

# Mobile Security Seminar

Empowering Business Users Securely

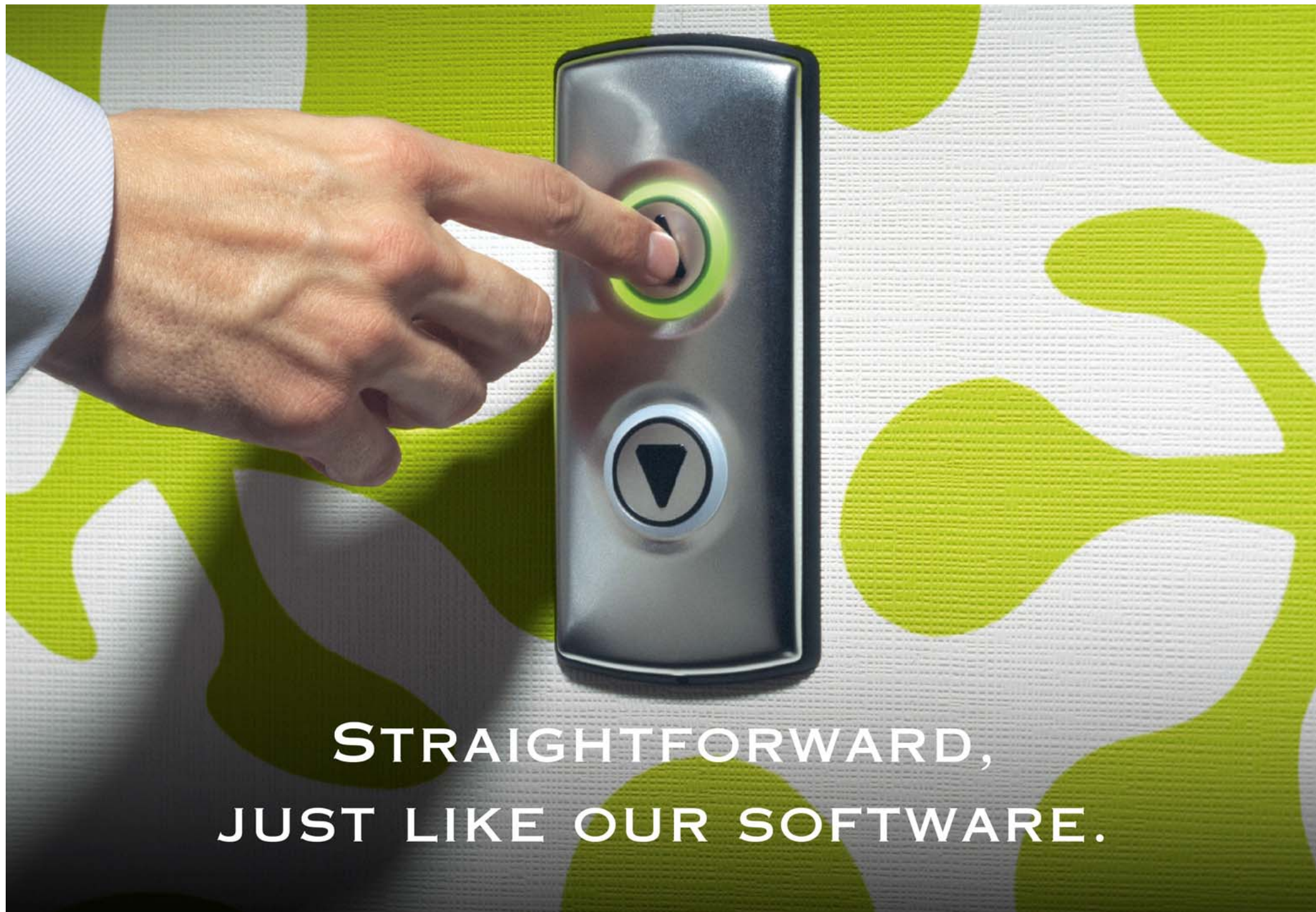
**Martin Nokes, Managing Director**  
**Loic Pfister, Software Engineer**

31 January 2013



swiss made  
software



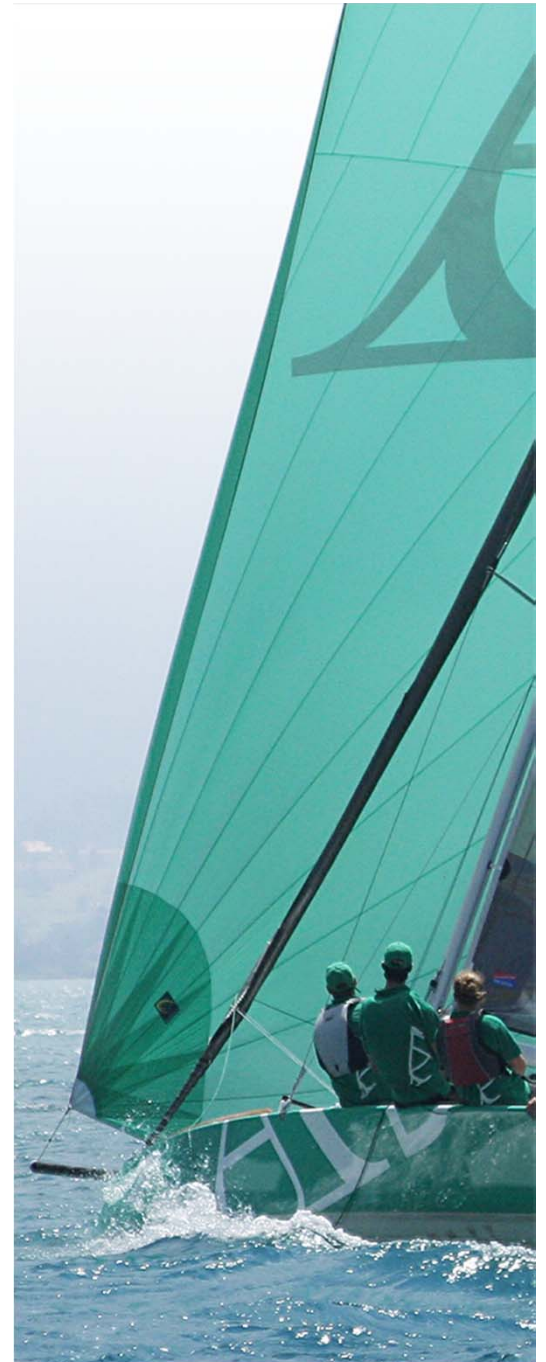


**STRAIGHTFORWARD,  
JUST LIKE OUR SOFTWARE.**

# Today' s Agenda

<b>09.30 am – 10.30 am</b>	<b>Enterprise Mobile Security &amp; Live Jailbreak</b> Martin Nokes, Managing Director Loic Pfister, Software Engineer
<b>10.30 am – 11.00 am</b>	<b>Coffee Break</b>
<b>11.00 am – 11.30 am</b>	<b>Case Study – UBS Mobile Banking</b> Moritz Kuhn, Principal Consultant Seet Teck Kiang, Director of Sales and Business Dev
<b>11.30 am – 11.45 am</b>	<b>Questions and Answers</b>
<b>11.45 am</b>	<b>Event Closes</b>

# Enterprise Mobile Security & Live Jailbreak





# Speakers

(i)



- **Martin Nokes**
- **Managing Director**
- **[martin.nokes@adnovum.sg](mailto:martin.nokes@adnovum.sg)**
- **Direct +65 6372 9786**
  
- **15 years industry experience**
- **Delivery and consultancy**
- **Finance, government, telco**

# Speakers

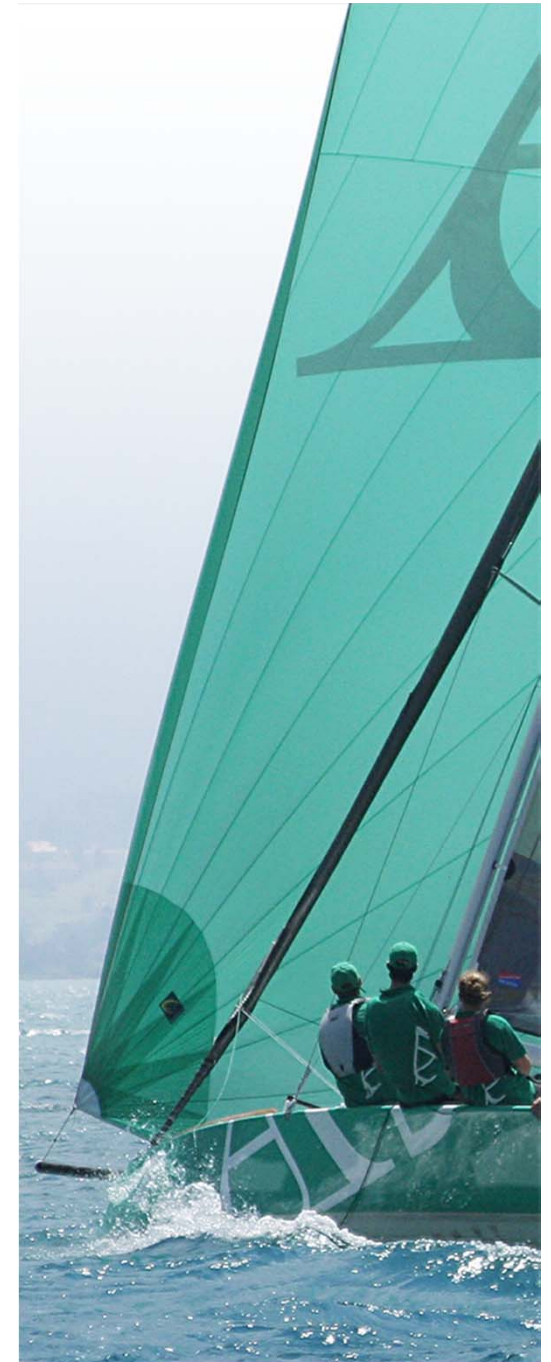
(ii)



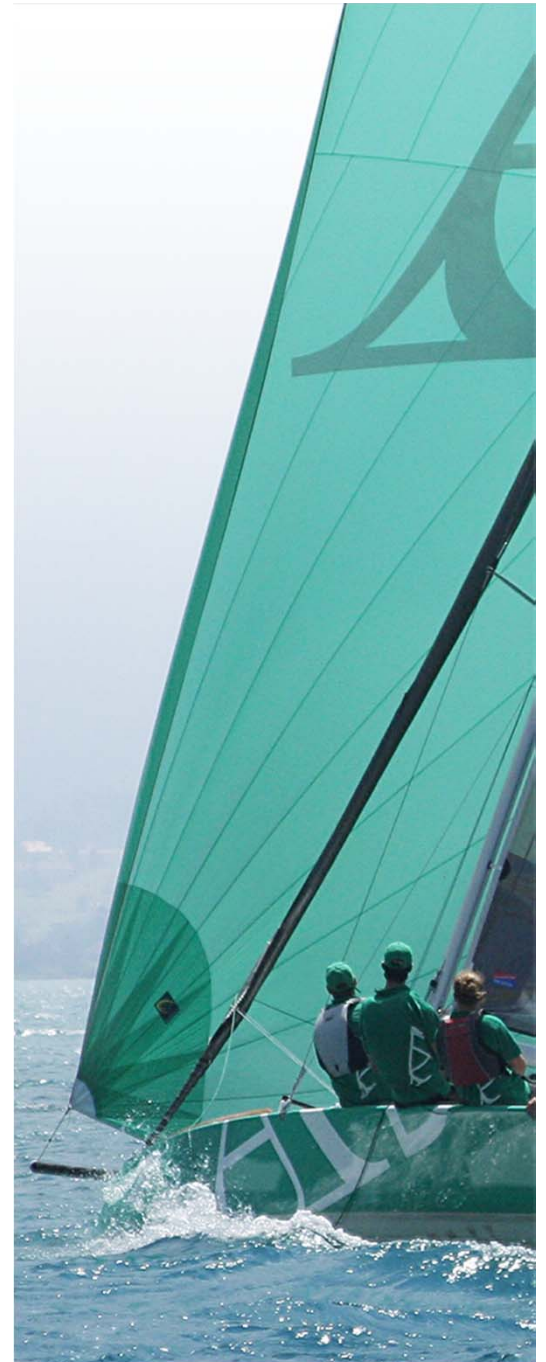
- **Loic Pfister**
- **Software Engineer**
- **loic.pfister@adnovum.sg**
- **Direct +65 6372 9785**
  
- **2 years industry experience**
- **Research Fellow at A\*STAR**
- **GIAC certified exploit researcher and penetration tester**

# Agenda

- **Live Jailbreak Part 1**
- **Company Intro**
- **Mobile Security**
  - Why?
  - Stakeholders
  - Managed Devices vs. Focus on the App
- **IT Risk and Security Overview**
- **Enterprise Mobile Security**
  - Differences vs. Traditional Applications
  - Biggest Threats/Risks
  - Approaches
- **Live Jailbreak Part 2**



# Live Jailbreak Part 1





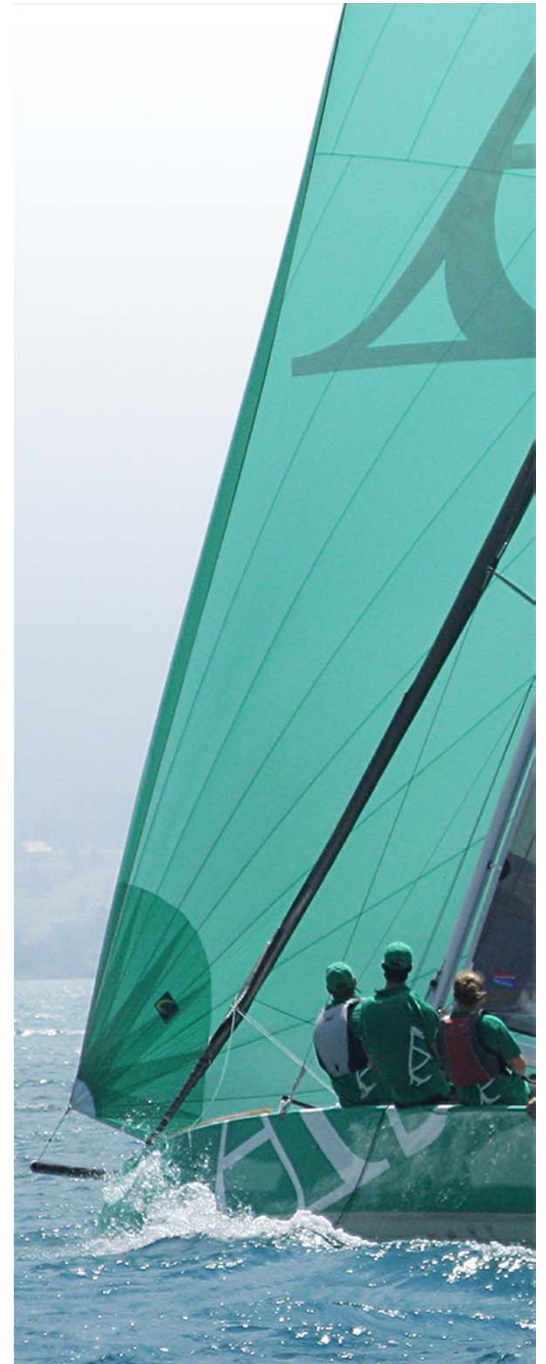
# Scenario

- iPhone or iPad running iOS 4.x 5.x or 6.x
- Protected by pass code
- Borrowed/lost/stolen while locked/turned off
- To demonstrate how easy it is to access the data on the device

# Steps

1. **“Jailbreak” the device**
2. **Transfer of all data to notebook**
3. **Browse unencrypted data**
  - Contacts, pictures, screen shots of running apps, etc
4. **“Brute force” the pass code**
  - “Brute force”: Try repeatedly until we get the right one
  - Necessary for retrieval of the private key
5. **Browse encrypted data**
  - Which was protected by the pass code
  - User IDs and passwords of Gmail, Facebook, Skype, Twitter
  - Wi-Fi passwords
  - Etc.

# AdNovum Company Overview



# AdNovum: Swiss Quality Engineering

## Core Competence

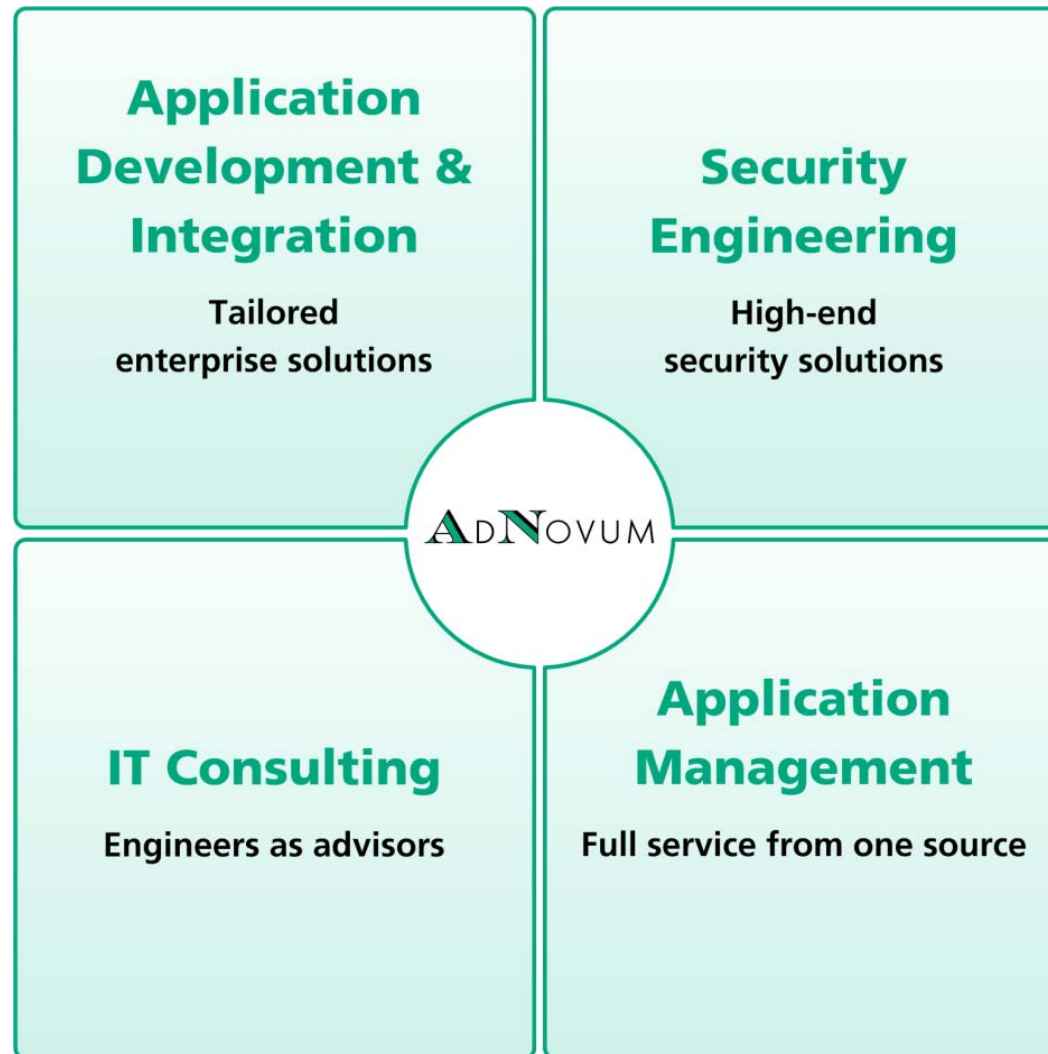
- High-End Security & Software Engineering

## Key Data

- Est. 1988 – privately owned joint-stock company
- Zurich (HQ), Singapore, Berne, Budapest (Hungary)
- 300 employees, 70% BSc/MSc/PhD Computer Science



# AdNovum: Service Offering





# Customers and Industry Focus

## Finance



Mercedes-Benz  
Financial Services



SCHWEIZERISCHE NATIONALBANK  
BANQUE NATIONALE SUISSE  
BANCA NAZIONALE SVIZZERA  
BANCA NAZIUNALA SVIZRA  
SWISS NATIONAL BANK

The Swiss National Bank



## Government



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Federal Government of Switzerland



Canton of Zurich, Switzerland



Central Provident Fund Board,  
Singapore

## Insurance



Helsana



## Logistics / Industry



## Telecom



Sunrise



# How AdNovum Can Help You – Mobile



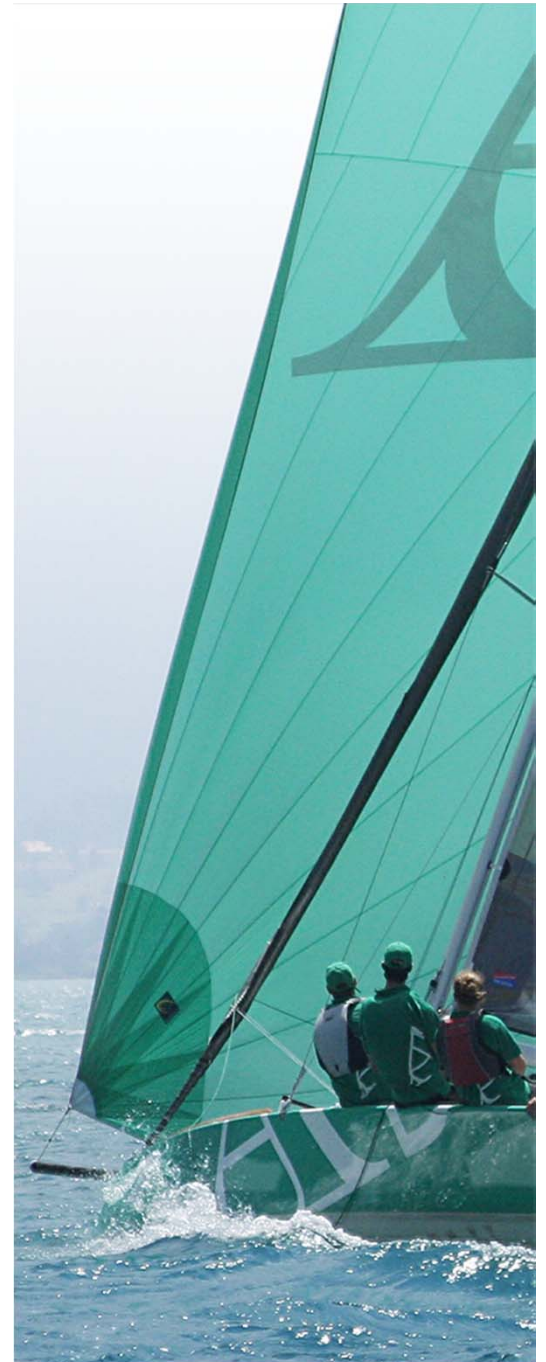
To date, there are approximately 800'000 users of our mobile enterprise applications (which have high-end security requirements) across banks, corporations and government agencies.

Our mobile development hub is based in Singapore and tapping on our extensive mobile enterprise experience, we are pleased to offer the following services:

- Design, Implementation, Delivery
  - End-to-end implementation of mobile applications (cross-platform)
    - iOS, Android, Blackberry, Windows 8
    - Smart phones and tablets
  - World-class user interface/experience design
  - Coverage of all security requirements for compliance & regulations
  - Integration with backend systems
- Consultancy
  - Workshops
  - Proof of concept (PoC) and prototype development
  - Requirements engineering
  - Architecture
  - Security reviews and penetration testing



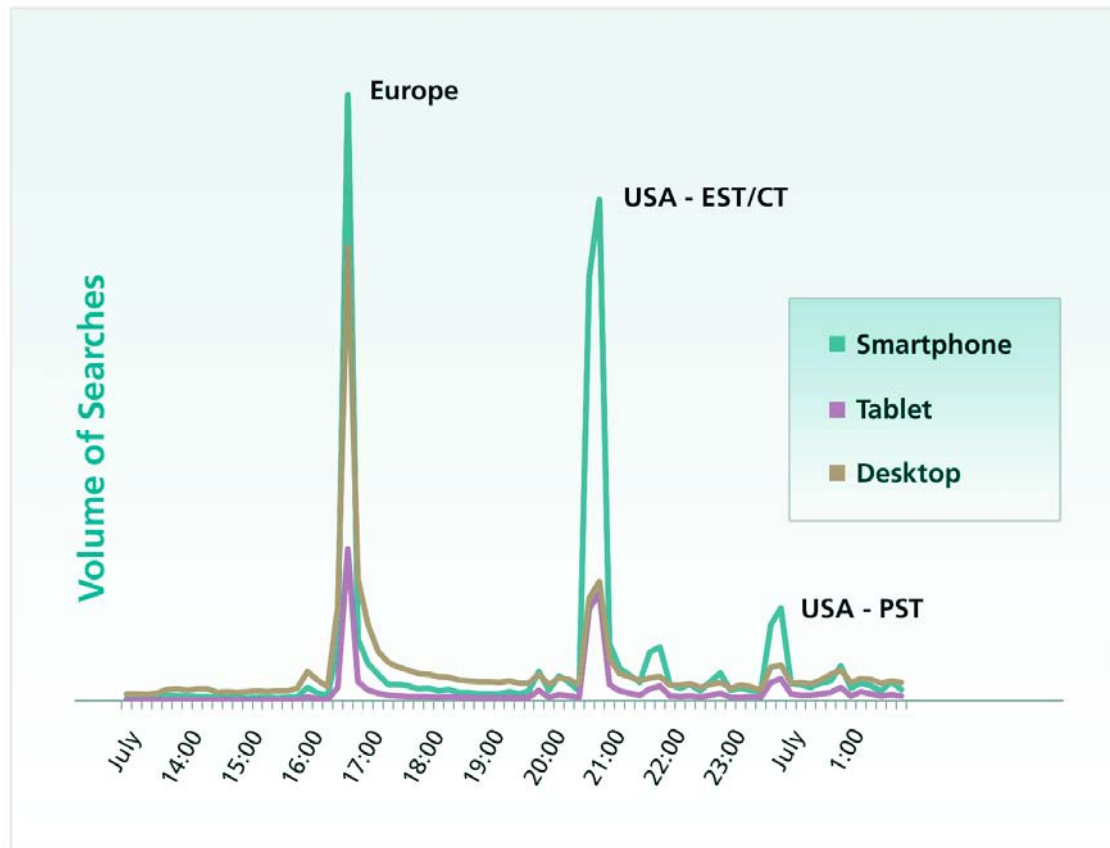
# Mobile Security



# Mobile – Why?

(i)

- Proliferation of mobile devices
- Businesses want to take advantage of opportunities



Global searches for Paul McCartney during local broadcasts of the Olympics opening ceremony (PST)

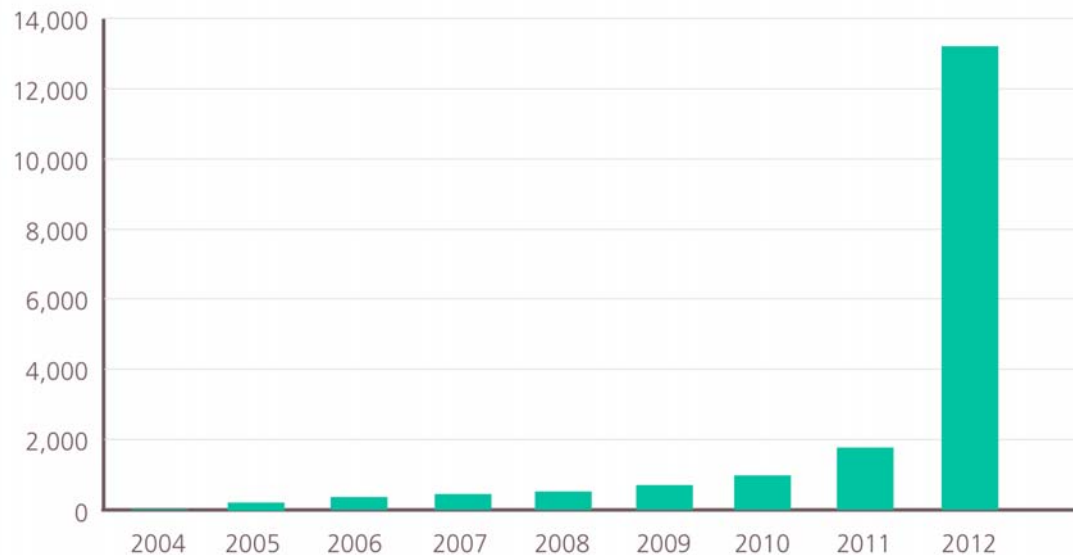
Source: Google

# Mobile Security – Why?

(ii)

To reach and satisfy their users, governments and enterprises are moving data and processes to mobile devices

→ Mobile devices become targets of attacks



Total mobile malware

Source: McAfee Threats Report, 2<sup>nd</sup> Quarter 2012



# Mobile Security – Why


(iii)

To reach and satisfy their users, governments and enterprises are moving data and processes to mobile devices.

→ Breaches happen

FILED UNDER [Cellphones](#), [Software](#)

## FTC asked to open an investigation into Carrier IQ

By Terrence O'Brien  posted Dec 2nd 2011 3:43PM

## Facebook Plist Mobile Security Hole Allows Identity Theft [Updated]

Written by: [Gareth Wright](#)

Apr 3, 2012

## Sensitive personal information stolen with Pr. William BlackBerry

July 16, 2010

[0 Comments](#)



Sensitive personal information about almost 700 Prince William County residents, including addresses and Social Security numbers, has been compromised after a county-issued BlackBerry was stolen from an employee's locked vehicle.

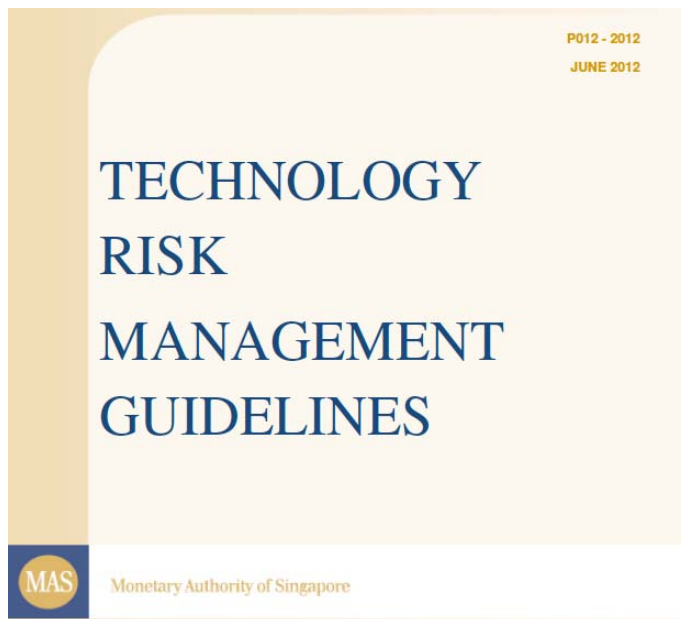
Sources: engadget, garethwright.com, Washington Examiner

# Mobile Security – Why

(iv)

To reach and satisfy their users, governments and enterprises are moving data and processes to mobile devices

→ Regulations and guidelines adjust



## b) Mobile Banking and Payment Security

Mobile banking and payments are extensions of online financial services and payments on mobile devices. Whilst mobile banking and payments face similar threats as those of internet banking and payments, Section 12.2 covers specific risks confronting the mobile security landscape and the importance of educating customers on security measures to protect their mobile devices from theft and loss as well as viruses and other malicious software.

# Mobile Security – Stakeholders



**“Empowering Business Users with mobile devices”**

→ Take the view of mobile app provider

# Mobile Security – Stakeholders

- Why take the standpoint of application providers?
- I thought business users all had managed, secure devices.



# Mobile Security – Managed Device Approach

**Managed approach is to apply and enforce policies and standards on a platform level:**

- Corporate devices issued to employees
- Policy enforces
  - Automatic locking, authentication (pass code length etc)
  - What 3<sup>rd</sup> party apps can be installed (if any)
  - Etc.
- 3<sup>rd</sup> party SW provides
  - Antivirus
  - Remote lock/wipe
  - Jailbreak detection
  - Etc.



# Mobile Security – Managed Device Approach

## Disadvantages of the managed device approach:

### 1. It doesn't protect against all risks

- E.g. remote-wipe will only work if the device is online

### 2. It's not feasible in many situations

- Apps provided to clients/partners
- Apps provided to citizens/residents
- Companies which wish to support BYOD
  - Not possible to enforce any policies or guidelines!

# Mobile Security - Application Security Approach

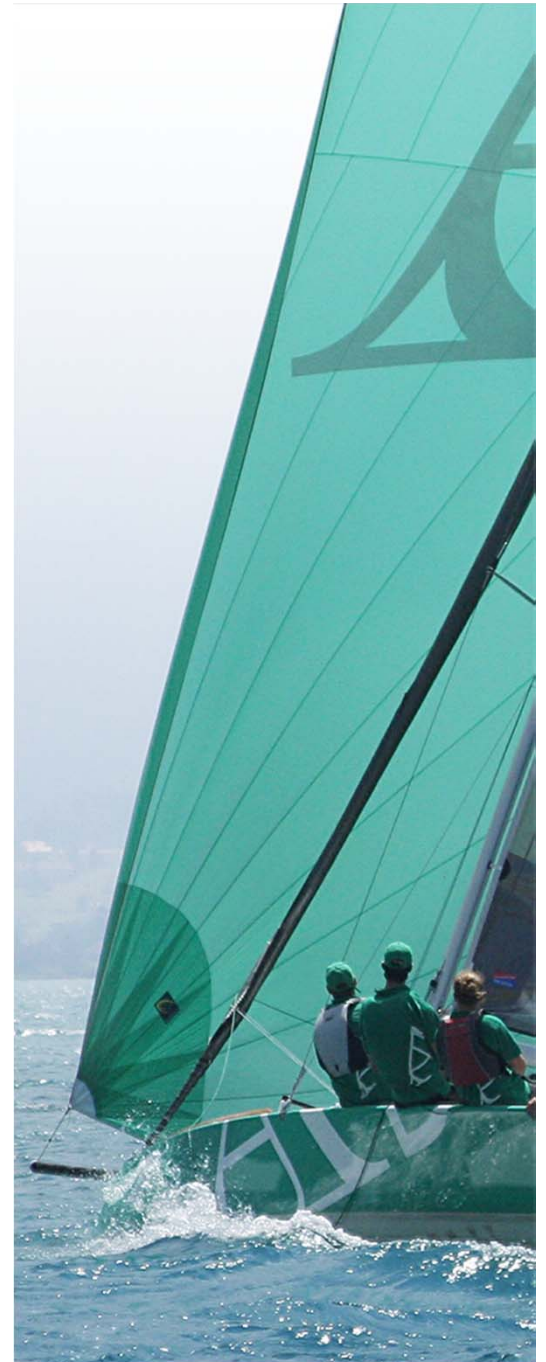
- **Assumes the device can be compromised**
  - And doesn't try to rectify this
- **Focuses on securing the app instead**

**This is the reality for many providers of applications**

- **Mobile banking and trading**
- **Social media**
- **Mobile ticketing**
- **Skype**
- **Etc.**



# IT Risk and Security Intro



# IT Risk and Security – General Principles

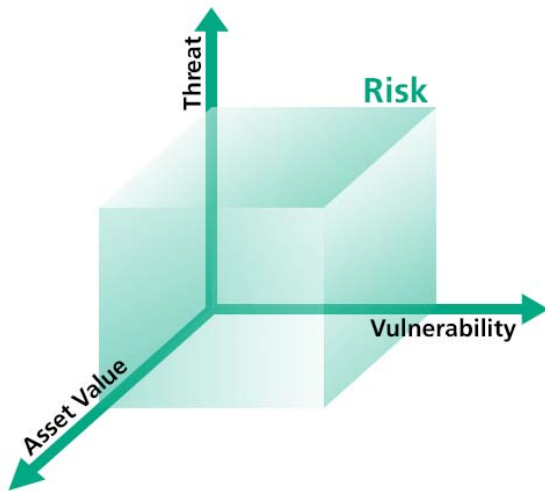
**Risk = (probability of the accident occurring) x  
(expected loss in case of the accident)**

- **Very simple formula**
- **Often very complex to apply in practice**

# IT Risk and Security – General Principles

In the case of IT security, the formula is expanded to:

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Asset Value}$$



## Example:

Threat: Thieves could break into our office and steal our equipment

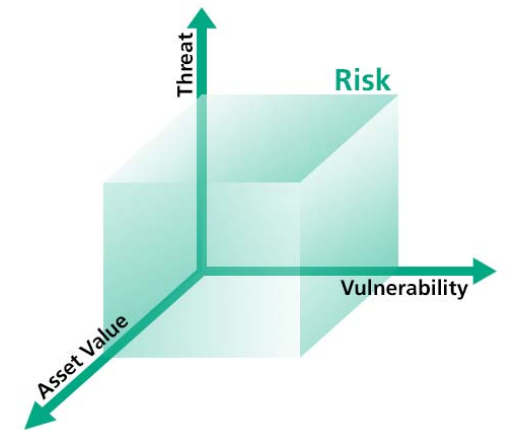
Vulnerability: The lock we are using on the doors is easy to pick

Asset value: See your balance sheet



# IT Risk and Security – General Principles

- **Identified risks can be**
  - Accepted
  - Transferred (e.g. insured or outsourced)
  - Mitigated (reduced) by applying controls
  - Avoided (e.g. not provided/implented)
- **Acceptable risk varies from person to person / corporation to corporation. Sector and regulation also have an impact.**
- **Control should not cost more than risk**



# IT Risk and Security – General Principles

## Example:

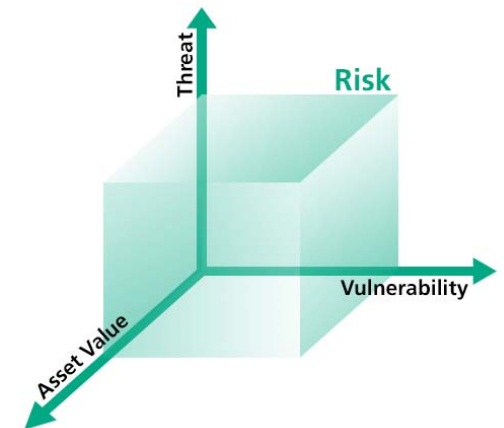
Threat: A pickpocket could steal my smart phone and gain access to sensitive data.

Vulnerability: My phone is not protected by a pass code.

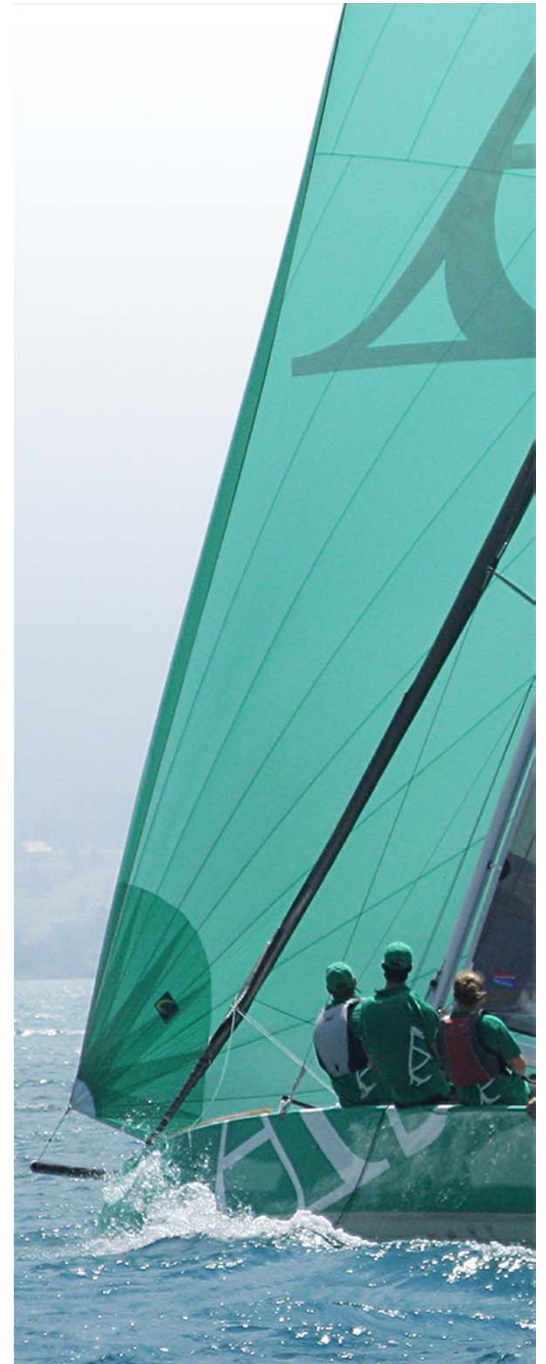
Control A: Set a pass code.

Control B: Don't store sensitive data on phone.

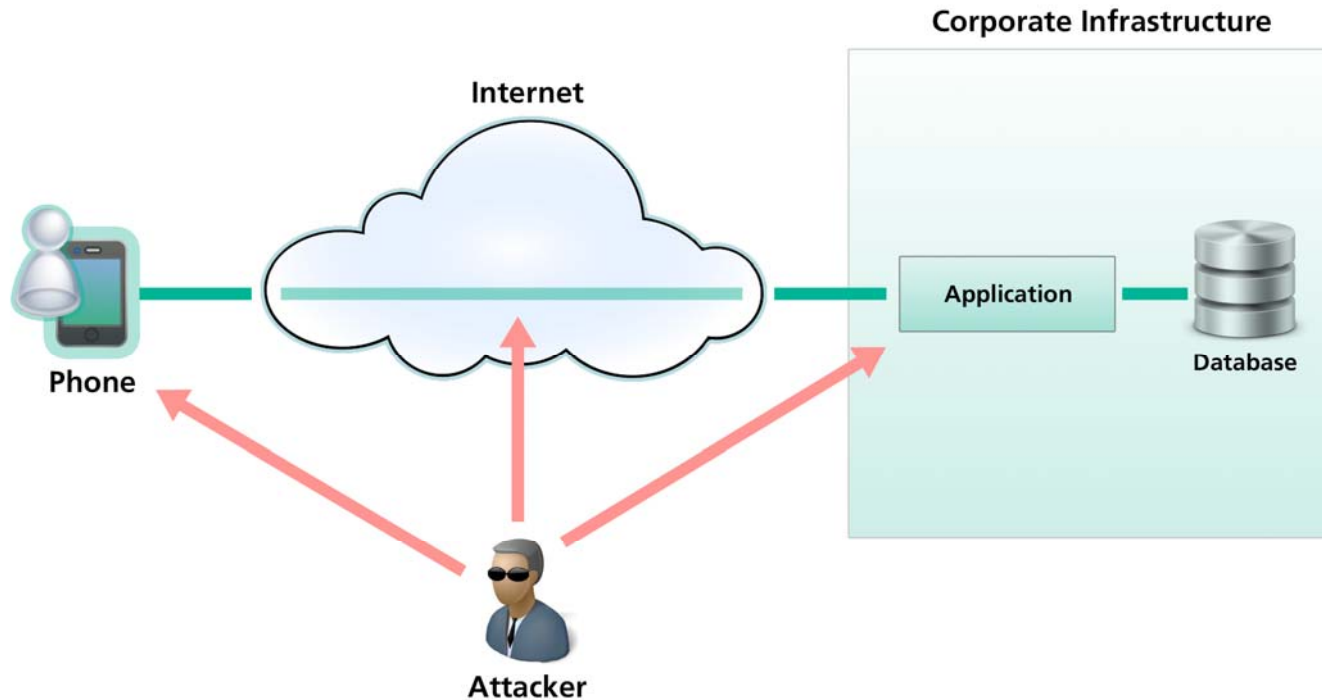
Control C: Always keep phone in office.



# Enterprise Mobile Security



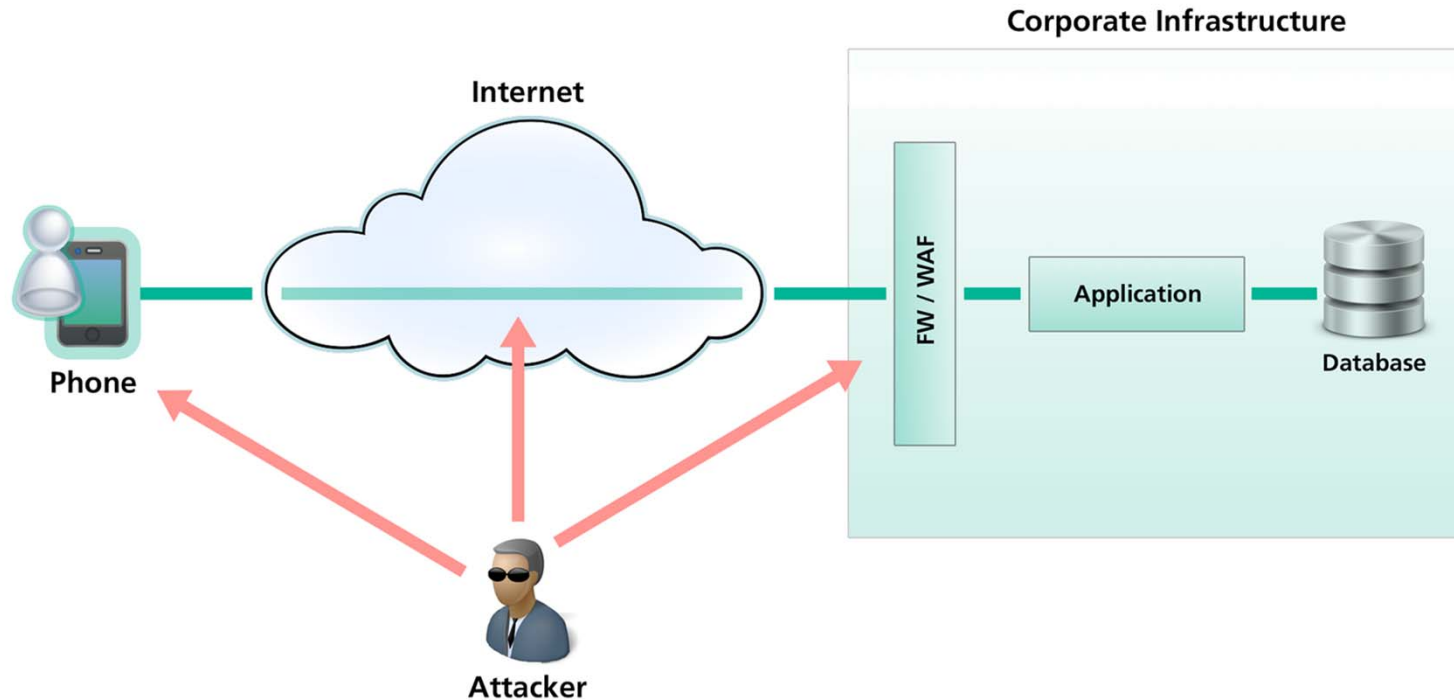
# Enterprise Mobile Security



Threats can be applied to the following components:

- Server-side application
- Communications channel
- Client

# Enterprise Mobile Security



- **Server-side application and communications channel:**
  - Identical threats, vulnerabilities and controls as in traditional applications
- **The differences are on the client!**

# Enterprise Mobile Security Differences (i)

Compared to traditional applications, the main security differences are:

- **Increased portability of device**
  - Higher likelihood of loss
  - Higher likelihood of it being stolen
  - Higher likelihood of someone viewing over your shoulder
- **Pass codes instead of passwords**
  - No proper keyboard makes entering passwords tedious
  - Far easier to brute force -> vulnerability





# Enterprise Mobile Security Differences (ii)

Compared to traditional applications, the main security differences are:

- **Expectations of users / willingness to accept security**
  - Always on, short attention span, fast interaction
  - Less acceptance by users of tedious, slow security controls
  - Enforce them and
    - Your app will not be used
    - User may find ways around (“I’ll just forward copies to my gmail account”)
- **New platforms and operating systems**
  - Each platform offers different security features and pitfalls
  - Features and pitfalls are different to ones on traditional platforms!
  - E.g. iOS take screenshot before app goes into background
- **Resources no longer an obstacle**



# Enterprise Mobile Security – Lost/Stolen Device (i)

**The biggest risk is losing or having your device stolen:**

- **Probability is high**
- **Potential damage is high**
  - All data exposed
  - Business logic exposed, e.g. proprietary algorithms
- **If the attacker knows what he is doing, device management software will not be able help**
- **If your app is running on non-managed devices, you cannot rely on pass code length or similar anyway**



## Enterprise Mobile Security – Lost/Stolen Device (ii)

- **Statistics are difficult to come by**
- **UK: Mobile phone is stolen in half of street crime**
- **Ireland: 6' 000 phones reported stolen Jan-July 2012**
  - Projected 10' 300 for whole year; population is 4' 500' 000; mobile phone penetration rate is 118%
  - Chance of 1:885 per inhabitant per year
  - Doesn't include lost phones, unreported thefts!
- **52% of Miami residents have experienced mobile phone loss and/or theft**
- **Quick poll in AdNovum's SG office:**
  - 55% have lost phone/had it stolen

Sources: National Mobile Phone Crime Unit (UK), Irish Times, Word Bank, Commission for Communications Regulation (IR), Lookout

# Enterprise Mobile Security – Doable?

- **Considering that**
  - Platforms are to be treated as vulnerable
  - Device management is to be treated as unreliable
  - So many phones are lost/stolen
  - Users won't accept tedious security measures
- **Can adequately secure mobile apps be implemented?**
- **In most cases: Yes**



# Enterprise Mobile Security – Basics

- **User awareness is critical**
  - Technical measures are never sufficient
  - Explain to and educate your user population
- **Enforce channel encryption**
- **Secure the server side**
- **Don't rely on security provided by platform/device**
- **Ensure your developers know what they are doing**
  - Best practices per platform
  - Reviews, guidelines, testing, awareness etc.

# Ensuring Devs Understand - Example

- iPhones and iPads capture the current screen when an app goes 'into the background' (swipe, home)
- The image is stored on the device
- It is not encrypted/protected by pass code



- Ensures smooth switching between apps
- Excellent for usability
- But what if my screen shows confidential information?
- Behaviour cannot be turned off or modified



# Enterprise Mobile Security – Approaches

- **Anonymise critical data before sending it to client**



- In many cases, certain contextual information is clear to the user anyway
- E.g. bank account details (e.g. account number, holder etc.)

# Enterprise Mobile Security – Approaches

- Use step-up authentication for usability



# Enterprise Mobile Security – Approaches

- Split tasks and require approval through 2<sup>nd</sup> channel



# Enterprise Mobile Security – Approaches

- Use a mobile-friendly 2<sup>nd</sup> factor authentication method
- May not be what you have in place



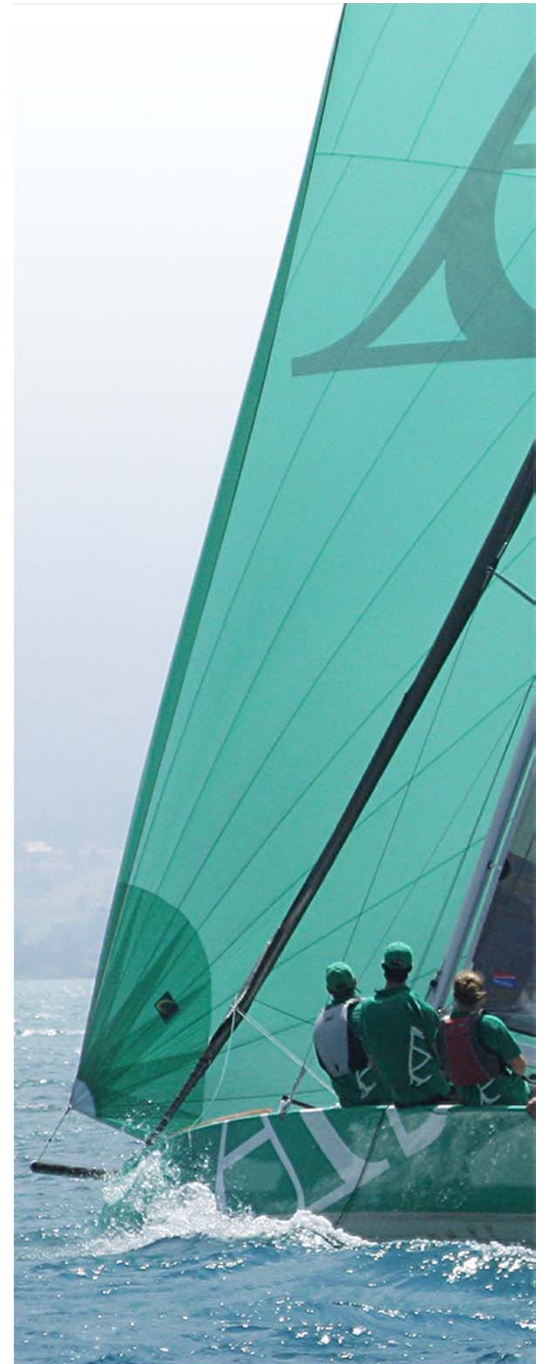
# Enterprise Mobile Security – Approaches

- **Don't cache critical data**
- **If you do cache critical data, encrypt it**
  - Using your apps own password/pass code
  - Not your own algorithm!
- **Keep confidential, proprietary algorithms on server**



3IEFtjyqCd96qF38sp9IQiJIKlNaZfx2GL  
?XefaYpbbAZ6z6Lk0Q+eE0XASe7aEEPfdx  
/9Ak4/0LnLiJRk05/2UNE5Z0a+3lcvITMm  
.Lem2/fQHZhGcQvkqZVqXx8SmNw5gzuvwj  
{CnmpR60V04rDRAS5uGL9fioSvze+q8Xqx  
}S+dzFDw5desMFS07JkecAS4NB9jAu9K+f  
.YcPrCn4s3Er iUgvL30zPR4P1chNu6sa3Z  
lJuQ530b9Tha FH8YcE/VqUFdw+bQtrAJ6N  
jLLQRPQdrmnWskKzn0Sarxq4GjpRTQo4hp  
}5nvkEkoIAjW5HaDKiJriuWldtN40XecWv

# Live Jailbreak Part 2





# Scenario

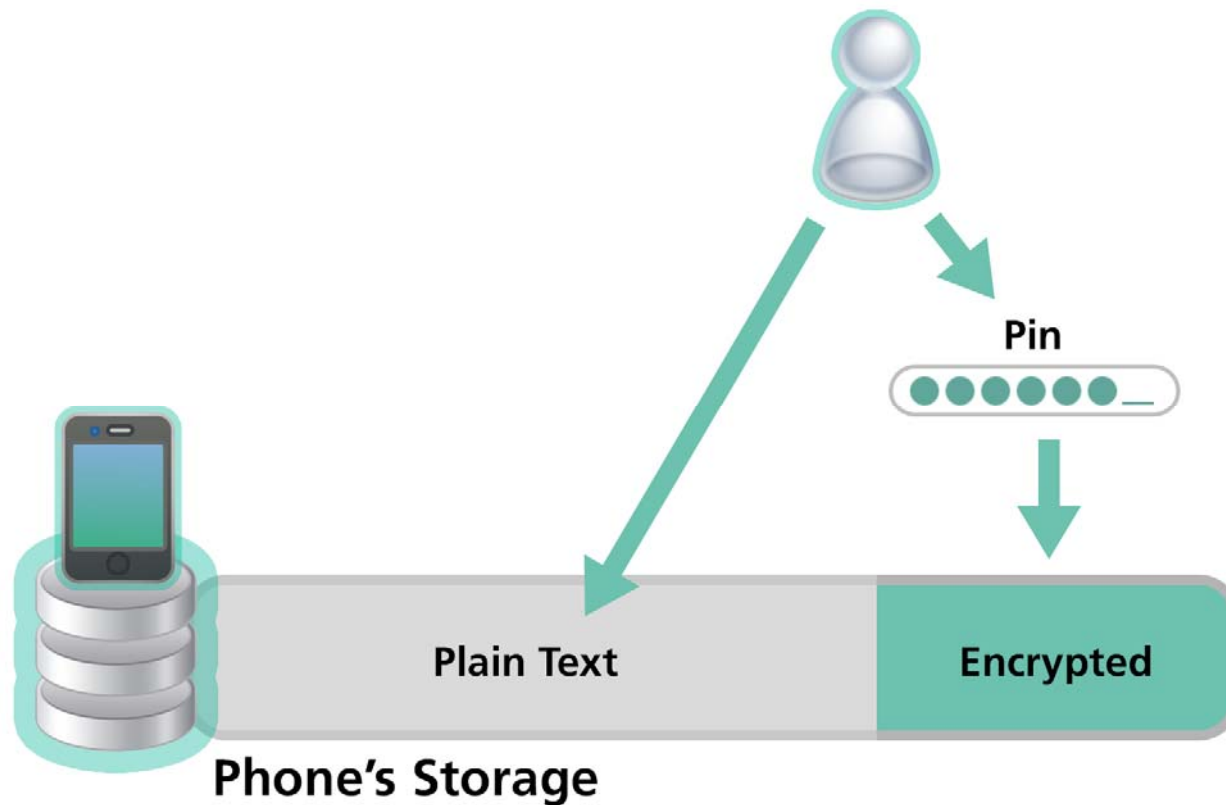
- iPhone or iPad running iOS 4.x/5.x/6.x
- Protected by pass code
- Borrowed/lost/stolen while turned off/locked
- To demonstrate how easy it is to access the data on the device

# Steps

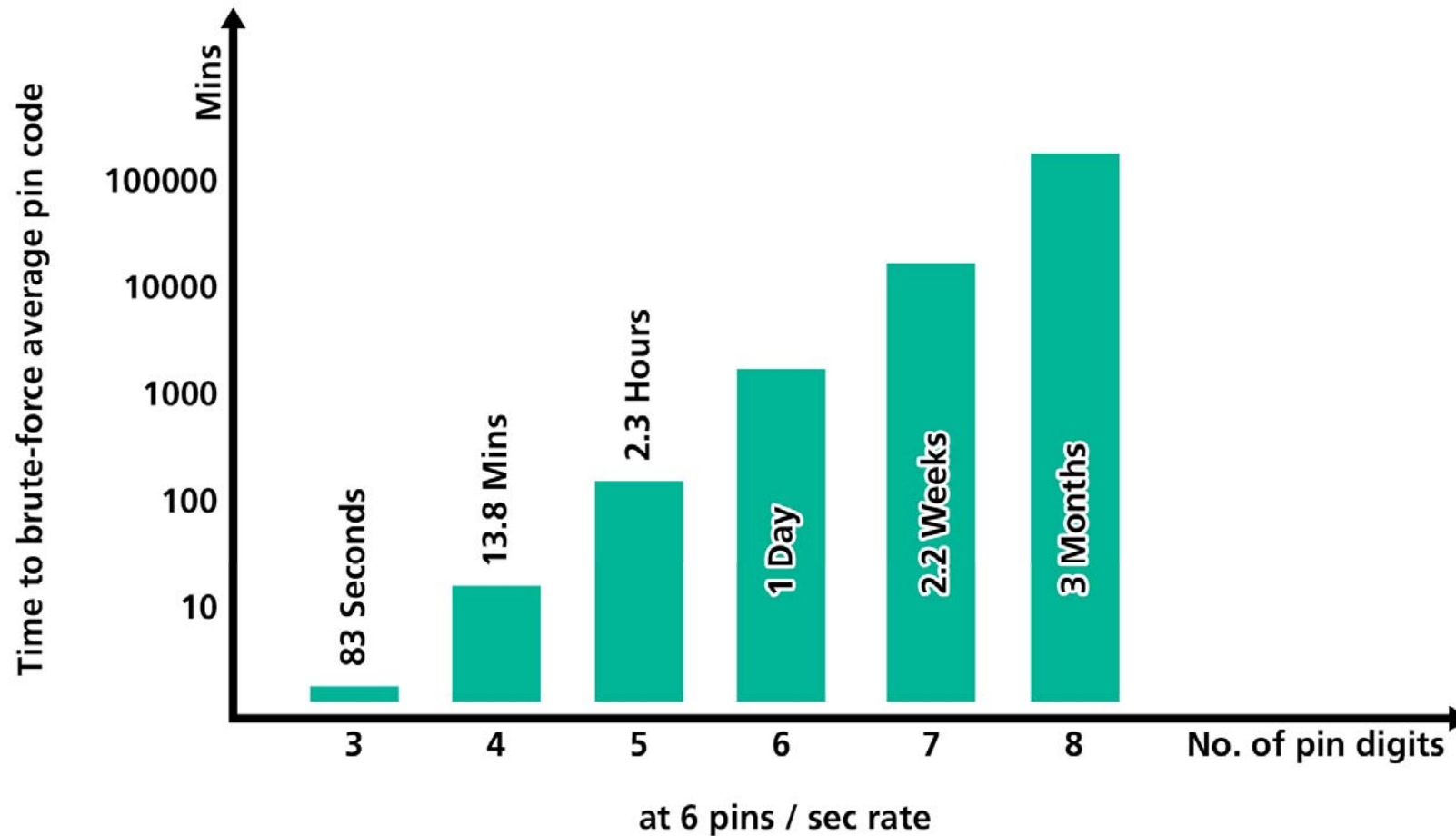
1. **“Jailbreak” the device**
2. **Transfer of all data to notebook**
3. **Browse unencrypted data**
  - Contacts, pictures, screen shots of running apps, etc
4. **“Brute force” the pass code**
  - “Brute force”: Try and try until we get the right one
  - Necessary for retrieval of the private key
5. **Browse encrypted data**
  - Which was protected by the pass code
  - User IDs and passwords of gmail, Facebook, Skype, Twitter
  - Wi-Fi passwords
  - Etc.

# Encrypted vs. Plain Text Data

- App (i.e., the developer) decides where data is kept



# How Long Will Your Pass Code Last?



Valid for iPhone 4. Source: AdNovum

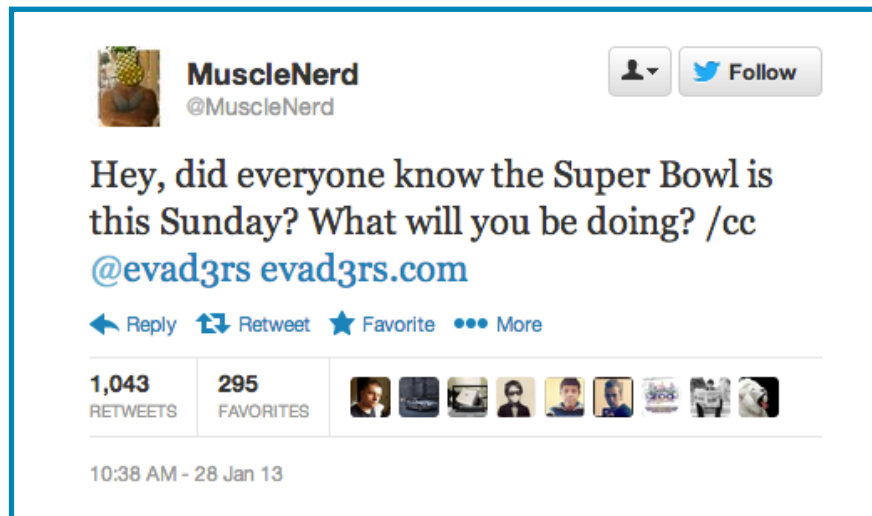
# iOS Jailbreak Chart

	4.3	4.3.1	4.3.2	4.3.3	4.3.4	4.3.5	5.0	5.0.1	5.1.1	6.0	6.0.1	6.1
iPhone 3GS												
iPhone 4												
iPhone 4S												
iPhone 5												
iPad												
iPad 2												
iPad 3												
iPad 4 & iPad Mini												

	Jailbreak-able
	Not jailbreak-able
	Not applicable

# iOS 6 Jailbreak

- Next jailbreak release this Sunday?
- All remaining devices will now be breakable?



# UBS Mobile Banking

## A Case Study

**Moritz Kuhn**

Principal Consultant

**Seet Teck Kiang**

Director for Sales & Business Dev.

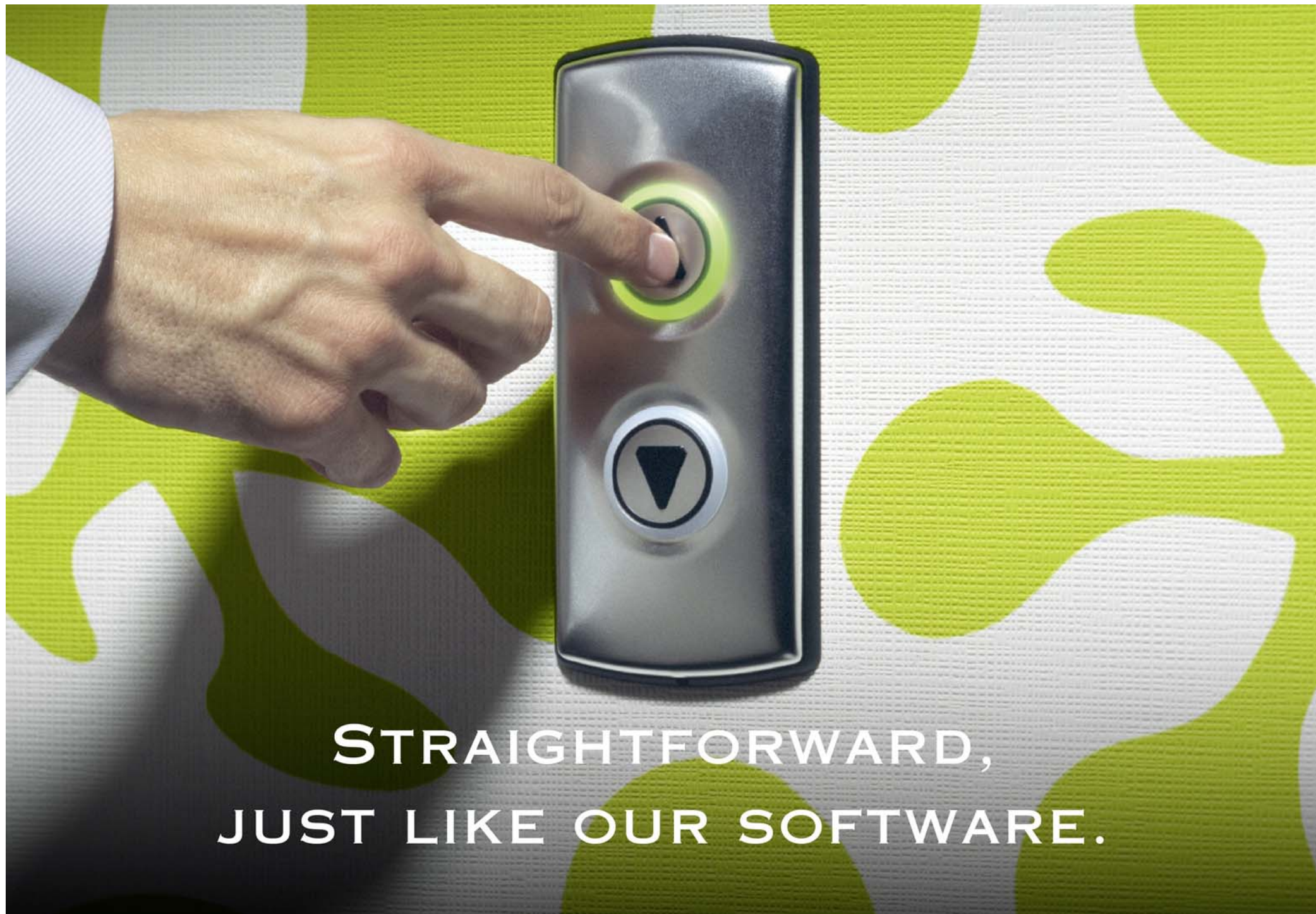
January 31, 2013



swiss made  
software







**STRAIGHTFORWARD,  
JUST LIKE OUR SOFTWARE.**

# Speakers



- **Moritz Kuhn**
- **Principal Consultant**
- **[moritz.kuhn@adnovum.sg](mailto:moritz.kuhn@adnovum.sg)**
- **Direct +65 6372 9511**
  
- **5 years industry experience**
- **Consultancy and project management**
- **Finance, e-health, government, telco**

# UBS Mobile Banking – Functional Scope

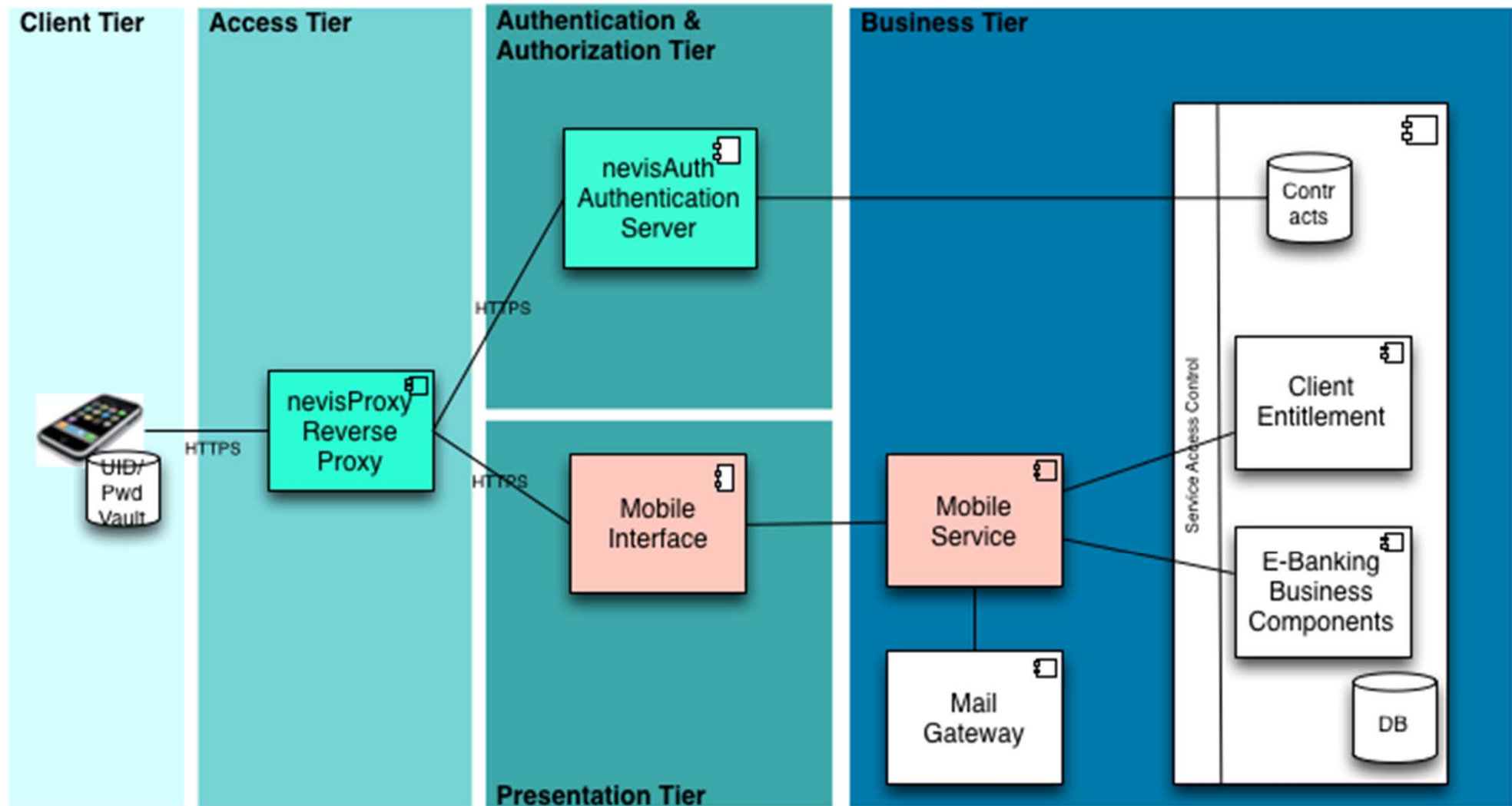


## Features

- Account balances
- Latest account transactions
- Portfolio overview by asset class
- Detailed information on individual custody account and portfolio positions
- Credit card transactions and amount still available
- Open credit card invoice amount
- Scanning of payment slips  
(optimized for iPhone4 and only for clients domiciled in Switzerland)
- SMS Pull: query the account balance by SMS, authenticated by mobile number

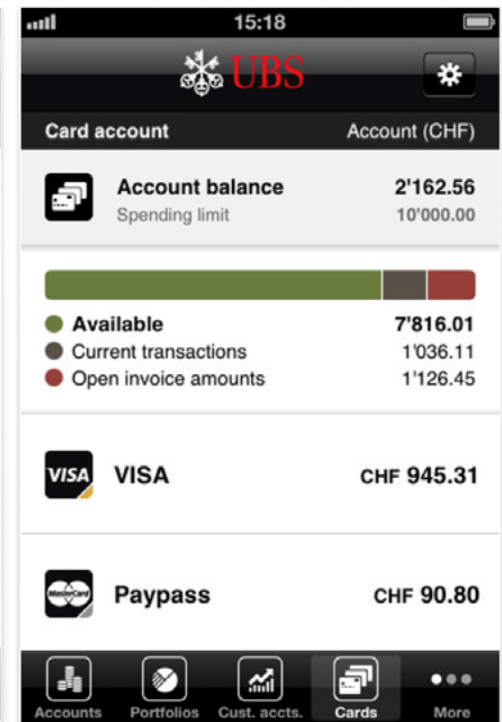
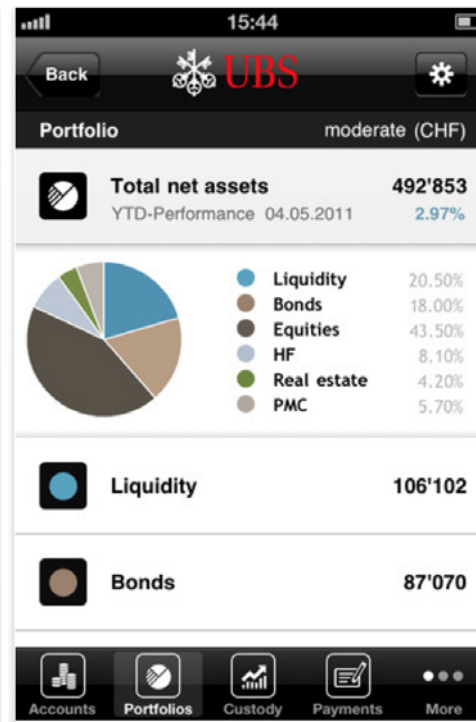
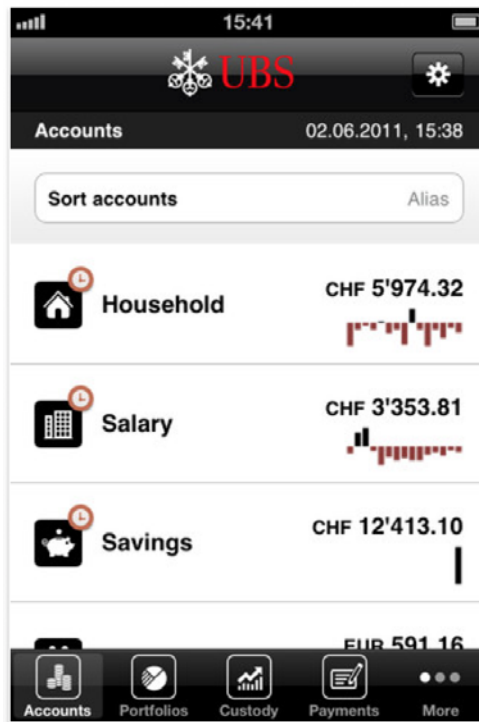


# Mobile Banking Architecture

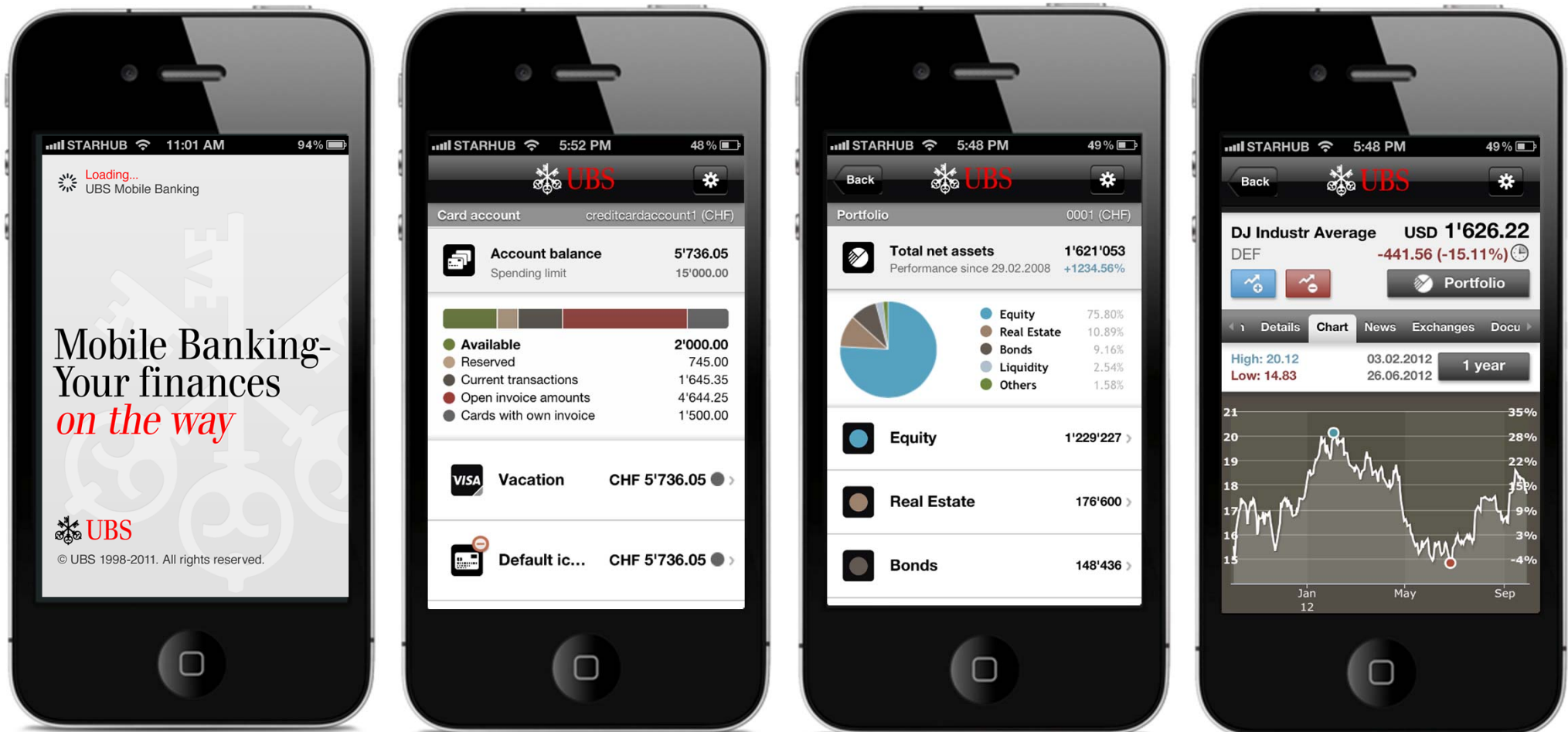




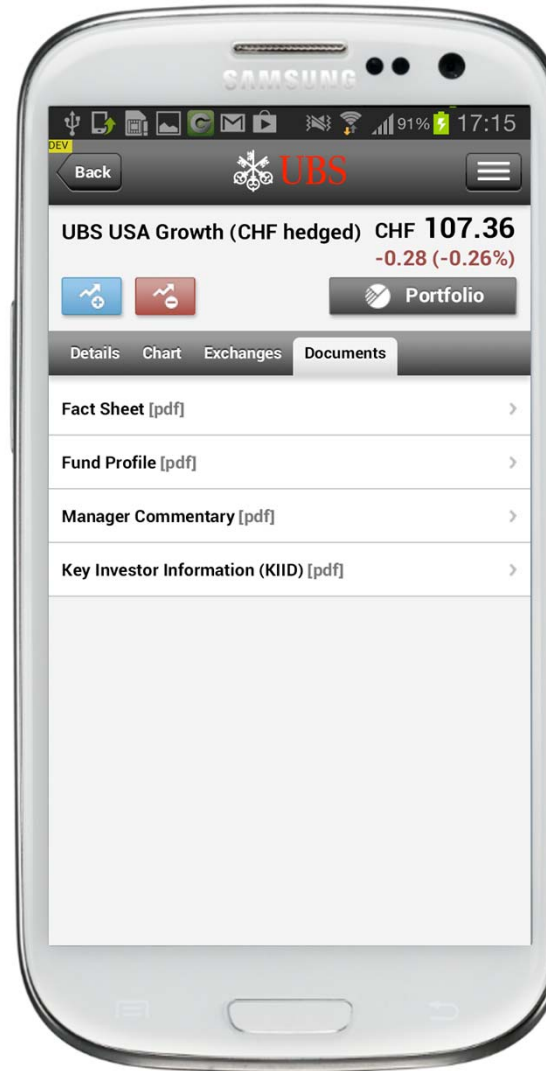
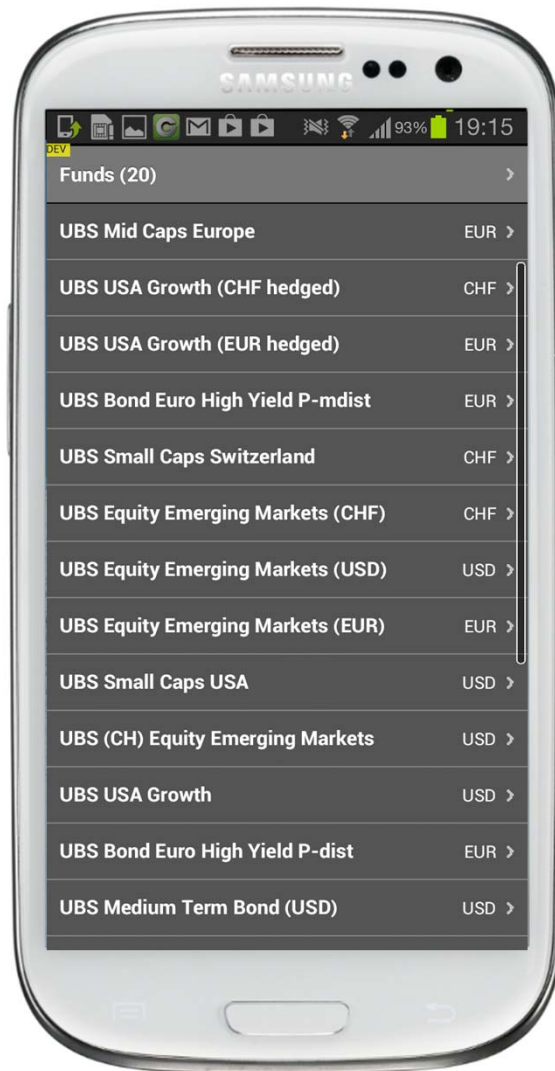
# UBS Mobile Banking – Demo



# UBS AG – Mobile Banking (iPhone)



# UBS AG – Mobile Banking (Android)

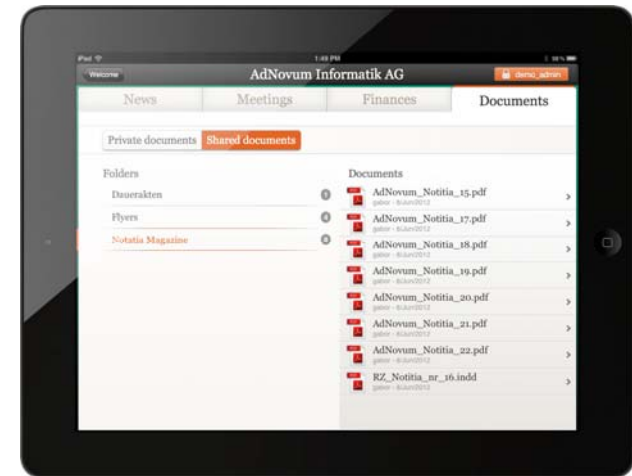


# DockPit



## Functionalities:

- Secure iPad app for board members
- Structured exchange of documents
- RSS feeds of company related news
- Fixing of meeting agendas and attaching its related documents
- Financial reporting documents for the financial year
- News, minutes, financial data, agendas
- Supports images, videos, PDF, Office documents



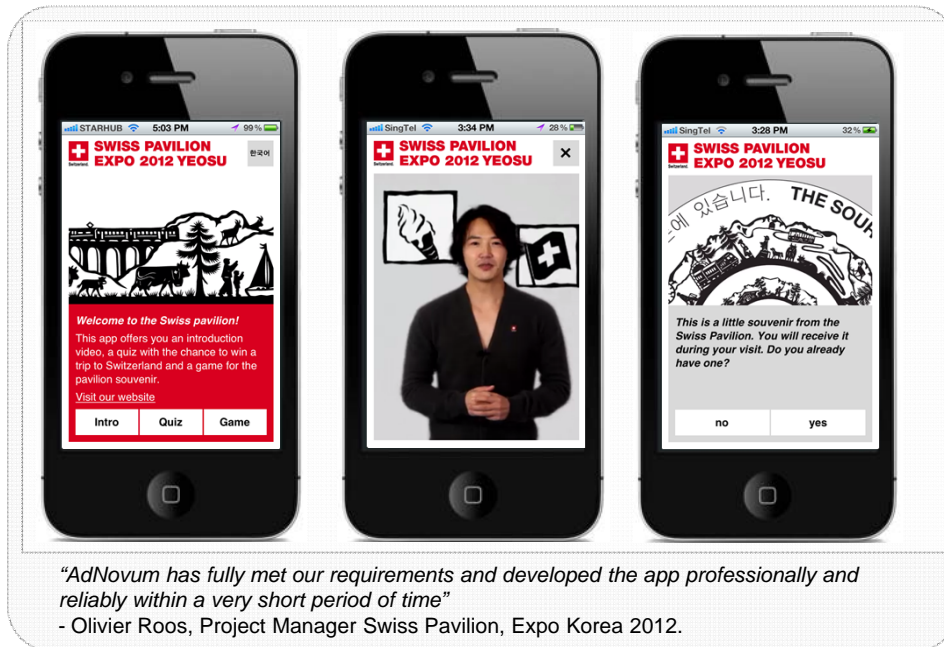
## Security features:

- Avoidance of all local document caching
- Full bi-directional data encryption (SSL)
- Automatic logout/screen lock
- Authentication by user ID and password
- Server-side protected by Nevis





# Swiss Pavillion Expo 2012



"AdNovum has fully met our requirements and developed the app professionally and reliably within a very short period of time"

- Olivier Roos, Project Manager Swiss Pavilion, Expo Korea 2012.

## About Swiss Pavilion Expo 2012 by FDFA

- Launched by the **Swiss Federal Department of Foreign Affairs** which is in charge of Swiss foreign relations
- The Swiss Pavilion Expo 2012 was held in conjunction with the Korean government to provide Switzerland an opportunity to strengthen its image in Korea and maintain important connections

## Objective & Scope

- The Swiss Game Yeosu is designed with the latest augmented reality and 3D Engagement capabilities in a game format to interact with potential visitors of the Expo exhibition in a fun and memorable way.

## Technological & Creative Involvement:

- AdNovum developed the technology design, R&D of advance visual functionalities, implementation, creative design and integration process.
- In the process, AdNovum has produced unique mobile functions that involve Augmented Reality, Visual Recognition, and 3D Engagement Capabilities

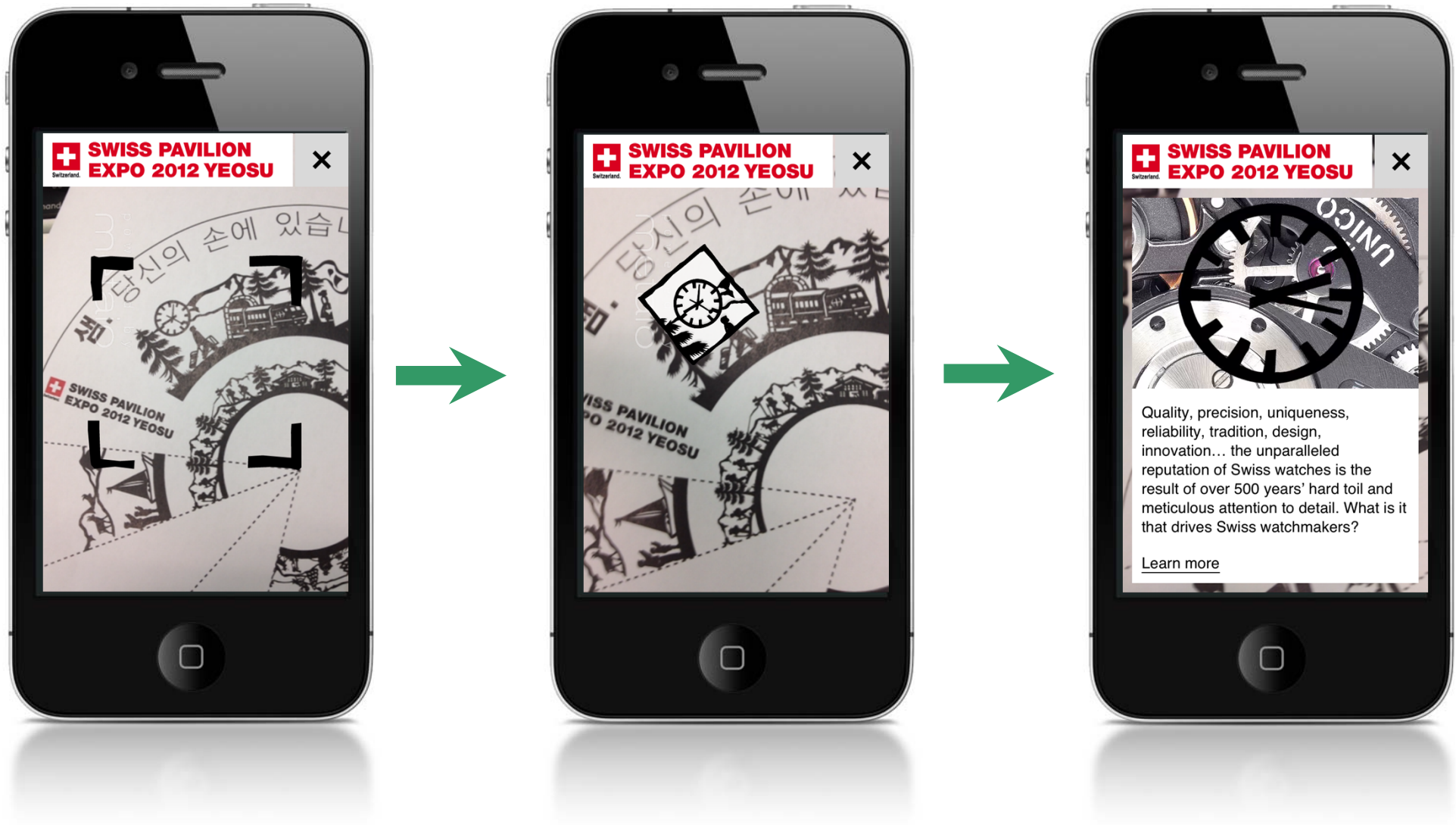
## Scope of Project:

- Project Name : Swiss Game Yeosu
- Value of Project: Sponsorship
- Platform: Hybrid Android and iPhone App (Framework on Metaio)
- Language support: Korean and English
- Duration of Project: About 1 calendar Months

## Benefits

- Launched from May to Aug 2012, the fun, creative games, quiz and advance visual features of the mobile app help showcase the Swiss brand of high-end technology and culture.
- Visual Recognition technology recognizes life imagery and actively engages the viewers in a fun way with their environment.
- Good application that ***integrates advance mobile functions with a strong creativity and human centric design***

# Image Recognition (Smartphone Camera)



# Augmented Reality (Smartphone Camera)



# International Financial Organization

## Mobile App for Delegates



*"I would also like to thank you again for the wonderful job you and your team did, and also the unwavering support we got from you."*  
- Jyotsana Varma, Office of the Secretary

### About this International Organization

- HQ in Manila, the organization helps facilitate the economic development of Asian countries & improve lives of over 1.8 billion people.
- Supported by the UN, with over 2,900 staff across 59 countries with US\$ 21.72 billion in approved financing in 2011.

### Objective and Scope

- The mobile application was designed to provide a boost of interaction between the **4,500 delegates** and the Governors Annual Meeting Summit across an intense 4-day summit in May 2012.
- Advanced security and multiple platform supports are key priorities.

### Technological Involvement:

- AdNovum developed the technology concept, implemented the application, creative design and integrated it into the client's environment.
- Authentication is effected by AdNovum's security framework that is also used for the protection of delegates.
- Developed by AdNovum's Singapore developers.

### Scope of Project:

- Platforms: Range of smart phones and tablets
- Implemented using HTML5
- Duration of project: Less than 2 calendar months
- Subsequent release implemented for next Annual Meeting (2013)

### Benefits

- Launched in May 2012, the mobile application provided delegates with a convenient single point of access to all summit related information such as city information, program schedules embedded with interactive functionalities such as **live-polling, live-survey, video feeds and live-tweeting**.
- Delegates in audience can participate in panel discussions in real time.
- Delegate registration
- Secure profile management and intra-delegate messaging





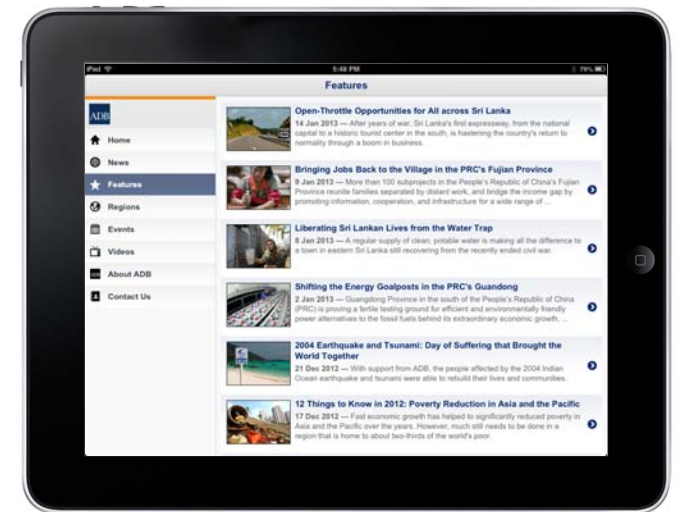
# International Financial Organization

Integration with Twitter, YouTube, Google Maps, RSS News Feeds



# International Financial Organization

## (Tablet version)



# Swiss Mobiliar Insurance

MobiAdvisor

- Client Advisory Application

**Die Mobiliar**  
Versicherungen & Vorsorge

- Top 3 Insurance Provider with 1.3 Million Policy Holders
- Bespoke mobile platform (tablet)
- Sales tool to equipped insurance advisors in conducting client meetings and deal closures

## Features:

- Navigation by customer categories
- Library of marketing documents
- Localization and segmentation of customers on Google Maps
- Interactive consulting tool based on XLS content and logic
- Calendar with managing customer-Dates
- Location based meeting planner
- Integration with CRM
- Digital signatory

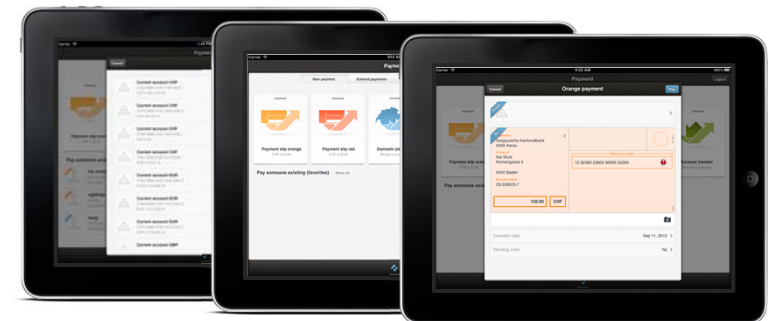


# Avaloq Mobile Banking

- Leading core banking solution
- Secure, bespoke mobile platform
- Platform allows Avaloq users (banks) to easily implement and customize transactional mobile banking

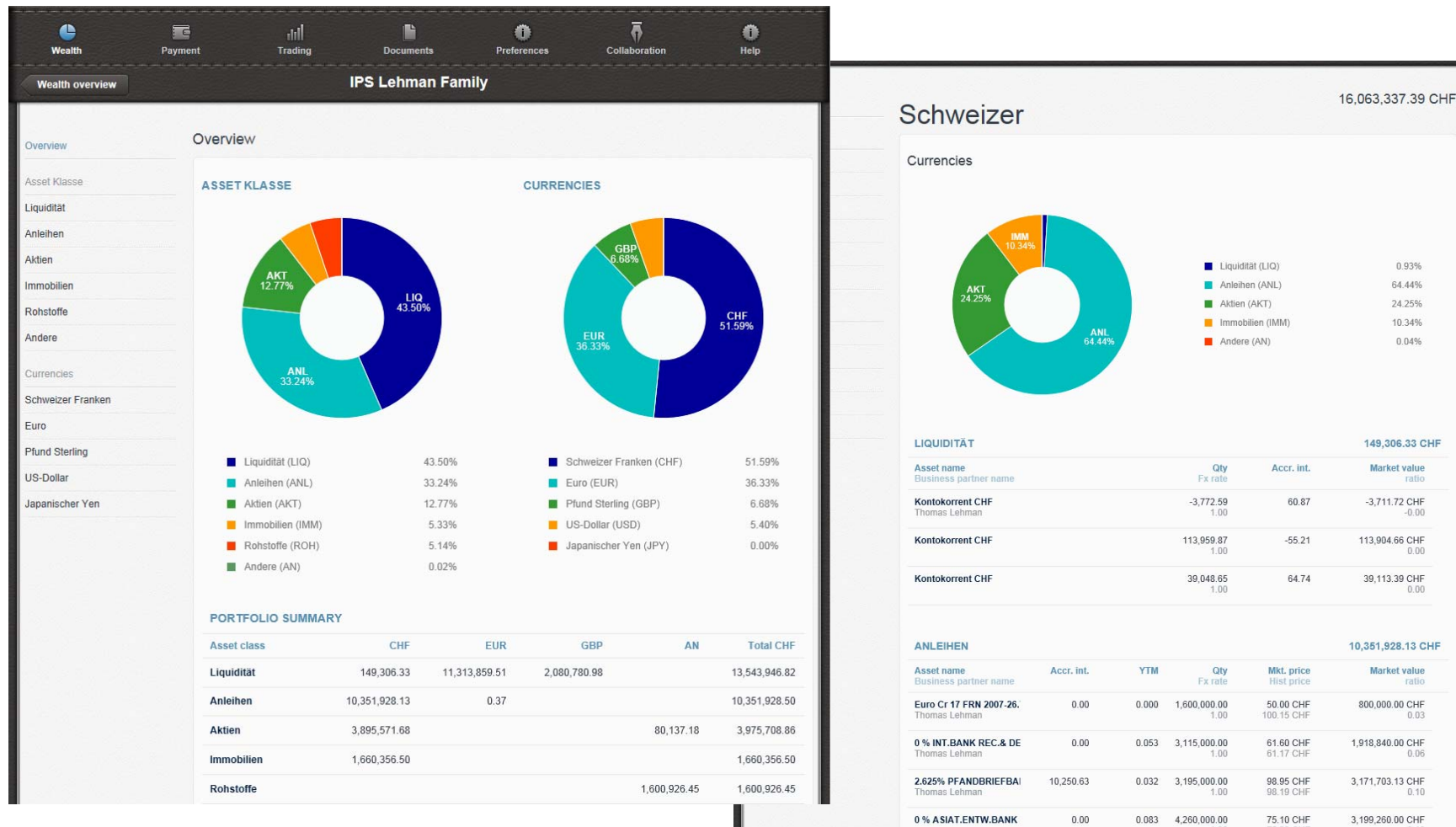
## Security features:

- **Multi-level security concept with step-up**
  - Single factor
  - Weak 2 factor
  - Strong 2 factor
- **Full bi-directional data encryption (SSL)**
- **Transaction signing**
- **Secure local cache**





## Demo Screenshots – Wealth Banklet



# Avaloq - Mobile Banking

## Demo Screenshots – Trading Banklet

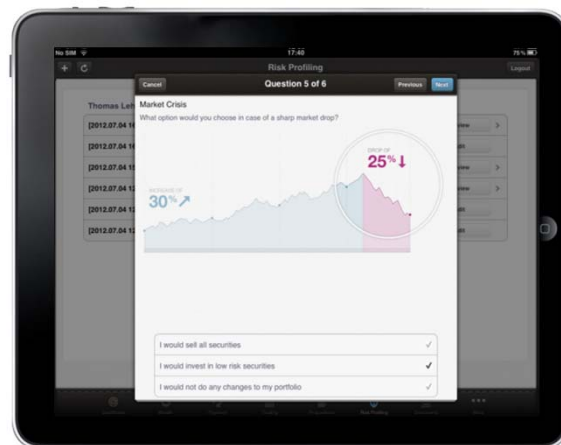
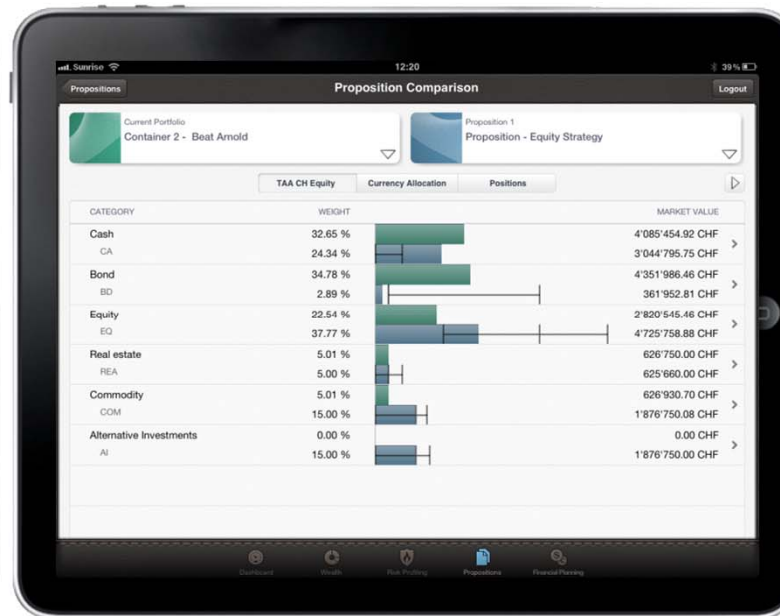
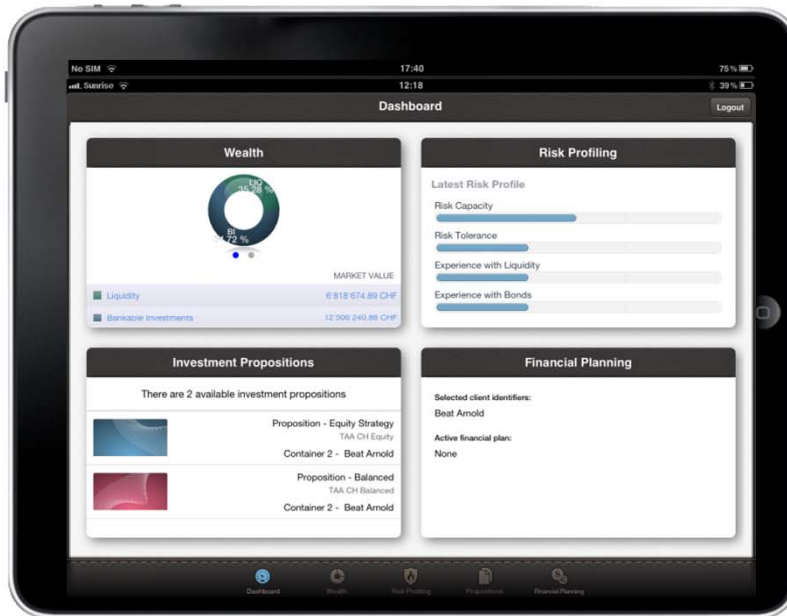
The image displays three overlapping screenshots of the Avaloq mobile banking interface, specifically the trading section.

**Top Screenshot (Instrument details):** Shows the 'Instrument details' screen for 'UBS N' (Namensaktie, ISIN CH0024899483, Listing XVTX / CHF). It features a line chart showing price movement from 23.09.2011 to 02.07.2012. The chart has tabs for Intra, 1W, 1M, 6M, YTD, 1Y, 3Y, and All. To the right of the chart, there are fields for Close, Open, Last, Bid, Ask, Range, and Change. A 'Buy' button is visible.

**Bottom Left Screenshot (Search):** Shows the search interface with a 'Buy' button at the top. Below it is a 'Title search' field with 'UB' entered. A list of search results is shown, including '2047256', '5447', 'UBSN', 'UBSN\_OLD', and 'UBS (Lux) Bond Fund Fcp - USD -A- Distr. (608428)'. Each result includes a brief description and a 'Buy' button.

**Bottom Right Screenshot (Buy equity):** Shows the 'Buy equity' screen for 'UBS N'. It includes a table with columns: Bid, Ask, Last, Change, Price (CHF), Order quantity, and Date/Time. The table shows data for 9/21/12. Below the table, there are input fields for 'Order quantity' (set to 100), 'Estimated market value (CHF)' (1,216.00), 'Execution type' (Limit), 'Order limit' (13.00), and 'Expiration date' (End of month). At the bottom, there are fields for 'Money account' (Kontokorrent CHF) and 'Portfolio' (Thomas Lehman 01). An 'Ok' button is at the bottom right.

# Avaloq - Client Advisory App



# How AdNovum Can Help You – Mobile



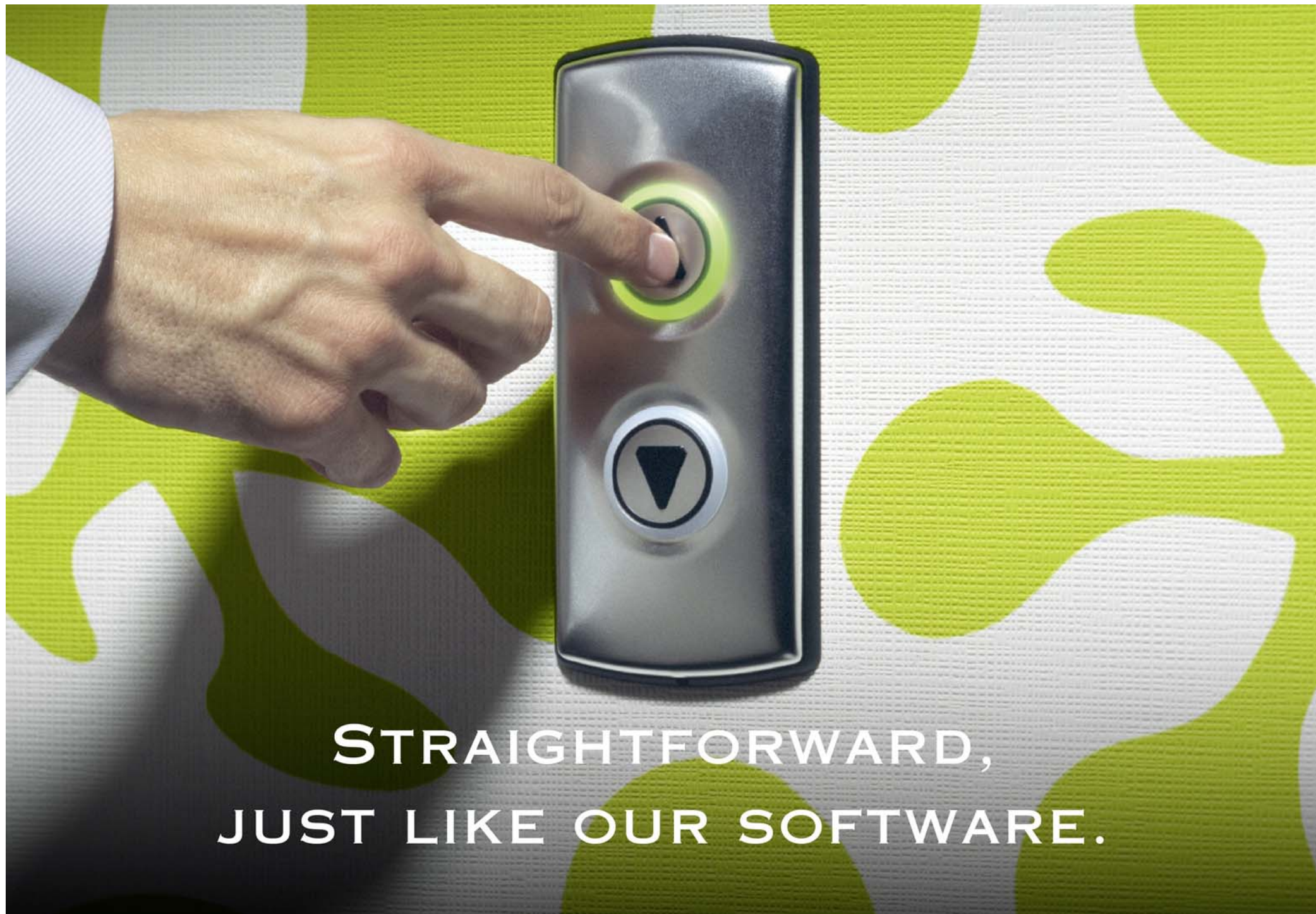
To date, there are approximately 800'000 users of our mobile enterprise applications (which have high-end security requirements) across banks, corporations and government agencies.

Our mobile development hub is based in Singapore and tapping on our extensive mobile enterprise experience, we are pleased to offer the following services:

- Design, Implementation, Delivery
  - End-to-end implementation of mobile applications (cross-platform)
    - iOS, Android, Blackberry, Windows 8
    - Smart phones and tablets
  - World-class user interface/experience design
  - Coverage of all security requirements for compliance & regulations
  - Integration with backend systems
- Consultancy
  - Workshops
  - Proof of concept (PoC) and prototype development
  - Requirements engineering
  - Architecture
  - Security reviews and penetration testing







**STRAIGHTFORWARD,  
JUST LIKE OUR SOFTWARE.**

AdNovum Singapore Pte. Ltd.

72 Anson Road, #07-01 Anson House, Singapore 079911

<http://www.adnovum.sg>, [info@adnovum.sg](mailto:info@adnovum.sg)

Main +65 6536 0668, Fax +65 6536 9267

