International Private Bank selected Sysmosoft SENSE to release its business-critical Mobile Reporting Solution for Relationship Managers in a compliant and safe manner.

Executive summary

As mobility presents new business opportunities, the private bank was searching for mobile solutions to enable its traveling relationship managers to access and present prepared documents to private clients. By combining a dedicated App with Sysmosoft SENSE technology, the private bank was able to quickly release a solution that significantly increase efficiency of its staff during customer's meeting without compromising security or infringing compliance policy.

Business Challenges

Given that the solution had to handle highly restricted client information, subject to specific Swiss Banking Regulation (FINMA), the Private Bank was seeking a trusted and reliable mobile solution that can match expectations of business decision makers (management, security, auditors, architecture) with limited resources and capacity.

Confidential Customer
International Private Bank

Industry
Finance, private banking

Location
Geneva, Switzerland

Employees
+2'000 employees with 200 asset managers across other locations

Product
Sysmosoft SENSE

MEET SECURITY REQUIREMENTS
Ensure the solution incorporates state-of-the-art security to protect client data and pass audits

MEET COMPLIANCE REQUIREMENTS
Ensure the solution can fulfil compliance controls requested by auditors (cross-borders, FINMA)

MEET ARCHITECTURE REQUIREMENTS
Ensure the solution can be integrated with infrastructure and existing systems

DELIVER ON-TIME
Ensure the solution can be released on time without being blocked by security / audits.

DELIVER WITHIN BUDGET
Ensure the solution does not require additional costs to meet security / compliance expectations

Solution Approach

SENSE is comprised of a corporate gateway, installed and controlled within the bank premises, and a mobile layer, injected within the bank's mobile App. The front-end of the mobile App, including its business logic and design, is made by the bank according to its specifications. Complex background tasks related to the protection of client data and enforcement of compliance policy are delegated to SENSE.

The Bank App uses SENSE to display financial documents without leaving trace of client data, encrypt client data end-to-end with audited mechanisms (algorithms and key exchange), perform convenient strong authentication prior to authorizing access to client data, block and report relationship managers trying to access data from specific countries, and generate reports that contain information required by auditors (who, where and when client data was accessed / stored).

Business Benefits

From a business perspective, SENSE enabled the private bank to release its business-critical mobile App on-time and according to the allocated budget without being blocked or delayed by security and compliance departments. Business project leaders achieved their objectives while architects, security officers and auditors benefit from a trusted and reliable solution that handles client data according to their expectations.

PASS SECURITY AUDITS
SENSE capabilities enabled the App to pass security audits, pen-tests and cryptography reviews

QUICK TO INTEGRATE
SENSE was deployed, configured and integrated within the bank infrastructure and its App in 7 days.

PASS COMPLIANCE AUDITS
SENSE capabilities enabled the App to pass auditors reviews and delivered required trust level

NO NEED FOR SPECIFIC KNOWLEDGE
SENSE was integrated by developers without requiring specific security knowledge

INTEGRATE INFRASTRUCTURE
SENSE modularity enabled to quickly integrate with specific authentication system and identity source

COMPATIBLE WITH IT MOBILE STRATEGY
SENSE was used on top of MDM for this specific use-case without impacting the IT MDM strategy

NO IMPACT ON USERS EXPERIENCE
SENSE have no impact on App behaviour or user's experience while self-protecting the App

OPTIMIZE COSTS OF FURTHER APPS
SENSE can be used across multiple Apps to avoid additional development & assessments costs

Next Steps

Based on the successful launch of its mobile solution, the private bank decided to replicate the use-case across several worldwide subsidiaries. The bank now plans to use SENSE technology as a corporate standard across all business critical Apps for its internal business staff that will have access to client information. This enables the bank to have an homogenous security / compliance layer across all of its business-critical Apps and doesn't need to perform deep assessments and security audits.

sysmosoft

COMPLIANCE CONTROLS

Cross-Border policy – client data shall be accessed only from authorized countries	SENSE enforces business rules to block access from specific countries or adjust security settings
No Client Data Trace – client data shall leave no persistent trace at endpoints	SENSE ensures client data leaves no trace in temp / caches and key storage from data
Client Data Access Monitoring – who, where and when client data is accessed shall be recorded	SENSE tracks apps, mobile users, mobile actions and mobile locations used to access client data
Client Data Location Tracking – location of client data shall be known at all time	SENSE tracks location where data is stored and how it is protected / encrypted (key location)
Configuration tracking - modification to configuration or security policy shall be tracked	SENSE tracks all actions and changes made by administrators on administration console

SECURITY CONTROLS

State-of-the-Art Security - client data shall be encrypted with trusted encryption algorithms & keys	SENSE implements state-of-the-art cryptography and key management controlled by the bank
End-to-end encryption - client data shall be encrypted at all time by the App itself	SENSE encrypts data in-transit and at-rest with application level security layer
Malware Protection - client data shall remains protected in case of infection of the device	SENSE encryption and keys are specific to the app and do not inherit from device vulnerabilities
Lost Device Protection - client data shall be inaccessible (brute force etc.) on stolen device	SENSE stores specific encryption keys server side (and not on device) for long term protection
Improper Behaviour Protection - client data shall be protected even if device is misconfigured	SENSE security level is homogenous across all devices whatever their ownership or configuration

COMPLIANT & SAFE SOLUTION