Dr. Jassine Boulkheir

International Sales and Marketing Manager

ybo@bit4id.com

About BIT4ID

Established in 2004 with headquarters in Italy, Bit4id was born to make simple, secure and consistent technologies for authentication, digital signature and encryption. In the last ten years we have affirmed ourselves in many countries both in Europe and outside Europe, having a direct presence in Spain, Portugal, England, Poland, Macau and Peru.

With our new DNA based on PKI technology, every company or service provider can implement the digital identity in a simple, straightforward and scalable way to meet new challenges…

Agenda

From Mobile First to Mobile Only

Growth of the global mobile

- More Online Activities Performed on Mobiles than PCs
- Simplicity and ubiquity, mobile advantages

PKI and Mobility

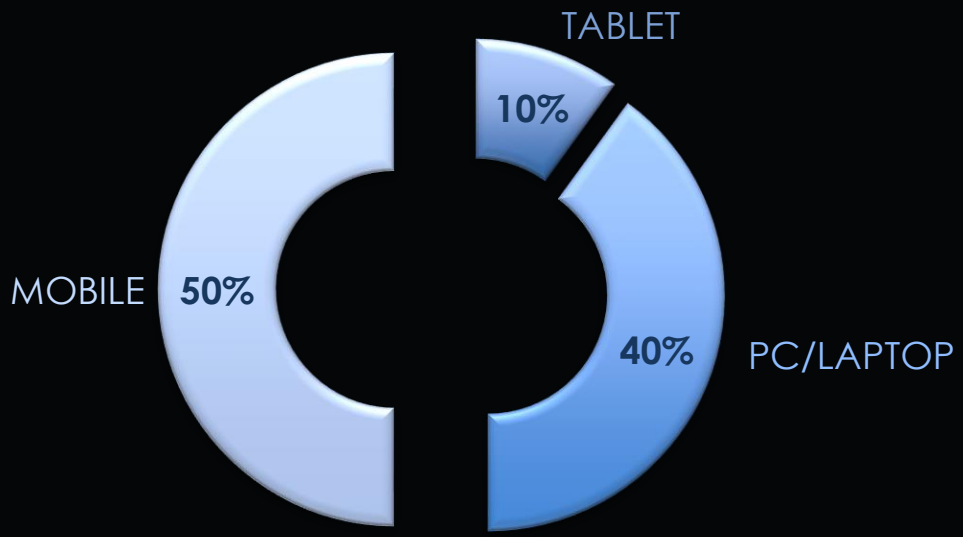
- State of art
- Mobile concerns
- How is addressed PKI on smartphones

DigitalDNA

- Wearable approach
- One single app for securing my life
- Use cases

More Online Activities Performed on Mobiles than PCs

Average number of online activities among internet users



Question: in the past month, which of the following things have you done on the internet via any device? **Source:** GlobalWebIndex Q2 2017 | **Base:** 72,529 Internet Users aged 16-64

Growth of the global mobile workforce

Employees are moving toward smaller, more portable devices and tablets, wearables and ultrabooks are expected to be the primary work devices by 2020

IDC predicts the US mobile worker population will hit 105.4 million by the year 2020, which is approximately 73% of the US workforce

73%

Gartner reports that 70% of mobile professionals will conduct their work on personal smart devices by 2018

70%

DigitalDNA

PKI and Mobility

State of art

DigitalDNA

PKI and Mobility

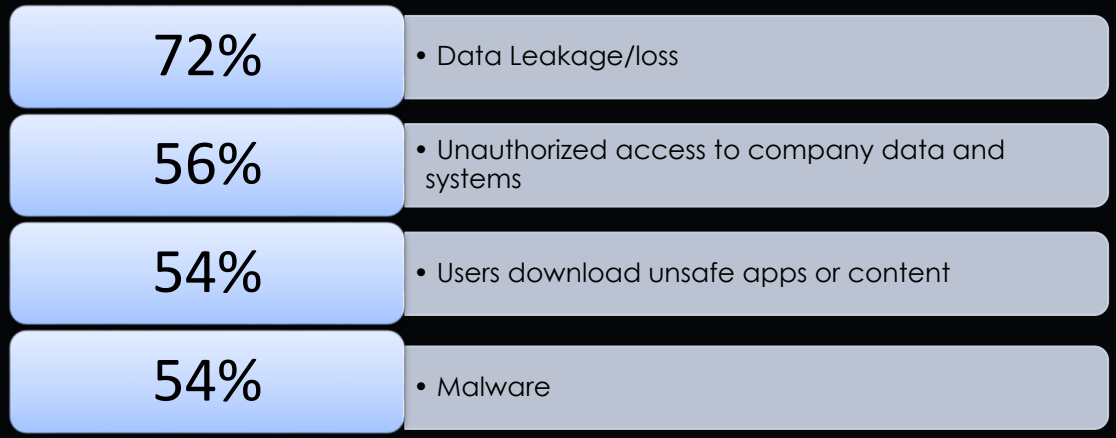
Question?

Whats About security???

DigitalDNA

Mobile concerns

According to a survey of 800 Cybersecurity Professionals, the main security concerns related to BYOD are:



DigitalDNA

1 in **5**
had suffered a mobile security breach

How to address PKI on Smartphones

Where can I store my digital identity, secret keys and PKI certificates?

Native Keystore
Standard APIs

Proprietary
Containers/EMM

Secure Elements
TEE/eSE

Smart Card
NFC/c-LESS

Cloud Remote
HSM

DigitalDNA

DigitalDNA

Native keystore

Keystores are certificate containers

Advantages

- Quick & Easy to deploy - Multiple options to install a certificate
- Only way to enable native apps – default mail client

Disadvantages – A security nightmare

- All applications can access certificates and the private key (what you know is not required)
- Duplication of certificates
- Cost attached to a new certificate & cost management
- Security
- No legal value

DigitalDNA

DigitalDNA

Proprietary keystore

Proprietary keystores are mobile device management or enterprise mobile manager systems that use a combination of software technologies to «hide» credentials into one single application. Customers use a proprietary implementation or the Native keystore.

Advantages

- Increased security

Disadvantages

- Limited to the EMM applications & only some use cases
- Cost of the mixed solution
- Cost of the management
- No compliancy with national/international legal value scheme
- No legal value

Hardware protected keys

These are tamper resistant hardware components embedded into the mobile device, such as a TEE/eSe.

Used in **Apple Pay** and **Samsung Pay**

Advantages

- Increased security

Disadvantages

- Not on all the phones
- Cost of the mixed solution
- Cost of the management
- No open
- No legal value

DigitalDNA

DigitalDNA

Smart Card c-Less

This solution uses an NFC device that is external to the mobile

Advantages

- Highest possible security
- Keeps existing security / don't need to deploy a new solution
- Works on unmanaged mobile
- 2 factors
- Legal value

Disadvantages

- Works only with Android

Cloud secure element

(Remote HSM)

Questa soluzione utilizza HSM remoti per custodire chiavi private e certificati.

Advantages

- Centralized management
- Works on unmanaged mobile
- Server to Server integration
- Legal value

Disadvantages

- It works only with online systems
- It works mono Provider
- No interoperability
- Large number of digital identities (high value, target for hackers), Single Point Failure

DigitalDNA

The wearable digital identity

2 Factors but Wearable

Works with iOS and

Android thanks to BLE

PKI Use cases

With unique interface, ONE SINGLE APP for securing my life

In addition to authentication, PKI provides additional use cases, all of which can be combined into a single credential.

Logical / Physical Access

Email Encryption

Digital Signature
With legal value

Internet Authentication and safe browsing

Endpoint Protection
Mobile and desktop logon

Ciphered chat

DigitalDNA

Digital identity suitable for mobile devices

Your digital identity

always available in your pocket

Authenticate yourself

to online services with a stylish,innovative and safe device

DigitalDNA

Sign electronic documents

on the move, by using your mobile deviceor from your desk with your PC

DigitalDNA

DigitalDNA is an innovative and safe device, able to hold qualified digital certificates.
With it, users can authenticate themselves to online services and sign electronic documents on the move, very fast and easily, keeping their digital identity always available in a pocket.

DigitalDNA can be used on mobile devices with the proper APP (downloadable from the Apple Store or Google Play and on PC by installing the software client from the CD-Rom partition within the token.

www.bit4id.com

Yassine Boulkheir

ybo@bit4id.com