Windows user switching.

5.2 Administration

Feature	Description & Benefits
Patented Segmented Hierarchy Model	In AccessMatrix, security policies, applications, users and administrators can be defined and managed based on i-Sprint's patented Segmented Hierarchy Model, which can easily represent an organization structure.
Policy Driven	In AccessMatrix, the corporate security policy can be enforced automatically top-down throughout the organization in real-time for all applications.
Granular Administration Rights	In AccessMatrix, granular administration rights are defined to control each aspect of the security administration functions, which can be assigned to different administrators defined at different segment based on the job functions.
Advanced Delegation	In AccessMatrix, various delegation options can be used to control the administration delegation: • Own + Delegate • Own + 1 Level Delegate only • Own only • Delegate only • 1 Level Delegate only
Scope Control	In AccessMatrix, assigned rights can be further controlled by scope, e.g. for a segment only or for an application only.
Dual Control	In AccessMatrix, administration-related change request submitted by one administrator (maker) must be approved by another administrator (checker).
Easy User Administration	In AccessMatrix, the user credentials, privileges and attributes of a large user population can be easily managed via GUI.
Flexible Group Management	In AccessMatrix, groups can be defined at different segment and be assigned to access normal applications or administration functions. Both users and administrators can be then assigned to different groups for easy management.
Multiple Registry	AccessMatrix security infrastructure can at the same time

Integration	be integrated with multiple external user registries e.g. Microsoft AD, LDAP and database.
Import & Export Utility	AccessMatrix provides XML based standard UIX utility to import and export user and application information.
House Keeping Utility	AccessMatrix provides standard House Keeping facility, which can be configured to cleanup/maintain tables.
USO Trainer	The USO Trainer can be used to learn the login and password change screens of application. The captured information can be exported to ADF file and then loaded into AccessMatrix security server.

5.3 Authentication

Feature	**Description & Benefits**
Pluggable Authentication Module (PAM)	AccessMatrix can authenticate users using different authentication mechanisms (PAMs): id/password, certificate, one-time password, etc. based on software, smart card, or token. Customized authentication methods can be easily integrated into AccessMatrix via PAM.
Concurrent Session Control	AccessMatrix can be configured to control concurrent login session: • Allow multiple login session • Don't allow multiple login session (reject the new login session) • Do not allow multiple login session (terminate the previous login session)
Session Control	AccessMatrix provides following methods to control login session: • User can logout from AccessMatrix • Administrator can force the user to logout immediately • Administrator can set maximum session lifecycle • Administrator can set idle session timeout
Re-authentication	Users could be required to re-authenticate by AccessMatrix using stronger authentication mechanism, based on the policy setting.
Authentication based on Time & Location Restriction	In AccessMatrix, administrator can specify when and/or from where a user can login.
State-Aware	AccessMatrix USO provides state tracking during the

	login process which in turns can intelligently handle complex login screen handling
Account State Control	AccessMatrix will verify account state during user authentication. The user account will be automatically Locked after the user failed to login for a pre-defined attempts. Administrator can manually Suspend a user account.
Password Policy Control	When authenticating to AccessMatrix, the user may be forced to change password if required by password policy. AccessMatrix will check the user's new password with the configured password policy.
Non-intrusive Single Sign-On	After successful login, AccessMatrix USO can help the user to automatically login to many USO enabled application without changing application source code.
Application password change	AccessMatrix USO can handle the application password change screens: • In Manual mode, prompt user for new password • In Auto mode, automatically generate a new random password
Self-service	AccessMatrix USO allows users to initialize and rest their application login information.
Screen Saver	AccessMatrix USO will force the user to set a password-protected screen saver for the user's workstation.
Follow-on Automation	The follow-on automation can be used for various scenarios like navigation of screens and menus, transaction automation, etc.
Offline Access	After successfully login to local PSE via PTD, AccessMatrix USO allows user to access the SSO functions in offline mode.
Multiple profile	AccessMatrix USO allows user to select different profile to access the same USO-enabled application.
Single Sign-Off	AccessMatrix USO can be configured to auto sign-off from an application when a USO session terminates

5.4 Audit

Feature	**Description & Benefits**
Security Audit Events	AccessMatrix logs the activities performed by normal users and administrators. The activities logged include actions such as login, change password, access to application & object, and security administration activities

	and also event result such as success and failure.
Audit Reports	AccessMatrix provides the following standard audit reports: • Audit report by user • Audit report by application • Audit report by segment (department) • Privilege report by user • Privilege report by application

Table 1 – Standard USO Features

6. CONCLUSION

The benefits of leveraging AccessMatrix in providing the SSO solution are as follows:

- This common security infrastructure will enable organizations to achieve single sign-on to applications for internal users without any source code changes.

- With our server based implementation approach, organizations can easily deploy the USO solution across their environment.

- USO provides a single and consolidated view of user privileges in the entire organization: how many applications a user can access.

- USO can ensure the compliance of application passwords to corporate security policy and enhance the authentication process.

- USO provides powerful administration services for security administrators to easily and effectively manage application entitlements and security policies throughout the entire organization. This unique technology enables highly scalable security and user administration to reduce on-going operational costs by delegating user administration tasks to departments within each organization.

The USO server based single sign on technology simplifies the deployment and implementation challenges for large enterprises. With USO technology, there is no manual software installation on each of the client desktop and application login information is stored centrally on the security server.

USO's unique architecture enables organizations to introduce Single Sign-on to their existing applications. The USO promises to deliver the solution that many organizations are looking for today – SSO without source code changes. Our server based SSO technology has greatly simplified the deployment and implementation efforts.

6.1 Transition to a Common Security Infrastructure

Other than providing the Enterprise SSO features with our Universal Sign-On (USO) product, i-Sprint's AccessMatrix suite of security products address the access control (4A's: Administration, Authentication, Authorization and Audit) market and security management.

With our many years of extensive experience in the banking industry and sound technical expertise in information security, i-Sprint provides an array of security products in

addressing the ever-increasing needs of consolidating security requirements in a holistic manner.

Built on the open architecture, flexible framework and latest technology, AccessMatrix provides a common security infrastructure to offer a complete enterprise security solution for various applications: web or non-web, new or existing, in-house developed or commercial package, with or without source code. AccessMatrix is the only security product family specifically designed to meet the security *administration, authentication, authorization* and *audit* requirements for global financial institutions and security sensitive environments.

i-Sprint's security solutions reflect the design philosophy that is gleaned from decades of real-life experience, in the implementation, review and audit, of world-class Bank-centric security systems. As such, the solution provides all the robustness and scalability of a centralized security infrastructure, while ensuring ease of use and mitigating technology obsolescence. Embedded in the solution, is complete and full auditability and accountability of all transactions. AccessMatrix™ enables multiple authenticating methods to co-exist therefore catering for user adaptation and change-management control.

The benefits of leveraging AccessMatrix Suite of Identity and Access Management solutions include:

1. Based on a common security infrastructure, our integrated security solutions facilitate the management of the user accessibilities of business applications and enable our clients to consolidate the authentication, authorization, administration, and audit services.

2. AccessMatrix provides powerful administration services for security administrators to easily and effectively manage application permissions, user privileges and security policies throughout the entire organization. This unique technology 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.

3. AccessMatrix provides a single and complete view about user privileges in the entire organization: how many applications a user can access and which role/roles are used to access which application.

4. AccessMatrix provides the application integration toolkit to enable fine-grained access control from application, to object, method and parameter levels. Authorization decisions are made based on application-specific roles that are assigned to internal and external users.

5. AccessMatrix will improve operational security by implementing security practices and principles that are not available in other security products e.g. separation of duties, least privileges and dual control. AccessMatrix has been built from the ground up to avoid the use of super-user.

6.2 Security Consolidation

With our AccessMatrix suites of Identity and Access Management solutions, we provide a common security infrastructure to enable organizations to adopt an incremental, evolutionary and strategic approach to address their application security requirements based on our Security Consolidation blueprint. Our proven "Security Consolidation" approach ensures organizations can maximize their return on investments in the short term and build up their security solutions based on a common framework to provide interoperability to cater for future business and integration requirements.

This "Security Consolidation" approach provides the flexibility for organizations to address their immediate identity and access management requirements while they are building a common security platform to cater for their future business and operations requirements.

Our suite of integrated security solutions help organizations address their security needs. Our current product offerings, AccessMatrix™ Universal Access Management (UAM), AccessMatrix™ Universal Sign-On (USO), AccessMatrix™ Universal Credential Manager (UCM) and AccessMatrix™ Universal Authentication Server (UAS), are engineered to meet the high standards of security sensitive environments.

With our proven security consolidation process, we enable our clients to leverage an incremental, evolutionary and strategic approach to address application security requirements based on a common security infrastructure.

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 Credential Management solutions for global financial institutions and high security sensitive environments. Our mission is to deliver a suite of bank-grade, integrated enterprise class Credential Management and Versatile Authentication solutions to address 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