Mobile software security
Building trust in mobile apps
More use of mobile devices

53%

Of polled smartphone users say they use their device to pay online - 2014

26

Times per month for mobile apps usage against less than twice a month for a branch visit for the average customer - 2014

1.91B

>2B UNITS

Forecast of smartphone shipment from 2015 to 2017

Forecast by Forecast Analysis: PCs, Ultramobiles and Mobile Phones, Worldwide, 4Q15 Update

Building trust in mobile apps
But more mobile threats

“Fraud is increasing on channels like mobile”

“Expanding list of devices and channels through which consumers are becoming accustomed to transacting.”

“The volume of malware targeting users of mobile devices grew more than three times in 2015, compared to 2014. The most dangerous threats in 2015 were ransomware, malware capable of obtaining unlimited rights on an infected device, and data stealers, including financial malware”

Mobile threats: “android malware landscape similar to Windows”
Industries need to protect their online resources and IP

- Protection of their mobile apps with a lack of control of their consumers’ devices on the field
- Protection of their mobile apps whilst reaching a maximum number of end users, through their smart phones
Individuals need to protect their data

- Personal data in case of device theft or malwares
- Their online resources
Mobile software security, the players

**BROWSERS** provide built-in security features and libraries for developers

- HTML 5
- JavaScript
- CSS

**DEVICE MAKERS** protect their OS with built-in security features and they provide encryption tools for developers

**THIRD PARTIES** provides multiple means to protect mobile apps, through Software Development techniques

- HTML 5
- JavaScript
- CSS
Mobile software development techniques to allow app to:

**DEFEND**
- Reverse engineering, privacy and Intellectual Property (IP) protections to protect apps programming code, personal data and licenses
- Integrity of apps
- Authentication of users and devices

**DETECT**
- Unsafe environment in the mobile phone

**REACT**
- Stop execution or send an alert to a risk management back-end server

Through software development techniques and cryptography
Mobile software security at work

Software Development
Design of mobile app security solutions

Approval process for submitting apps to OFFICIAL APP STORES

User enrolment & app usage

Self-protecting mobile app

Apple Store
Google play
Mobile software security, a layered approach

Security layers

- NOTIFICATIONS TO RISK MANAGEMENT SERVER
- STRONG USER AUTHENTICATION
- SECURE ENVIRONMENT DETECTION
- PROTECTION OF APP INTEGRITY
- PROTECTION AGAINST REVERSE ENGINEERING
- ENCRYPTION

Depending on what is at stake, multiple security layers can be added, increasing the level of security.
Examples of other security solutions which can enhance mobile software security

- **Trusted Execution environment (TEE)** provides a trusted environment in the main processor of a mobile device:
  - Trusted User Interface (Trusted UI)
  - Storage of sensitive data, such as fingerprint
  - Execution of Trusted Applications (TAs)
  - Owned by OEMs (through Trustonic)

- **Secure Elements** from Secure Element Issuers (SEI)
  - Storage of sensitive data
  - Secure Execution of Applications
  - Multi-tenant SIMs, owned by MNOs
  - eSE, owned by OEMs
Mobile security solutions assessment

Regardless of their types, security solutions should always meet end-user convenience.
Mobile software security is a broad topic that covers other elements: back-end/cloud security, network security and also, a network of more and more connected objects, such as wearables and automotive devices.

There is no unique method to protect apps in unsecure environments, but rather an addition of security layers which can increase the overall level of security.

Mobile software security can be combined with hardware-based security solutions:
- Reinforcement of sensitive data storage and integrity of service execution in hardware zones

Security solutions should always include end-user convenience when they are designed.
Gemalto mobile security solutions support multiple security frameworks to deliver best-in-class digital security and facilitate service deployment in a fragmented mobile market. We are also involved in the definition of international standards for digital security.

We support multiple industries, including Banks, Enterprise, Transport, MNOs, OEMs, Government…, globally

From traditional case studies such as m-Payment, m-Banking, m-Ticketing, we are now seeing a trend towards mobile ID with government-led initiatives such as digital driving license.

Contributors
Rémi de Fouchier, Vice President, Marketing Communications, Gemalto
Didier Benkoël-Adechy, Marketing Communication Manager, Gemalto
Carl-Eric Codere, Technical Product Manager
Guillaume Pierquin, Product Marketing Manager, Gemalto
Thank you