



White Paper

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

7th Jul 2005

Abstract

With increased number of applications, corporate users are experiencing increasing difficulties in managing their authentication ids and passwords across a wide varieties of internal and external applications and platforms to support their day-to-day business activities.

This paper explains the Universal Sign-On technology how it can provide the non-intrusive to SSO (Single Sign-On) approach to help organizations address the challenges with increasing number of ids and passwords that are required by the users. This unique SSO approach can be achieve without any programming or source code changes for the target applications.

COPYRIGHT NOTICE

Copyright © (2000-2005) by i-Sprint Innovations Pte Ltd All rights reserved.



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

CONTENTS	3
1. INTRODUCTION	4
2. PASSWORD CHALLENGES	5
3. UNIVERSAL SIGN-ON (USO)	6
3.1 How USO WORKS	6
3.2 ACCESSMATRIX SECURITY INFRASTRUCTURE.....	7
3.3 ACCESSMATRIX USO COMPONENTS	7
3.3.1 <i>Trainer</i>	7
3.3.2 <i>USO Client</i>	8
3.3.3 <i>USO Agent</i>	8
4. STATE-AWARE TECHNOLOGY	9
5. FLEXIBLE ADMINISTRATION	10
6. SUPPORT MULTIPLE AUTHENTICATION METHODS	11
7. USO WORKING MODES	12
7.1 ONLINE VS. OFFLINE.....	12
7.2 AUTO VS. MANUAL.....	12
8. SECURE STORAGE IN USO	14
9. SUMMARY OF FEATURES	16
10. CONCLUSION	18
CONTACT INFORMATION	19

FIGURES

FIGURE 1 – ACCESSMATRIX USO SIGN-ON MODEL	6
FIGURE 3 – ACCESSMATRIX HIERARCHY-BASED ADMINISTRATION MODEL.....	10
FIGURE 4 – ACCESSMATRIX PAM FRAMEWORK SUPPORTS MULTIPLE AUTHENTICATION METHODS.....	11

TABLES

TABLE 1 – ACCESSMATRIX COMPONENTS.....	7
--	---

1. INTRODUCTION

As organizations are developing more and more information systems to automate the business processes, users find themselves struggling against the surge in the number of ids and passwords in order for them to have access to the various applications. This is due the requirement that every new system requires a new login. Each user must have a unique identity, a user ID or username, on that system. And he or she must also provide a password that allows the system to verify the claimed identity—that is, to authenticate the user. In addition, each system demands its own authentication because it needs to verify the identity of the user, but simply does not trust any previous authentication.

With increased number of applications, corporate users are experiencing increasing difficulties in managing their authentication across a wide variety of internal and external applications and platforms to support their day-to-day business activities.

Often organizations do not have access to the source code so that they can modify the applications to achieve the single sign-on objective. On the other hand, even though they have the source code but the potential risk of modifying a working mission critical application may cause any necessary service disruptions. Therefore, organizations are searching for cost effective and safe approach to achieve single sign-on.

We will describe in details of the AccessMatrix Universal Sign-On (USO) product and explain how it can enable organizations in managing their applications, to achieve Single Sign-On (SSO) without any source code changes and meet the changing security requirements.

2. PASSWORD CHALLENGES

Although organizations worldwide are moving their applications to the standard web platform today, a large number of legacy applications e.g. client/server, host, thin client based application continue to exist inside the organization. These age-old applications are often implemented in a distributed environment with proprietary application-specific security module. Many of them use static ID and password to authenticate the users, implement different security policy and user management modules. Over time, organizations face tremendous challenge in managing these applications to meet changing security requirements and user's expectations such as conformance to enterprise password policy and request for Single sign-on (SSO).

AccessMatrix is a new generation of enterprise security administration, access control and Single Sign-On system with a design focus on mission critical application environment such as those in the financial sector. Unlike other SSO product, which only supports web-based applications, AccessMatrix is designed to meet the SSO challenge of both web and client/server applications.

By leveraging the robust, flexible and scalability of the AccessMatrix security server and the API tight integration approach, the USO loose integration approach provides a complementary and comprehensive application security solution to meet the access control challenges of most organizations.

USO was developed using the robust components of on AccessMatrix infrastructure supporting 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 without any source code modifications to address the SSO requirements.

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 server based solution has eliminated the need for manual software installation on client workstations and minimize 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. USO provides a self-service facility to enable users themselves to manage their IDs and Passwords, which greatly simplifies the implementation efforts.

3. UNIVERSAL SIGN-ON (USO)

Universal Sign-On (USO) is a non-intrusive Enterprise Single Sign-On (SSO) solution.

3.1 How USO Works

By leveraging on the AccessMatrix security server as the single sign-on server, the user benefits from additional security services like administration, audit and application level authorization. USO's facilities for auto-installation, auto-configuration and self service, greatly simplify deployment and reduce maintenance effort. The central security server stores the users' security related properties for each application.

The USO Client software is automatically downloaded to the user's desktop when the user logs in for the first time. The USO Client software monitors the user's desktop to detect a login screen match and automatically logs in to the target application on behalf of the user.

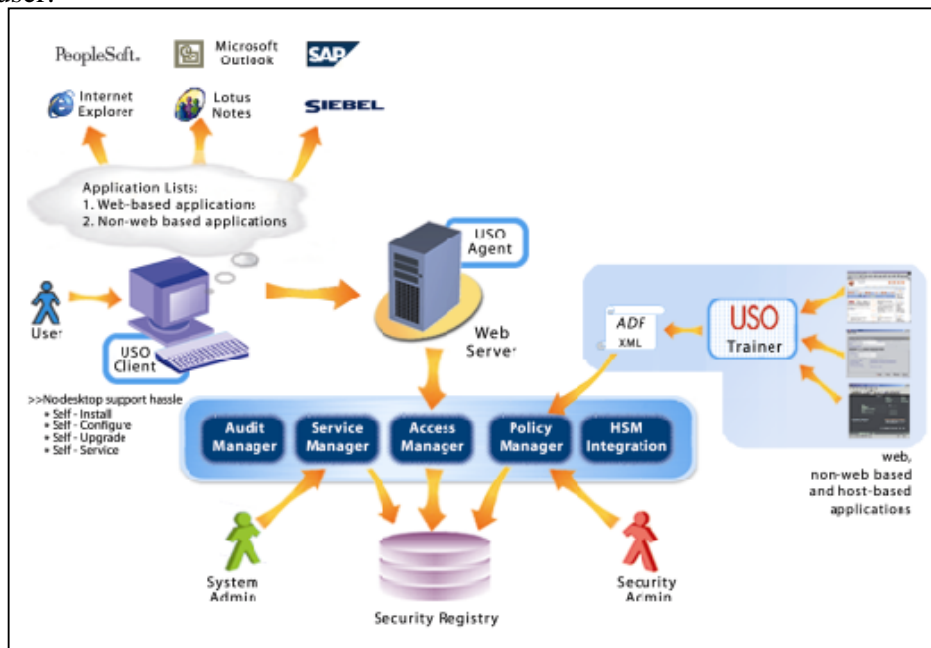


Figure 1 – AccessMatrix USO Sign-On Model

The figure above shows a top-level view of AccessMatrix Universal Sign-On model. The model illustrates a combination of primary and secondary sign-on operations.

3.2 AccessMatrix Security Infrastructure

The USO leverages the AccessMatrix security infrastructure for administration, authentication, authorization and audit services.

The following minimum AccessMatrix components are required to support the USO operation:

AccessMatrix Components	Functions
Policy Editor (PE)	<ul style="list-style-type: none"> • Policy management • Application Management • User Management
Access Manager (AM) and Application Security Agent (ASA)	<ul style="list-style-type: none"> • Used for primary sign-on and retrieve target application information for secondary sign-on.
Service Manager (SM)	<ul style="list-style-type: none"> • Used to configure and start/stop AM and PM

Table 1 – AccessMatrix Components

3.3 AccessMatrix USO Components

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

3.3.1 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.

3.3.2 USO Client

- The USO client component is resided 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 in 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.
- The USO client agent 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.

3.3.3 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 retrieve the application list that the logged-in user is allowed to access and pass to the USO client.

4. STATE-AWARE TECHNOLOGY

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 to solution can address unique sign on and screen navigation requirements.

5. FLEXIBLE ADMINISTRATION

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

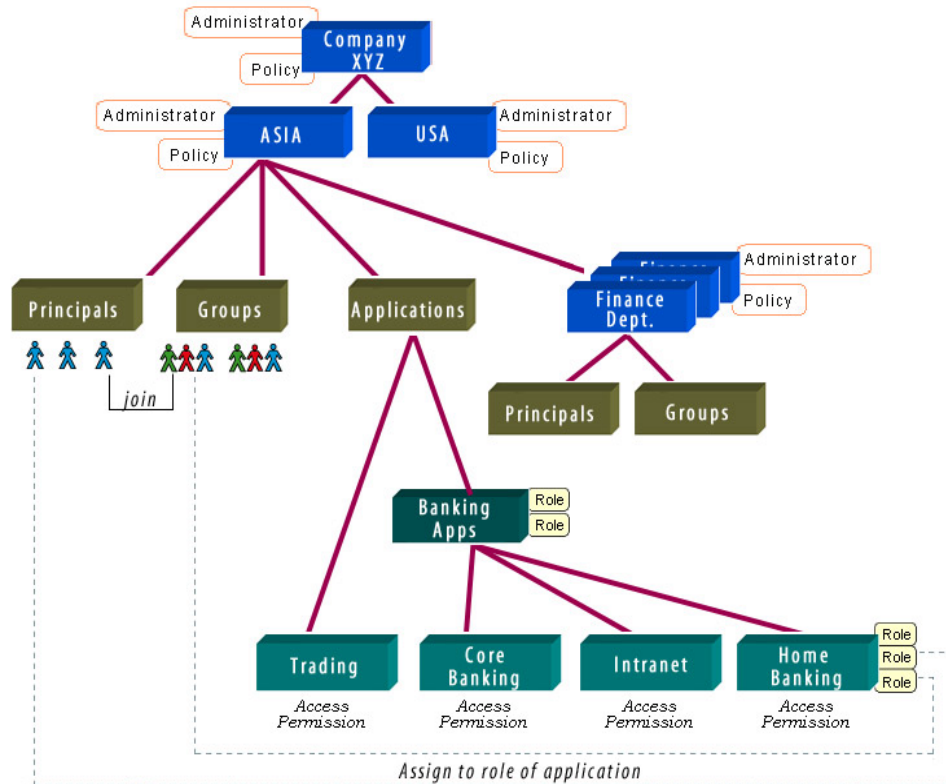


Figure 2 – AccessMatrix Hierarchy-Based Administration Model

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.

Security administrators can be created at segment level to manage security within their respective segments and sub-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.

6. SUPPORT MULTIPLE AUTHENTICATION METHODS

The users must be authenticated to AccessMatrix USO before the SSO feature is granted to access the target applications. AccessMatrix implements the standard PAM (Pluggable Authentication Method) framework to support various authentication mechanisms:

1. Static passwords (e.g. default, Microsoft Active Directory, LDAP, etc.)
2. Dynamic passwords (e.g. RSA Secure ID, ActivCard Token, iKey, USO Token, etc.)
3. X.509 digital certificates
4. Other authentication schemes (e.g. biometric devices)

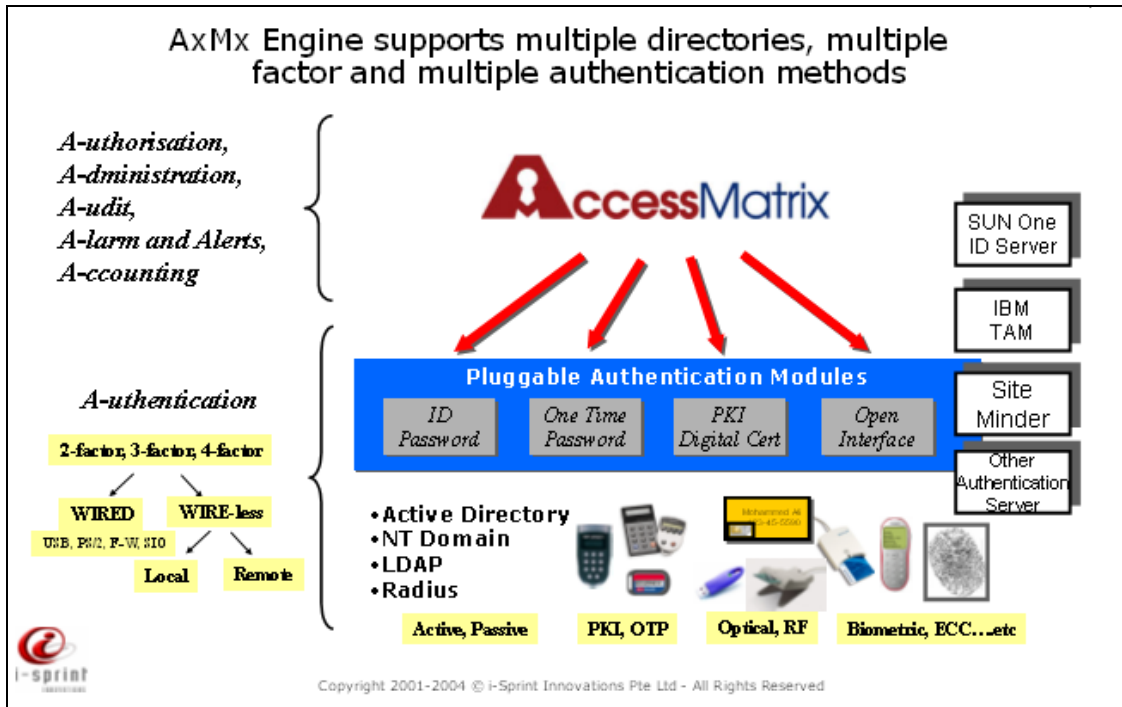


Figure 3 – AccessMatrix PAM Framework Supports Multiple Authentication Methods

With the PAM framework, AccessMatrix supports 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.

7. USO WORKING MODES

7.1 Online vs. Offline

There is two modes for USO to perform: Online and Offline. The default and normal USO working mode is Online, which means that users have to perform primary sign-on to the AccessMatrix security server via the USO Agent. The application information will be downloaded to the user's USO Client for secondary sign-on to the target applications.

The USO also provides Offline mode to certain users and certain applications. In this case, users don't have to login to AccessMatrix security server; instead, they login to the USO Client. The USO Client verify the user credential with the local PSE and PTD, then make use of the application information stored in the local PSE for secondary sign-on to the target applications.

A new application attribute "Offline Accessible" is defined on each USO application. It is controlled by the central security server.

A new principal attribute "Offline Capable" is defined to specify whether the interactive principal is offline capable. A copy of the application information will be stored in the user's PSE only if the application is Offline Accessible and the user is Offline Capable.

Note that applications marked as Offline Accessible can also be accessed in Online mode. In this case, the application information stored in the security server will be compared with the information stored in the PSE and sync each other if necessary. In fact, this is way how the offline accessible application information is initially stored in local PSE and gets updated/synchronized.

7.2 Auto vs. Manual

There are two Login Submit modes for USO to control the application login process: Auto and Manual. In Auto mode, the USO will automatically login to the target application without prompting the user. In Manual mode, the USO will fill up the information but wait for the user to confirm.

The Login Submit mode is controlled by USO Client. It can be defined as General Setting or as application level Login Submit control option, which will override the General Setting.

There are two Password Change Submit modes for USO to control the application password change process: Auto and Manual. During password change in Auto

mode, the USO will automatically generate a random password and fill up the new password field without prompting the user. In Manual mode, the USO will wait for the user to type in the new password.

The Password Change Submit mode is defined at application level and controlled by the central security server.

Note that the SSO mode Password Change Submit mode are controlled by the central security server, which means the security officers can change (of course with proper control of PE) the setting that is come from the ADF file.

8. SECURE STORAGE IN USO

In order to support offline SSO and secure SSO environment, USO client can securely keep application information at the OPTIONAL local PSE (Personal Security Environment) file that is protected by a smart card as follows:

- * The user's application password is encrypted using a 3DES key before store in the PSE file.
- * The integrity of the PSE is protected using the 3DES key:
 - o There is mac field in the file
 - o mac = hash(file context except the mac field + the key)
- * The 3DES key is stored in the smart card.
 - o The key is randomly generated during the PSE creation
 - o The key is protected by the smart card such that it can be read from smart card only after smart card authentication.
 - o If the smart card itself supports key generation feature, the USO client will call the smart card API to generate a 3DES key.
- * When a user click an application, the USO client will
 - o The USO client tries to read the key from the smart card. The user will be prompted for pin again if the smart card is removed before.
 - o The USO client reads the encrypted application password from the PSE file.
 - o The USO client decrypts the password and login to the application on behalf of the user.
 - o The USO client immediately removes the 3DES key and the application password from the memory.

Notes:

- * The user's SSO password and the 3DES key are NOT stored in the PSE file.
- * The user's SSO password, the 3DES key and applications passwords are not cached in memory. They are removed immediately after use.
- * The user's application password is stored in the PSE file only if the user is "Offline Enabled" and the application is "Offline Accessible".
- * The user attribute "Offline Enabled" and application attribute "Offline Accessible" are defined and controlled at USO security server side, and can not changed at the user side.
- * At USO security server side, the user's application passwords are encrypted using another random 3DES key, which again could be protected by a HSM (Hardware Security Module).
- * During transmission, the user application passwords are sent over the SSL secured channel.

- * The user application passwords are always encrypted during transmission, at the USO server's database, at the USO client's memory or at the USO client's PSE file.

9. SUMMARY OF FEATURES

The unique features of USO are as follow:

- **No manual software installation on Desktop** – Quick deployment with no disruption to client desktop.
- **No source code changes in Applications Desktop** – Non-Intrusive approach to enable single sign-on to multiple applications without source code change.
- **Integration with Web Portal** – USO provides a web interface to enable users to launch applications from a single point of entry and it can be easily integrated with all leading major portal servers and application servers.
- **STATE-aware Technology** – USO has a unique technology and detect the various states during the login process so that it can handle very complex login process and provide a user a very seamless interface.
- **Application Trainer program** - Can generate the ADF (application definition file) which is a XML based file for simplify the application setup and configurations for USO.
- **Self Service** - Administrators can initiate the self-service feature to enable users to supply their UIDs or PWD for the target applications when they first login.
- **Auto password change** - If you do not want the users to know the password to login to the target applications, the "AUTO" feature will generate the new password automatically during the password change process.
- **Manual password change** - If users require knowing the password of the secondary login, the "Manual" feature will prompt users for the new password during the password change process.
- **Reset password** - This feature allows users to reset the password for the login of target applications in case the password in USO registry is out of sync with the target application.
- **Password Policy for Target application** - The USO client can generate password for a target application based on the password policy rule defined for each application. This will greatly automate the password change process when the AUTO password change policy is enabled.

- **Job Role based Login** - USO supports multiple login profiles per user per application. This eliminates the need for a user to remember different user id and password for different job roles for the same applications.
- **Offline Mode** - USO supports single sign-on without LAN connection to the USO server. This is extremely useful to support executives who needs to travel and enjoy the single sign-on convenience. This offline mode can also be used as a redundancy feature in case of the USO server cannot be reached due to network, hardware or software problems.
- **Version Control** - The USO agent will be updated/downloaded to the client workstation automatically if there is new version of the software available

10. 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.



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 or contact us at any of the following offices:

About i-Sprint

i-Sprint Innovations specializes in Identity and Access Management solutions for global financial institutions and high security sensitive environments. Our mission is to deliver a suite of bank-grade, integrated enterprise class application security solutions. i-Sprint's own unique brand of security products, intellectual properties and patents are designed to exceed global financial services regulatory requirements. We help organizations of all sizes across the world to securely and cost-effectively, Authenticate, Authorize, Administer and Audit, access to their information assets. Our Client list includes leading global and regional financial institutions, MNCs and government agencies.

©2002-5 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.