AccessMatrix™ UAS
future proof universal authentication server

UAS End-to-End Encryption (E2EE) for Credential and Data Protection

Key Benefits

- Prevent exposure of sensitive information and maintain confidentiality and integrity of transaction data
- Avoid potential security threats from internal and external hackers from within the network
- Enhanced security with flexible authentication and audit policy by supporting strong authentication methods and user-centric activity tracking
- Ensure compliance with powerful reporting capabilities to report user activities and security violations
- Provide 100% assurance that other than the trusted hardware for generating the PIN, nobody will know the user's password/pin, including middle tier servers like web servers

Technology Challenges

Static Login ID/ PIN is one of the common authentication mechanisms to confirm users' online identity.

Protecting customers' PIN information has become one of the top initiatives for Service Providers such as Banks, SaaS Application Providers and cloud Providers.

As organizations look to conduct more and more business online, 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. Online Service Providers must ensure that the delivery channels for conducting the transactions are safe and secure while ensuring audit trail, data privacy and regulatory compliance.

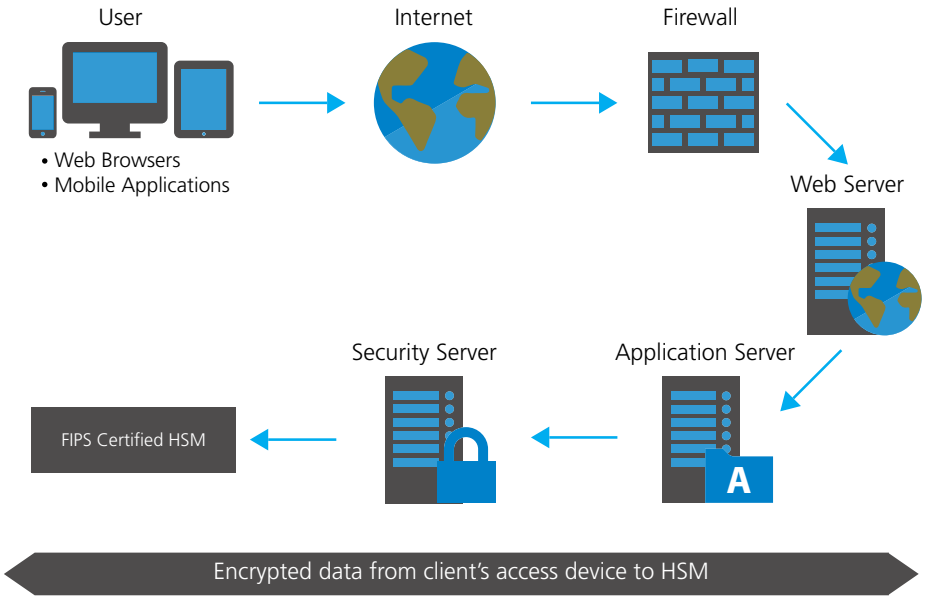
Internet based applications today employ simple security measures like Secure Socket Layer (SSL) to protect customer's PIN and other sensitive data transmission between the web browser and the web server. As the data arrives at the Web Server and Application Server, it is converted back to its clear text form, hence rendering it open to malicious attack.

Integration with HSM

E2EE creates a secured channel between the client's access device and Hardware Security Module (HSM). Within this channel, the Password is encrypted at the client's access device and can only be decrypted for verification by the HSM located in a physically secure location within the organization. In doing so, 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.

"Besides Secure Socket Layer (SSL), the FI should implement end-to-end encryption security at the application layer so that customer PINs and passwords are not exposed at any intermediate nodes between the browser and the host where PINs and passwords are verified"

-Monetary Authority of Singapore
Technology Risk Management Guidelines
June 2013



System Requirements

- Server OS: MS Windows Server 2012/ 2016 and Red Hat Enterprise Linux 7
- Application Server: Oracle WebLogic, IBM WebSphere, Apache Tomcat and JBoss Web Server
- Java Runtime: JRE 1.8 and JRE LTS
- Database for Policy Store: MS SQL Server, Oracle RDBMS and Oracle MySQL
- External User Store: Active Directory, LDAP v3 compliant directories and JDBC compatible databases
- FIPS Certified HSM
- Mobile Platforms Supported: iOS, Android and Windows Mobile

"The MA however expects that sensitive data should also be encrypted while they are transmitted between the web servers and FIs' 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 FIs' web servers or internal networks were to be penetrated"

-HK Monetary Authorities

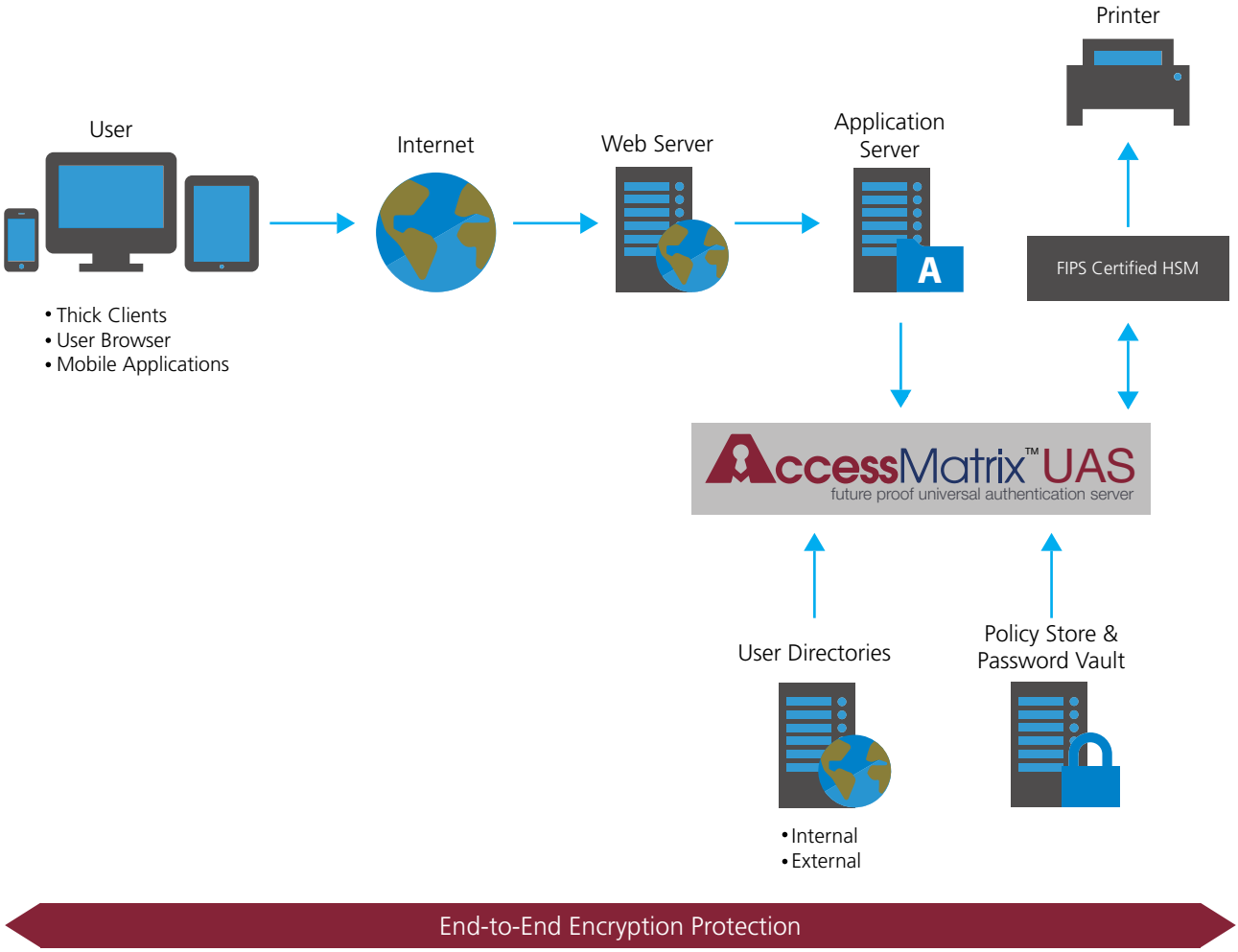
Product Features

The pre-integrated and tested E2EE solution comprising of AccessMatrix™ UAS and FIPS certified HSM devices can reduce integration complexity and shorten the time to deployment for E2E password protection for security sensitive applications. The solution provides the following proven features to address the E2E Protection requirements:

- Simple to use Security Services APIs for application integration and shields the complexity of HSM integration. Easy to deploy solution for credential encryption on the user's browser.
- Flexible Administration module for Fine-Grained administration delegation and user management.
- Comprehensive audit and reporting module will provide user-centric reporting capabilities to report access activities and security violations.
- Add-on Module for E2E of ATM PIN in transit from Web Channel and translation of ATM PIN based on ISO9564 format for integration compatible with existing infrastructure.
- Encryption libraries for popular mobile platforms like iOS, Android and Windows Mobile.
- Proven HSM interface with leading brands of HSM devices. E2EE creates a secured channel between the client's access device and Hardware Security Module (HSM). AccessMatrix™ Security Server and HSM work as an integrated solution to provide a certified tamper-resistant vault.
- Although E2EE with HSM is recommended, for deployment where HSM is not available, UAS has software E2EE solution where password is encrypted end-to-end from client device to UAS and verification is done in UAS.
- Customizable Paper and E-PIN mailer interface for mail merge and secure printing of PIN mailer.
- Extensible authentication module to include 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.
- Proven scalability and reliability features to meet the most stringent service level and operational requirements for large scale deployments.

How does E2EE Work?

- UAS provides end point encryption libraries for web based, thick-client and mobile based applications. When User accesses the login page of a service provider e.g. Internet Banking service of a bank, UAS E2EE encryption library will be downloaded to the endpoint with a public key to encrypt the login and other sensitive information.
- After the user keys in the User ID and PIN information, the E2EE library 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.


Printer
User
Internet
Web Server
Application Server
FIPS Certified HSM
• Thick Clients
• User Browser
• Mobile Applications
AccessMatrix™ UAS
future proof universal authentication server
User Directories
Policy Store & Password Vault
• Internal
• External
End-to-End Encryption Protection

About i-Sprint Innovations

i-Sprint Innovations (i-Sprint) established in the year 2000, is the leader in Securing Identity and Transactions in the Cyber World that enables individuals, organizations, and societies to build trust and identity assurance for powering productivity gain through digital identity and identity of things (IDoT).

i-Sprint's unique brand of security products, intellectual properties, and patents are designed to exceed regulatory requirements such as global financial services. By incorporating the latest mobility/ biometrics/ cloud/ identification technologies, i-Sprint provides solutions that ensure secure access and protection of data, transaction and assets. i-Sprint delivers trusty, versatile and strong authentication, and identity management platform to secure multiple application delivery environments based on a common security platform.

i-Sprint's digital identity product offerings include adaptive authentication (biometrics, multifactor authentication and more), single sign-on services, end-to-end encryption (E2EE) authentication and data protection for transaction data and to secure access to the web, mobile, and cloud-based applications. i-Sprint's IDoT product offerings provide the next-gen anti-counterfeiting, track and trace, and interactive consumer engagement that aims to help business in building consumer trust, improve brand protection, personalize consumer engagement and provide business intelligence.

i-Sprint's clients include leading global and regional financial service institutions, government agencies, telecommunications, public utilities, manufacturing, healthcare, education, multi-national corporations and others. Currently, i-Sprint has a direct presence and active authorized partners across Singapore, China, Hong Kong, Taiwan, Malaysia, Thailand, Japan and the United States.

Global Headquarters
Blk 750D Chai Chee Road
#08-01 Viva Business Park
Singapore 469004
Global: +65 6244 3900
enquiry@i-sprint.com
www.i-sprint.com

For a complete list of our offices in
China, Hong Kong, Japan, Malaysia,
Thailand & United States, please visit
www.i-sprint.com/contactus