Salt Mobile

Case Study
Identity & Access Management Journey

Highlights

Our client is rated as one of the top four corporate banks in Asia. Its Institutional Banking Division's Internet and mobile delivery platforms support the complex banking needs of thousands of organisations across more than 10 countries in the region addressing their trade finance, foreign exchange, and transactional requirements.

- ☑ Salt Group has been one of the Bank's strategic security partners for over a decade and amongst other things has provided specialised professional services and security products, and in particular, user and transaction authentication solutions utilising a mix of PKI smart cards, and Vasco authentication tokens.
- ☑ Salt provided solutions based on SafeSign Authentication Server integrated with the bank's single sign-on and identity management solutions to provide a common user interface to the bank's extensive portfolio of business applications.
- ☑ The Bank sought to extend their identity management technology to support mobile device based user and transaction authentication to enable an improved customer experience, lower capital and operational costs and importantly, to provide the foundation for innovative service delivery models across all delivery channels.

The Bank elected to utilise Salt Group's mSign authentication suite, integrated with their existing Thales SafeSign deployment to enable rapid deployment of out-of-the-box mobile authentication functionality to their customers.

The implementation was completed over a 6 month period and has enjoyed significant positive feedback from the Bank's customers.

The Client

Our client is rated as one of the top four corporate banks in Asia. Its Institutional Banking Identity and Access Management solution supports thousands of organisations and tens of thousands of users across more than 10 countries in the region.

These users perform over 50 million transactions per month, with a total value exceeding AU$250 billion per month.

The Bank is a global leader in e-services delivery and in the implementation of the necessary infrastructure that ensures the high availability and high assurance delivery of critical business services to their customers.

The Challenge – Achieving high levels of security, a superb customer experience and eliminating reliance on costly hardware based solutions

The Bank was an early adopter within its Institutional Division of robust transaction signing solutions utilising PKI smartcards that bound the transaction to a user and ensured the integrity of the transaction from point of entry through to the Bank's processing systems.

Whilst servicing the Bank's needs well for many years the suitability of smartcard based authentication reduced over the years due to high costs of card management and costs associated with ongoing verification of associated software within customer operating platforms. The need for support of mobile banking platforms, where smartcard readers are not readily supported also impacted on the suitability of smartcard tokens.

Moreover, the prevalence of browser based malware exposed the bank to increased risk through attack on transactions prior to the signing function being completed on the card. The costs of PIN PAD card readers to mitigate this attack type were prohibitively expensive.

As an alternative to smartcard tokens, the Bank had introduced hardware tokens in some markets.

These were not considered a suitable long term alternative to smartcards due to customer usability issues and the high costs of purchase and distribution. They were also unsuited to transaction signing use cases that had been previously well accommodated with smartcard usage.

Accordingly, the Bank was looking for a more flexible, user-friendly, and convenient authentication solution that could be used across all delivery channels and provide their institutional customers with an intuitive and contemporary way to authenticate themselves and their transactions. Something that aligned with the way they worked already. Something that could integrate well with the Bank's emerging service delivery options and support the assurance levels that the Bank needed to comply with its operational risk demands.

The Solution

Salt Group had worked with the bank over many years on the development of the bank's Identity and Access Management infrastructure which included the Oracle Identity stack, CA SiteMinder and Thales SafeSign Authentication Server (with HSMs) and Card Management System.

Salt played lead architectural and deployment roles in refreshing the Bank's early bespoke smartcard based solutions with the introduction of a suite of COTS products as described above, including a transition to new smartcard based technology for secure logon and transaction signing and later introduction of authentication tokens.

The IDAM system protects around 10 business applications.

In 2017, for the reasons outlined above, the bank elected to complement the smartcard and token authentication options with Salt's mSign authentication suite which interworked seamlessly with the existing Thales SafeSign Authentication Server to provide a convenient, high assurance method for customer logon and transaction authentication.

Solution Features

mSign provides intuitive logon and transaction authentication workflows using mSign's Connected Mode whereby a bank customer would receive alerts on the mobile device for approval or rejection after authorising this action by PIN or biometric. Solution features include:

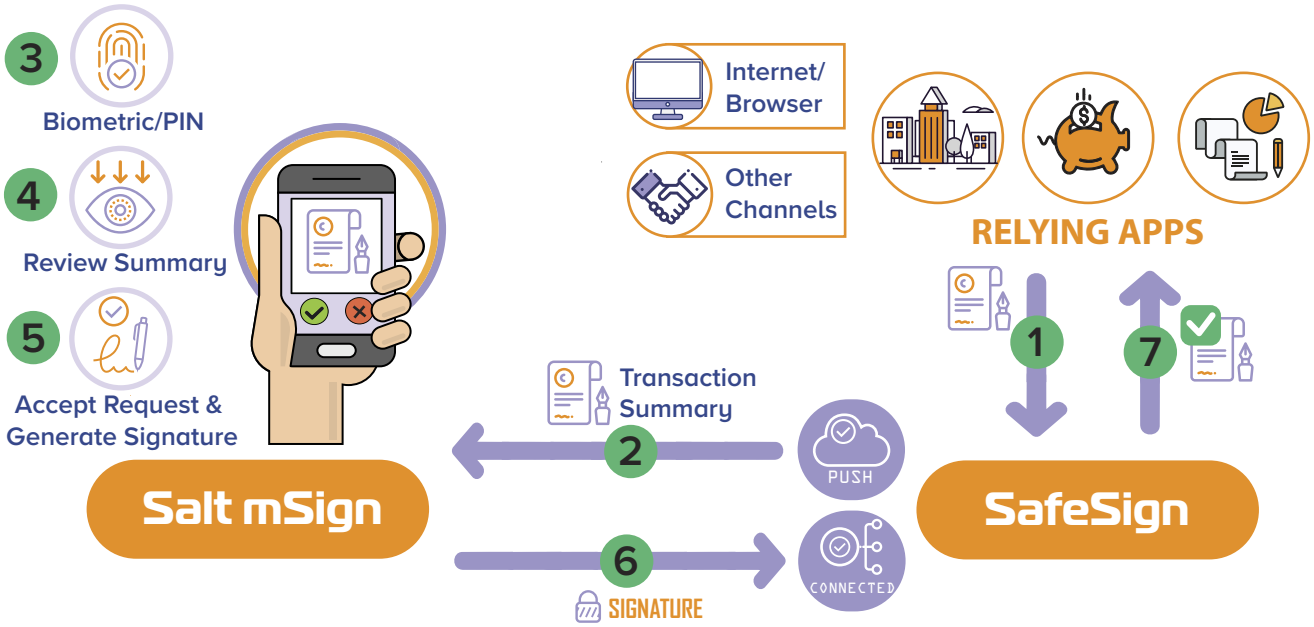
- Connected mode operation utilises the mobile channel for authentication request and response messaging between SafeSign and the mSign mobile application. This abstraction of the authentication channel from the delivery channel enables the bank to provide strong authentication services for transactions regardless of their entry point; internet, mobile, operator assisted. The approach also removes the risks associated with browser based malware.

- mSign provides full "what you see is what you sign" capability for transaction authentication. All of the business application defined information displayed to a user is signed providing a superior model to specialised tokens where contextless information is entered into a token with the risk of man-in-the browser attacks.

- The mSign token supports an offline mode in the event of mobile device communications unavailability. In this mode mSign will operate in the same way as a specialised security token, albeit providing an improved user interface and biometric support.

- Self-service user account and mSign activation provides a superior and streamlined registration process compared with smartcards and tokens. This is a major customer service benefit enabling essentially instant onboarding of new users within the institutional banking client office.

- Fully integrates with existing SafeSign Authentication Server as a new authentication service, with standard Thales secure audit facilities, HSM support and failover resilience.



Solution Benefits Summary

- **Simplifies Deployment** – Salt mobile tokens enable a simple one step installation and token activation process to be completed enabling users to start to use the online service immediately upon account establishment.
- **Increases User Satisfaction** – Salt mobile tokens enable users to simply approve authorization requests on their mobile using their PIN or biometric rather than entering tedious transaction summaries into a hardware token.
- **Reduces Overall Cost** – Salt mobile tokens substantially reduce capital and ongoing device management and replacement costs associated with hardware tokens.
- **Zero Mobile App Development** – The bank simply filled out the mSign configuration sheet and supplied the necessary branding artwork. Salt applied these to the standard mSign product which was subsequently tested and approved by the bank for deployment to production in a matter of weeks.
- **Easy to Use** – Server side RESTful API enable rapid onboarding of Institutional Applications in a matter of weeks.