CASE STUDY

THE MOST PROFITABLE BANK IN SINGAPORE

i-Sprint's AccessMatrix™ Universial Authentication Server (UAS): End to End Encryption - Login Protection for Corporate Internet Banking Services

ORGANIZATION PROFILE

- Business Category: Banking & Finance
- Total Assets: S$218 billion (2011 Jun)
- Size: 15,000 persons (2011 Feb)
- Number of Seats: 500,000
- Others: The 'strongest' and most profitable bank in ASEAN

THE BUSINESS ISSUE

The Bank needed a web-based Internet Banking channel to replace their legacy client-server system. It must comply or exceed security guidelines outlined by the Monetary Authority of Singapore (MAS).
The solution should provide for:

1. End-to-end protection of customer PIN.

i.e.: Customer PIN must be protected throughout the process of creation, assignment, printing and delivery.

This is in compliance with the Monetary Authority of Singapore Internet Banking Technology Risk Management Guidelines, Version 3.0, June 2008Guideline

> "…. the encryption security pertaining to the customer's PIN and other sensitive data should be maintained end-to-end where possible. This means the encryption process is kept intact from the point of data entry to the final system destination where decryption and/or authentication takes place."

SOLUTION

AccessMatrix™ UAS future proof universal authentication server

AccessMatrix™ UAM common security platform for enterprise applications

- i-Sprint's security consolidation methodology was applied throughout the project to assist the bank to implement and deploy our AccessMatrix™ Universal Access Management (UAM) and AccessMatrix™ Universal Authentication Server (UAS) as the standard access control and single sign-on platform for the bank to achieve:
  - Single Sign-On to all Internet banking services and applications. Fine grain access control to ensure proper access authorization based on business rules and access privilege
  - Flexible user administration model to enable corporate customers to make their user profiles and access privilege
  - Integration of security tokens to enable strong user authentication and transaction authorization
  - Enforcement the compliance of information security policy for all e-banking applications
  - Reduction of application development and maintenance efforts by leveraging a common security infrastructure

- Platform for UAM and UAS
  - Sun Solaris Servers (E250 – 2CPUs X 2)
  - Oracle RDBMS

HOW DOES IT WORK?

- AccessMatrix™ Universal Access Management (UAM) allowed the Bank to achieve:
  - Tightly integrated Single Sign-On for **Users**
  - Single Point of Administration for security **Administrators**
  - Application log consolidation platform for **Auditors**
  - Application security integration platform for **Developers**

- UAM provides a common application security infrastructure that;
  - Improves application usability and user experience by providing the **Single Sign-On** feature
  - Enforces security policy with best practices
  - Improves Productivity by avoiding unnecessary code development
  - Implements E2E encryption to meet the security requirements of the Central Bank
  - Reduces Cost in security administration and application audit log management

OTHER

This Bank chose AccessMatrix Universal Access Management (UAM) and AccessMatrix Universal Authentication Server (UAS) solution to be their core security infrastructure technology to support all business critical e-banking applications. Other than leveraging the single sign-on features of AccessMatix , the Bank took full advantage of the technology's hierarchical administration model to decentralize user administration, thereby enabling their key corporate customers to administer their own user id and access privileges. The bank had also derived other functional benefits e.g. the fine-grained access control and interface to their PIN mailing system. They have also scaled the SSO features of AccessMatrix to include existing e-Treasury and the e-Futures applications. In addition, they creatively extended the AccessMatrix server to securely manage their database passwords thereby allowing existing applications to securely sign-on to the target databases. The first application went live in April 22, 2002.

To comply with Monetary Authority of Singapore regulations, E2E encryption had also been easily introduced and implemented with HSM technologies.

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.*

©2000-15 i-Sprint Innovations Pte Ltd. All rights reserved.
A Hierarchy Model is a patent of i-Sprint Innovations Pte Ltd. i-Sprint, i-Sprint logo, AccessMatrix and AccessMatrix logo are registered trademarks of i-Sprint Innovations Pte Ltd. All other trademarks and registered trademarks are 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.