

AccessMatrix™ Universal Authentication Server (UAS) enables organizations to deploy a wide variety of authentication methods to address the business requirements for strong authentication and evolving authentication mechanisms, through a single, unified framework.

End to End Encryption (E2EE) for Credential Protection

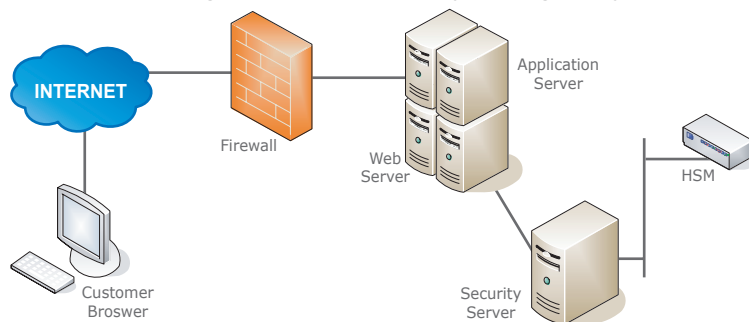
AccessMatrix™ UAS E2EE addresses the potential security exposures of Internet/Web based applications which can be exploited by attackers to eavesdrop secure sessions or spoof the web servers for sensitive data once it is “clear texted” by the SSL decryption process. AccessMatrix™ E2EE provides an integrated solution with software and tamper resistant hardware security modules (HSM) to effectively protect against such credential theft. This proven end-to-end security is designed to protect sensitive information such as credit card numbers, user PINs or password entered from a client’s web browser. As a result, it enables organizations to encrypt sensitive information from the point of entry to point of comparison.

"The MA however expects that sensitive data should also be encrypted while they are transmitted between the web servers and FI's internal systems. In particular, FIs should consider the need to apply strong "end-to-end" encryption to the transmission of highly sensitive data (e.g., customer passwords) so that the data are encrypted all the way between customers' devices and institution's internal systems for processing the data. This would help to ensure that such highly sensitive data would not be compromised even if FI's web servers or internal networks were to be penetrated" HK Monetary Authorities

The Business and Technology Challenges for Internet Based Applications

As organizations look to conducting more and more business on-line, the need for security increases. The Internet in particular, offers major opportunities for organizations to reach new markets with expanded range of products and services. The very accessibility and dynamism of the Internet brings both benefits and risks.

In moving to a Web presence, there is a sense of loss of security, as compared with the physical world. The challenge of providing secure remote transactions via wired and wireless networks is daunting. Service Providers such as Banks needs to provide sufficient protection and assurance to ensure that the delivery channels for conducting the transactions are safe and secure while ensuring audit trail, data privacy and regulatory compliance.



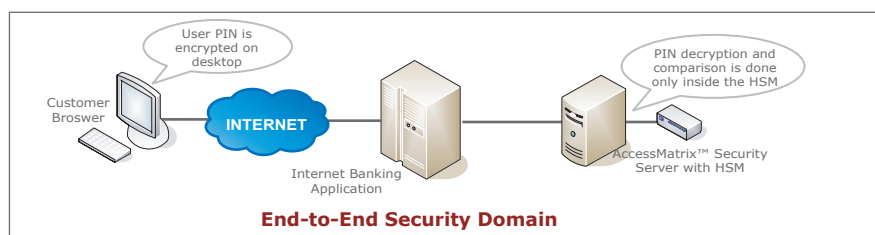
"... the encryption security pertaining to the customer's PIN and other sensitive data should be maintained end-to-end where possible. This means the encryption process is kept intact from the point of data entry to the final system destination where decryption and/or authentication takes place."

*The Monetary Authority of Singapore
Internet Banking Technology Risk
Management Guidelines, Version 2.0,
June 2003*

Internet based applications today employ simple security measures like Secure Socket Layer (SSL) to protect information transmission between the web browser and the web server to prevent the potential exposure of customer's PIN and other sensitive data. However, standard SSL technology can only protect against attacks originating from the Internet itself however, as the data arrives at the Web Server, it is automatically converted back to its clear text form, hence rendering it open to attack. To address this potential exposure, some organizations and even government regulatory agencies are pushing for end-to-end encryption solutions that will ensure that sensitive information continues to be protected from its point of entry until it is finally validated or used by the application.

E2EE Overview

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 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.



How does E2EE Password Protection work?

- i. 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.
- ii. 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.

- iii. 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.
- iv. 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.

Process Flow

The E2EE Login Protection Solution leverages the i-Sprint AccessMatrix Integrated Security Architecture and HSM devices to provide the ultimate level of security for passwords. Pre-integration and testing of the necessary infrastructure provides a plug-in solution to simplify the integration efforts.

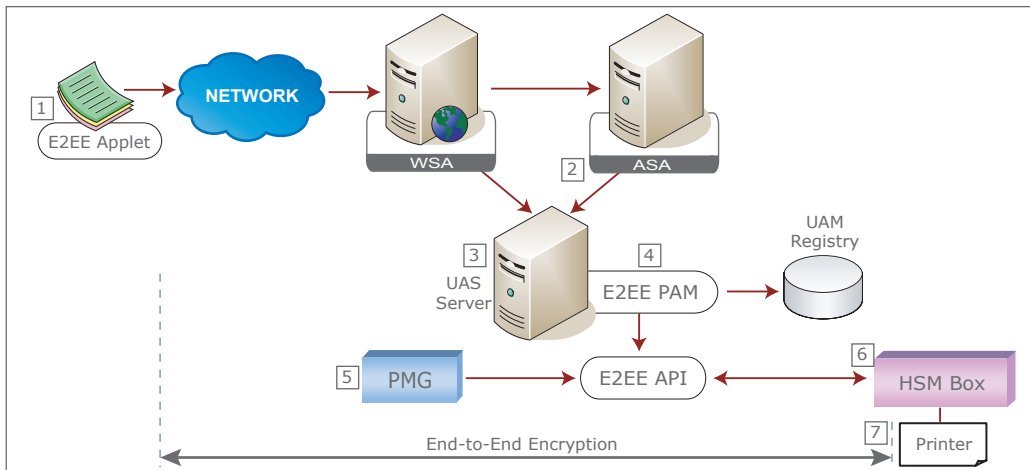


Figure 1: E2EE Architecture

As shown in figure above, the key E2EE components are:

1. **E2EE Applet** loaded within the web browser at the user's desktop.
2. **ASA** – the API library used to communicate with UAS server for E2EE operation.
3. **UAS server** – a Java server, a.k.a. Access Manager (AM).
4. **E2EE PAM** – the E2EE authentication module within UAS server that calls the **E2EE API** to perform pin verification, change password etc.
5. **PMG** – password mailer generation module, a module that calls the E2EE API to perform password generation and password mailer printing.
6. **HSM** – HSM devices for performing the password generation, verification etc.
7. **Printer** – a printer directly attached to HSM box via serial line for password mailer printing purpose.

About i-Sprint AccessMatrix Universal Authentication Server (UAS) with E2EE Module

AccessMatrix Universal Authentication Server (UAS) is designed to address the access control and single sign-on needs for web based applications. It is a comprehensive application access control, single sign-on and security administration system. It also controls and manages user access to multiple web based applications. The pre-integrated and tested E2EE solution comprising of AccessMatrix UAS and HSM devices from major suppliers can reduce integration complexity and shorten the time to deployment for E2E password protection for security sensitive applications.

Leveraging on the AccessMatrix Integrated Security Architecture, UAS fulfils the most rigorous form of application security by providing security administration, authentication, authorization, and audit services (4As) to business applications within an organization. UAS provides the necessary security infrastructure to enhance the E2EE implementations such as: ➤

With UAS, multiple web applications can access a common set of security services via tight integration with the AccessMatrix security server. The above proven modules can greatly reduce the efforts to implement the E2EE password protection solution and some of the major benefits includes:

Enhanced User Identity Protection with Multi-Factor Authentication:

Applications can also leverage on UAS's capabilities to supports other authentication mechanisms like certificates, hardware OTP tokens, smartcards, biometric devices, etc as and when the need arises without any major changes to the code.

- i. Security services APIs for application integration and shield the complexity of HSM integration.
- ii. Administration module for administration delegation and user management.
- iii. Audit and reporting module.
- iv. Java applet for credential encryption on the user's browser.
- v. HSM interface to leading brands of HSM devices.
- vi. PIN mailer interface for mail merge and secure printing.
- vii. Enforcing password policy such password history, password aging, password quality check, etc.

Enhanced Application Security with Scalable Security Infrastructure:

Built on JAVA technologies, open architecture, flexible framework, and continually adopting the latest technologies, AccessMatrix provides a common security platform to offer complete enterprise security services (Administration, Authentication, Authorization and Audit) to all business applications (both web and non-Web applications) for multiple delivery channels, which will meet the current and future requirements of our clients.

Further details about i-Sprint's products are available at www.i-sprint.com. To reach us, please email to enquiry@i-sprint.com or contact any of the offices or our resellers in your area.