sqs.com

Case Study - Banking & Financial Services

Enhancing the Contactless Cards UAT. Enabling faster and efficient transactions.

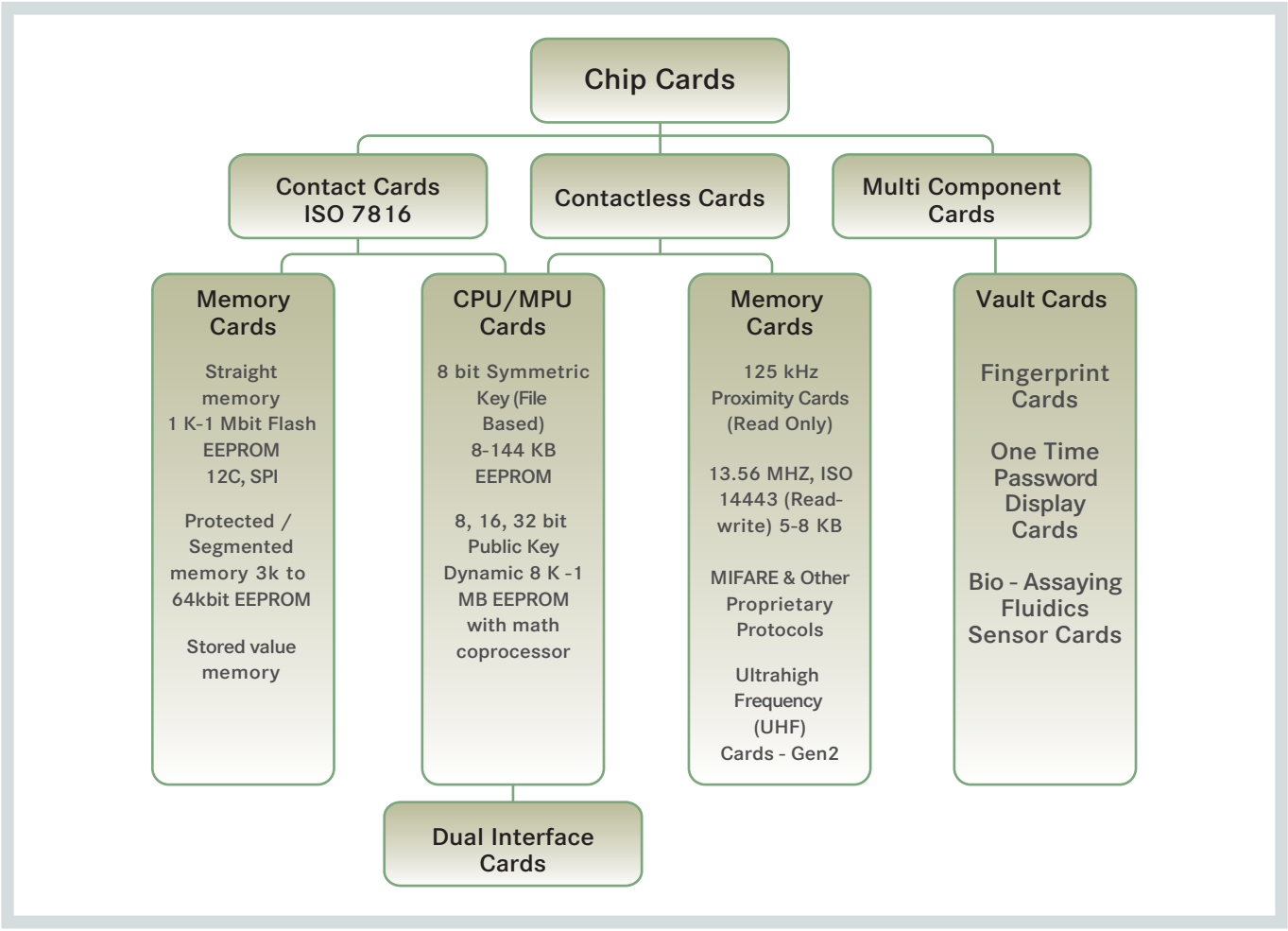
A leading European Bank established successfully across various Credit/Debit & Business Card products intended to issue contactless credit cards for newly acquired customers. With Transport for London (TFL) planning to phase out Oyster Card ticketing and their plans to accept Contactless Cards & Near Field Communication (NFC) enabled mobile phones, the management of the bank thought that this would be the opportune time for adopting this technology. An accomplished expert across the AML domain, with a very laudable track record in North America, the Senior Project Manager was urgently summoned to headquarters to supervise and manage the transition.

Knowing little about payment cards per se, the Senior Project Manager had to quickly get to speed with the technology involved. She sought the help of the in-house whiz kid to run her through a primer. Next morning, the Senior Project Manager had this illustrated note on her table.

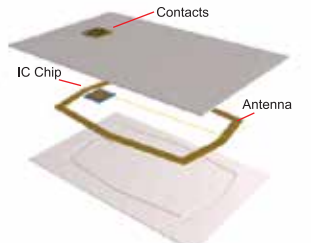
Payment Cards are single layer or multilayer plastic cards of 85.00x53.98 mm in size, complying with ISO/IEC 7810 ID-1 standards that could be electronically linked to an account of the card-holder. They could be Credit cards, Debit cards, ATM cards, Charge cards, Stored-value cards, Fleet cards, Gift cards, Scrip cards or Electronic Purses/Wallets. In terms of access technologies, they could be Magnetic Stripe cards or Chip cards (also known as Smart cards).

Magnetic Stripe Cards are governed by ISO/IEC; 7810, 7811, 7812, 7813, ISO 8582 and IEC 4900 standards, that define the physical properties of the card viz., its size, flexibility, location of the magnetic stripe (Magstripe), magnetic characteristics and data formats. They also provide standards for financial cards including allocation of Card-number ranges to different card issuing institutions.

Smart Cards or Chip Cards or **Integrated Circuit Cards (ICCs)** contain embedded ICs that can process data. There are two main categories of smart cards; **Contact Cards** and **Contactless Cards**, with each of them being Memory cards or CPU/MPU cards as shown in the diagram.



Dual-interface cards implement contactless and contact interfaces on a single card with some shared storage and processing.



Contactless Cards

Conforming to ID-1 of the ISO/IEC 7810 standards contain a tamper-resistant security system (e.g. a secure cryptoprocess or and a secure file system) and provides security services (e.g. protects in-memory information). They essentially rely on Near Field Communication (NFC) technology that:

- Uses short range, high frequency wireless communication
- Enables simple and safe two-way interactions among electronic devices
- Requires that two NFC devices are brought within centimeters of each other
- Affords a fast and easy to use system without compromising existing service security
- Allows consumers to perform contactless transactions

The NFC N-Mark may appear on NFC-enabled devices. It marks the spot on devices or objects where NFC technology works when they are brought close together. For example, you can bring a mobile phone near a poster to download information.

Applications

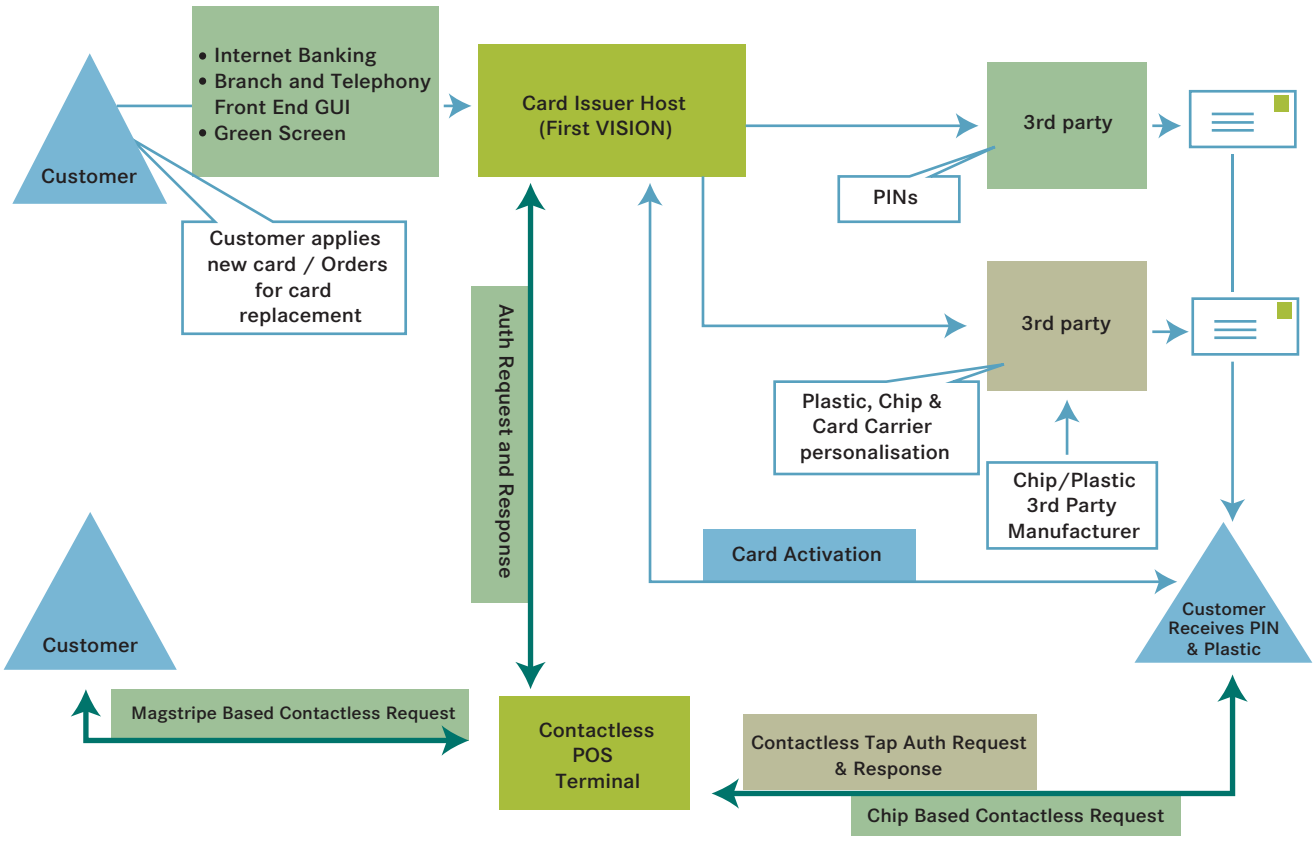
Contactless smart cards do not require physical contact between a card and reader. As such they are popular for payment and ticketing. Typical uses include mass transit and motorway tolls. Other everyday applications that are likely to be NFC enabled are Vending machines, ATMs, Mobile phones, Parking Meters, Turnstiles, Drivers licenses, Patient cards and many more to come. Contactless smart cards are part of ICAO biometric passports to enhance security for international travel.

Advantages

The benefits are directly related to the volume of SQS Contactless Card UAT information and applications that are programmed for use on a card. A single contact / contactless smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card. For example, a smart card can be programmed to only allow a contactless transaction if it is also within range of another device like a uniquely paired mobile phone. This can significantly increase the security of the smart card.

With a couple of readings and some explanations from the whiz kid, the Senior Project Manager was ready to digest the knowledge and experience of the cards business within the bank. Enquiring further she found that a testing specialist that the Senior Project Manager had heard about in USA was already engaged with the bank to perform testing for BAU & other projects.

The Senior Project Manager suggested that the bank engage the same firm and the whiz kid concurred. With the bank using the 'First Vision' application for Credit Cards processing, that they were familiar with, SQS was thus entrusted with the User Acceptance Testing (UAT} of Contactless Credit Cards.



Functionalities to be tested

The bank decided to issue contactless cards to AMEX & MasterCard customers which triggered

- Migration and upgradation from AMEX: SDA (Static Data Authentication) to DDA (Dynamic Data Authentication) as a pre-requisite to issue ExpressPay enabled AMEX cards and for increased fraud protection
- Migration from VIS CHIP to MChip for certain products as a pre-requisite to be able to issue MasterCard PayPass cards

Considering the fact that application service provider had the solution delivered across multiple releases, the following functionalities were to be tested:

- Account Boarding
- Card Carrier/Inserts
- Authorisation
    - Chip & PIN - Contact & Contactless mode (Scheme & Intra)
    - Chip & Sig - Contact & Contactless mode (Scheme & Intra)
    - Offline Counters
- Transaction Processing
    - Chip & PIN
    - Chip & Signature
    - Contactless Intra
    - Contactless Scheme
- Chargeback Processing
- Fraud Reporting
- Reporting

Key Challenges

In taking up the work, the challenges faced by SQS could be summarised as:

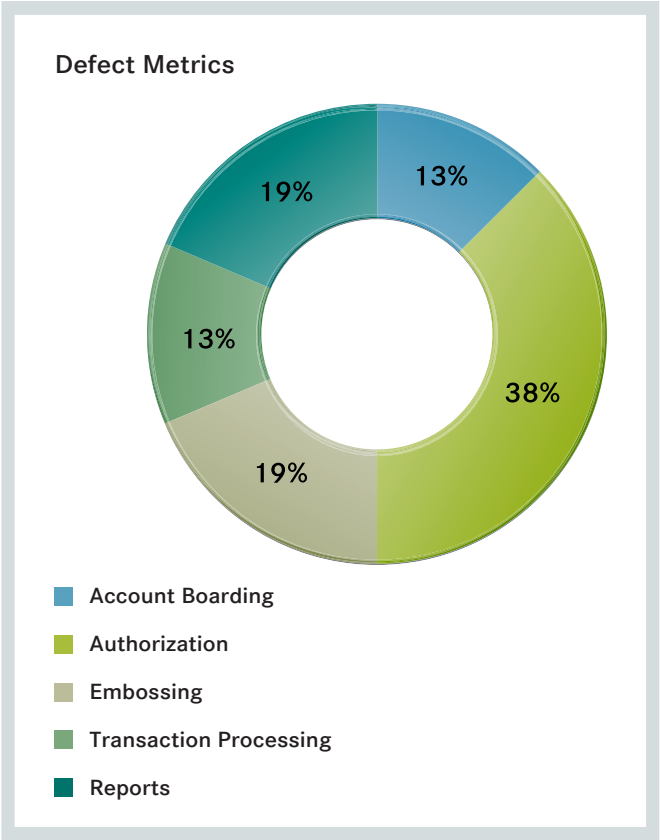
- Code delivery was split across two releases and hence testing had to be planned across two code bases
- The Contactless Card produced from SIT testing failed CPV (Chip Personalisation Validation) testing for MasterCard which meant UAT was to be conducted in parallel to Chip testing by FIME
- Chip offline counters being common for both contact and contactless transactions, it was challenging to test if the counter was being incremented and offline limits validated for both kinds of transactions
- Key design issues were identified on how the contactless chip counters are reset for different authorisation responses
- Design issues related to issuance of new cards/replacements/re-issue with Contactless cards were identified during the walkthrough sessions with the application service provider

The modus operandi: The SQS way

SQS recommended a ‘Testing and Implementation’ workshop be conducted and during which the approach suggested by us was:

- Transaction Processing
    - To split the testing phases such that during the initial code drop, testing was done using the ‘Test product’ set up in UAT region
    - A thorough functional testing on all active products was undertaken after the final code drop into UAT
    - SQS recommended that the implementation approach be similar to that of the initial First Occurrence Validation (FOV) using cards generated from ‘Test Product’ set-up in the production environment. Once successful, the project was to be rolled out to actual products which the customers hold
    - The above approach was appreciated as it was very productive and cost effective for the Bank
- Contactless Cards was produced by SQS from the UAT environment was thoroughly tested using the contactless POS terminals and Barnes tested before being sent to FIME for Chip certification. This ensured the Bank passed the 2nd Iteration of chip certification
- SQS prepared detailed scenarios for testing Chip-offline counters and limits. The bank’s Business and IT teams were walked through these scenarios
    - A separate walkthrough session was set up with POS terminal vendor to set up appropriate floor limit for both Contact and Contactless Authorisation to test and ensure the offline counters do get accumulated and validated with offline limits

- All the design issues were logged as Incidents and discussed with Risk & Fraud teams within the Business for them to understand the risk-exposure on account of these issues
    - Based on the risk-exposure suggested by SQS the incidents were appropriately triaged and fixes promoted



Way Forward

- Development and maintenance of a Test Coverage upon successful implementation of PayPass (MasterCard) cards, the Bank has decided to launch ExpressPay (AMEX) as well for which SQS was engaged from the study phase of the project
- With Phase-1 targeting new customers, the Bank is planning to issue Contactless (PayPass & ExpressPay) cards to their back book portfolio (Replacement, Additional & Lost or Stolen Replacements) as part of Phase-2 of this project

Contact

If you are interested in SQS' service offering regarding testing and quality management for the Banking & Financial Services industry, please do not hesitate to send us an e-mail: info@sqs.com