



Americas Summit

14 October 2015 New York

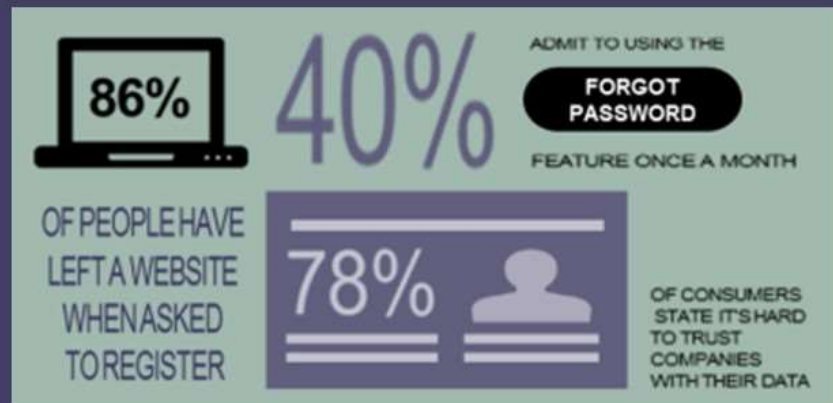
INTRODUCTION TO MOBILE CONNECT

ANA TAVARES LATTIBEAUDIERE



THE NEW STANDARD IN
DIGITAL AUTHENTICATION

USERNAMES AND PASSWORDS



INCOMPLETE TRANSACTIONS ESCALATING

It is vital for digital service providers to **reduce friction** and **increase loyalty** to maximise the number of successful transactions

69%

2011

72%

2012

74%

2013

Shopping cart abandonment is increasing as consumers shift to online and mobile shopping

UNIVERSAL LOGIN



Secure digital identity is now in our hands

ACCESS AND MANAGE YOUR BANK ACCOUNT

SHOP ONLINE AND MANAGE TRANSACTIONS

ACCESS YOUR PERSONAL HEALTH RECORD

MANAGE LOYALTY PROGRAMMES

AND MANY MORE....

IDENTITY THEFT, FRAUD

In 2013 Government documents/benefits fraud (34%) was the most common form of reported identity theft, followed by credit card fraud (17%), phone or utilities fraud (14%), and bank fraud (8%). Other significant categories of identity theft reported by victims were employment-related fraud (6%) and loan fraud (4%).



STRONG SECURITY

Simple Authentication

Choice of user experience:

- Seamless
- Click OK

Single factor = “something I have”

“Standard internet security” comparable to passwords and SMS one-time-passwords

(Level of Assurance 2)

Used to build a large base of enabled users

Two-factor Authentication

- Enter PIN

Two factors = “something I have and something I know”

Higher levels of security (Level of Assurance 3)

may allow premium authentication services

Strong Authentication

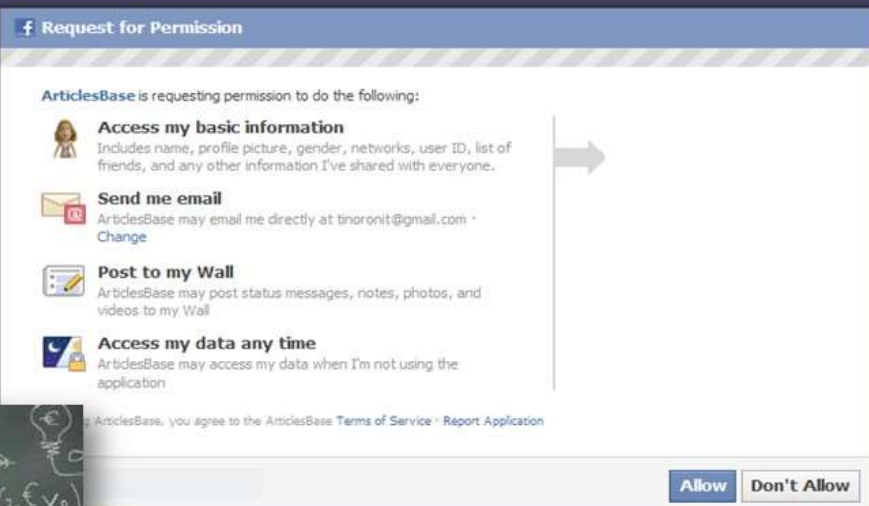
- Enter PIN
- wPKI encryption

Very high levels of security (Level of Assurance 4), including **non-repudiation** based on **wireless Public Key Infrastructure** (wPKI), requires crypto-SIM and applet



DO YOU REALLY NEED TO KNOW THAT?

TMI?



CONTROL OF PERSONAL DATA

Consumers expect digital services that are **secure** and want transparency on what information is being collected

61%

do not see enough value in online shopping to compromise their security

82%

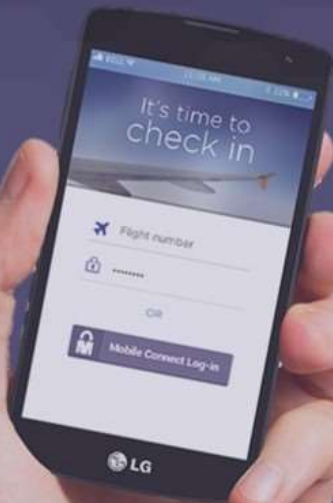
want transparency around when and what personal information is being collected

60%

however, are ok sharing personal data in exchange for deals and benefits

SERVICE DEMONSTRATION

Click to start



THE NEW STANDARD IN
DIGITAL AUTHENTICATION

ENHANCING CONSUMER ENGAGEMENT

Mobile Connect provides **simple, secure and convenient** access to online services, replacing the need for multiple usernames and passwords

It combines the user's unique mobile number and an optional PIN for added security, to **verify and authenticate** their identity



Using the **mobile as the authentication device**, user's can log-in to services from **a mobile, PC or tablet**, giving flexibility as well as security



Eliminates **consumer frustration**, reduces abandoned transactions and **drives more repeat business**



UNLOCKING MORE SALES REDUCING COSTS

Today, less forgotten passwords will **reduce operating costs** and ensure **less abandoned transactions**

In the future, attributes like **location** will improve the **user experience** and **further reduce** risk of identity theft, growing **loyalty, market share** and delivering **consumer insights**

Secure
data
verification

➤ **75%**

of consumers are interested in location being verified to their bank for easier use of their card abroad

Lower
operating
costs

➤ **30%**

of support calls are for forgotten passwords at an average cost of \$70 each to reset

\$4tn

the value of
abandoned
transactions in 2014

➤ **63%**

of which is potentially
recoverable by savvy
online retailers





Questions

