CASE STUDY

LEADING EUROPEAN PRIVATE BANK

i-Sprint's AccessMatrix™ Universial Authentication Server (UAS): E2E Encryption Authentication for Internet Banking Portal for Private Banking Clients

ORGANIZATION PROFILE

- Business Category: Banking & Finance
- Total Assets: over 860 billion euros in total assets.
- Size: 100,000 persons (2006 Feb) and active in more than 15 countries
- Others: The Top Ten Financial Institutions in Europe

THE BUSINESS ISSUE

The Bank needed a stronger web-based Internet Banking channel to serve its private banking clients in the Asia Pacific region. It must now comply or exceed security guidelines outlined by all the central banks in the Asia Pacific region including the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA) that calls for Banks to "afford sufficient protection of encryption keys and confidential data in an end-to-end authentication operation." (MAS-IB-TRM June 2003) Current technologies (e.g: SSL) do not provide the privacy and protection against today's sophisticated attacks from 'within' and 'without' the Bank.
Functional Requirement:

1. End-to-End Encryption Authentication Process
   i.e.: Customer PIN must be encrypted on the user's web browser and the encrypted information is transmitted over SSL to the backend server. The encrypted PIN and compared against the stored encrypted PIN inside a hardware security module (HSM). No component, such as application, web server, Security server, database, is able to recover the user's password in clear in this mechanism

2. Flexible User Administration solution with granular administration and delegation
   i.e.: From the security and user administration perspective, the bank unit in each country must be able to administer their own clients only. Because of the privacy issue, the RMs can only access the information of their own set of clients in their country of assignment.

3. End-to-End protection of customer PIN.
   i.e.: Customer PIN must be protected throughout the process of user creation, PIN assignment, PIN printing, PIN Change and PIN delivery. No internal staff can claim to have access or exposure to such private Client information. The Bank must be able to prove themselves harmless when challenged on such issues.

SOLUTION

- i-Sprint deployed our AccessMatrix Universal Authentication Server(UAS) E2E Encryption Module as the standard authentication platform for the bank to achieve the business needs.

- AccessMatrix E2EE creates a secured channel between the Customer's PC and Hardware Security Module (HSM). Within this channel, the Password is encrypted at the Customer's PC and the authentication process is managed by the AccessMatrix Security Server. The password can only be decrypted for verification by the HSM located in a physically secure location within the Bank. In so doing, the Password and other sensitive data can never be exposed, not even to the organization's internal applications and servers. The AccessMatrix Security Server and HSM work as an integrated solution to provide certified tamper-resistant vault, specifically designed for this sole purpose.

- The granular administration delegation in the AccessMatrix system is designed to address complex administration requirements of global Banks. There are various delegation control options:
  - **Delegate Only** – Administrator can only delegate but does not own the privilege
  - **Own and Delegate** – Administrator owns the privilege and able to delegate.
  - **Own only** – Administrator owns the privilege but cannot delegate it.

- 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 in the process before a sensitive administration task can be completed. Dual control can be configured to be turned 'on' or 'off' at different levels of the segment hierarchy.

- Platforms:
  - WinTel with Microsoft Software Server 2003
  - Microsoft SQL Server 2003
  - Safenet Protect Host White HSM with Online Banking Module

HOW DOES IT WORK?

How does E2EE Password Protection work?

- When User accesses the login page of a service provider e.g. Internet Banking service of a bank, an applet will be downloaded to the client's browser together with a public key to encrypt the login and other sensitive information.
- After the user keys in the User ID and PIN information, the applet will encrypt the information using the public key and submit to the server for processing.
- Once the encrypted information reaches the server, the server will pass the encrypted information received from the User and the corresponding encrypted PIN from the security server's database to the HSM for PIN verification. Decryption and PIN comparison will only take place inside the secure tamper-protected environment of the HSM device. As such, credential information remains totally encrypted throughout the system immediately after user input.
- Once verified and if the response from the HSM is positive, only then will the

User will be successfully authenticated to the system and the User can then proceed to perform the functions that have been assigned.

BUSINESS IMPACT

1. Complies with local Regulatory mandate, solutioned in 'time' and within 'budget'.
2. Promotes confidence and integrity of access for its high net-worth Clients
3. Lay the framework of Trust for a robust technology risk management process that should deal with all known attacks and provides a platform for a rapid response to future exploits.
4. Provide the flexibility of allowing the Bank and its Clients, to select a convenient and yet secure Authentication risk-based approach of accessing the Banking products.
5. Permits cross business unit usage of Authentication devices that reduces complexity of use for its Clients and reduces the cost of managing such devices, Bank-wide.

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.*