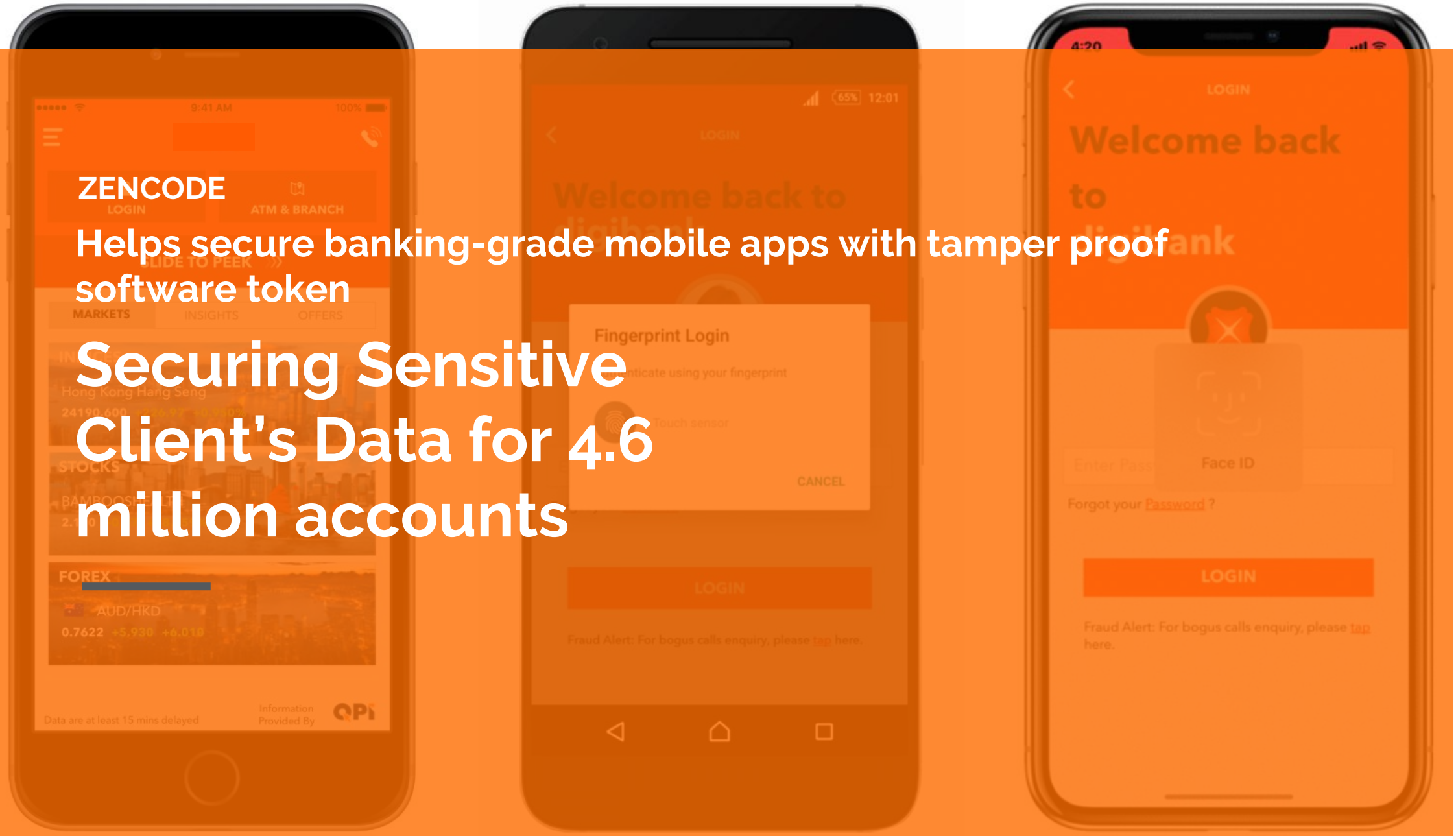
Zencode CASE

STUDY



ZENCODE

Helps secure banking-grade mobile apps with tamper proof software token

Securing Sensitive Client's Data for 4.6 million accounts

AT A **GLANCE**

Secure Mobile Apps

The world is getting more mobile, yet data security and integrity is under more threat due to confidential data residing on clients phones and the organisation's employee's personal phones. Hence the need for more advanced and multi-layered mobile app security.

However with banking records that problem is more pronounced as clients need to transact in the new world of cashless payments and instant transfers. Thus the need to ensure end-to-end security of the data; during transfer, within the mobile device and during client interaction with app.

SERVICES

Industry : **Banking**
Location : **Global**
Employees : **over 20,000**
Services : **Application Protection & Data Security**

THE **ORGANISATION**

Established on 16 July 1968 by the Government of Singapore to take over the industrial financing activities from the Economic Development Board, the bank's main purpose was to provide loans and financial aid to the manufacturing and processing industries and to help establish and upgrade existing industries in Singapore. The proposal included setting up a development bank, together with an economic body to attract foreign investments and provide financing and managing the industrial estates. The bank was incorporated in July 1968 and began operations in September of the same year.

With operations in 17 markets, the bank has a regional network spanning more than 250 branches and over 1,100 ATMs across 50 cities.

THE **CHALLENGE**

In 2017, the average number of breached records by country was 24,089.[1] There are around 24,000 malicious mobile apps blocked every day [2] and 31% of organizations have experienced cyber attacks on operational technology infrastructure. [3] The average cost of a malware attack on a company is $2.4 million. [4]

To prevent this from happening to Asia's strongest bank, there was a need to improve current hardware token implementation, as it impacted the rollout of security to older smartphone devices and newer smartphones as well. Furthermore if the app resided in a compromised mobile phone environment (user downloading a trojan horse app) it might lead to banking data being stolen from the user's phone.

[1] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&
[2] http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_
[3] https://www.cisco.com/c/en/us/products/security/security-reports.html#~stickynav=2
[4] https://www.accenture.com/us-en/event-cybertech-europe-2017?src=SOMS#block-insights-and-innovation/

ZENCODE

THE SOLUTION

To use Zencode's best-in-class solutions and consultancy.

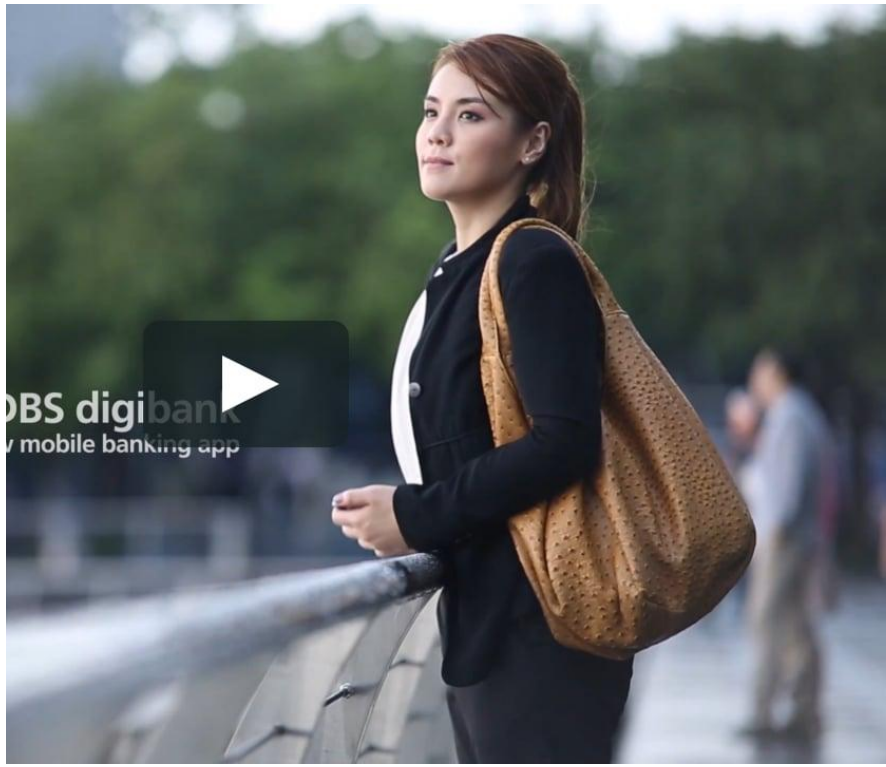
Zencode brings together best in class solutions from solutions that power the world's strongest financial institutions from banks to funds to stock exchanges.

Using solutions from virtual secure elements (software based tokens), to strongest cryptography mobile app containers to tamper detection solutions, Zencode has it all.

CASE STUDY

ZENCODE

With Zencode's System Integration and Mobile App Development



Zencode can develop customised mobile apps with secure app containers to prevent tampering of sensitive data within the app, even if the mobile phone is hacked or compromised.

Being able to integrate several different security solutions (from Horangi to BlackBerry Enterprise solutions to V-Key) and past experience with some of the strongest financial institutions in the world, Zencode is able to not just create a great User Experience, but one with a very strong security aspect

CASE STUDY

ZENCODE