SIM Authentication : a first step towards Mobile ID ?

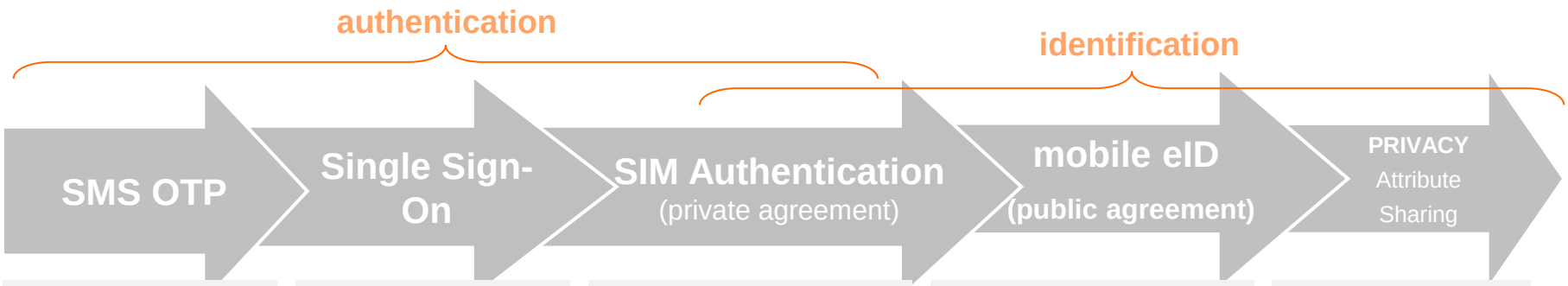
GSMA Mobile Identity Programme Kick-Off



France Telecom Orange | Group Marketing Innovation | Olivier Massière

September 18, 2012

OVERALL ROADMAP : from mobile Single Sign-On to Authentication to mobile ID



- Mobile phone used as an identifier
- Mobile network used by third party identity providers

- Operators are providing Identity credential management themselves

- Complementary to Single Sign-On services
- Added layer of security
- Trusted identity provisioning through private agreement

- Legally binding identification
- Official use cases made possible
- Universally trusted identity provisioning

- User-centric identity management
- Different level of information sharing with each service provider

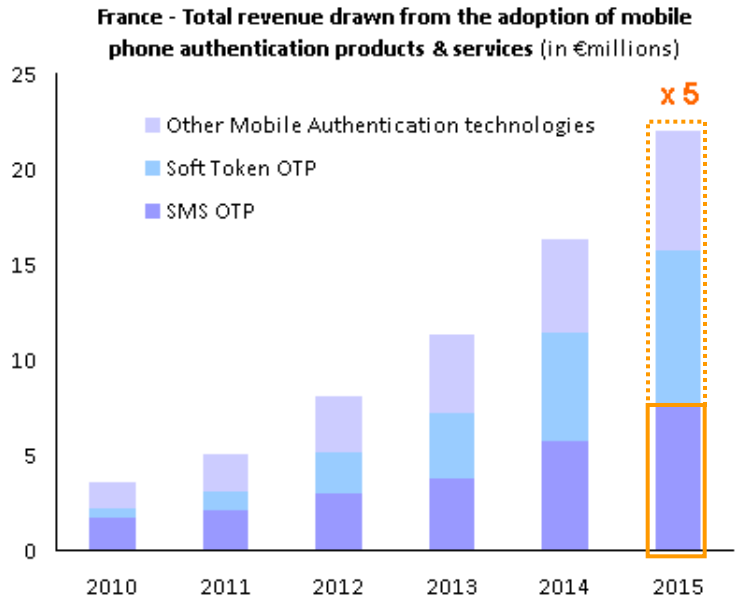
Operators take control of the identity management

Operators leverage their assets to add value to their service

Morning discussion

Mobile authentication market

market potential



Other Mobile Authentication technologies = mobile PKI, voice, Transaction Authentication Number and Biometrics

Soft Token = mobile application

Source : Goode Intelligence, mSecurity 2010 series, Data derived from EU forecasts (taking into account GDP, Internet and mobile penetration)

MNO services

SIM Card : mainly network authentication, some WKPI

Mobile Applications : mainly OTT

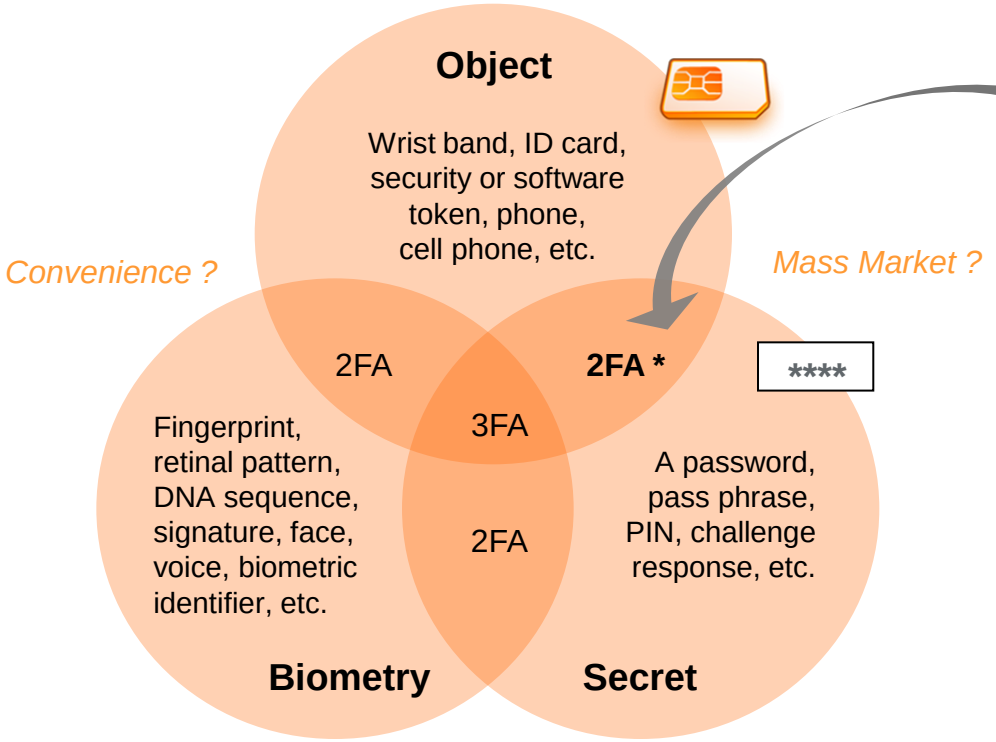
Wholesale SMS for OTP
- increasing volume ?
- decreasing value ?
- service evolution ?

Orange Vision : from mobile Authentication to mobile ID

Unitary Value	Services	Usage example	Requirements	Stakeholders
Manage your Privacy attributes	▪ Only Share specific personal data (age, gender) while protecting privacy	▪ Account opening for online gambling ▪ Orange Digital Coach	$$$ ▪ Enrolment in shop ▪ Paper ID verification ▪ Issuance of a mobile certificate ▪ Certificate renewal policies ▪ SIM card exchange (46Kb Applet)	Regulators, CNIL
ID verification & Legal Signature	▪ Prove your identity (name, age, country, address, social security number) ▪ Sign a contract with legal value	▪ Access e-Government services ▪ Vote for elections ▪ Sign an insurance contract agreement		Governments
Authentication (B2B2C risk management)	▪ Access a web service ▪ Validate a transaction	▪ Access a bank portal ▪ Confirm a wire order	$ ▪ Remote enrolment ▪ Light SIM applet (5Kb)	Private Sector

design to costs

SIM-Based 2FA *



* 2FA = Two-Factor Authentication

MNO solution : Personal Code attached to the user SIM Card



Push message
challenge <> response

Key success factors

KSF	Target	Effort required
Universality	100% of Mobile Users eligible Multi-Operator, inc. MVNO	**Select standard solution with interoperability capabilities**
Critical Mass	Multiple Service Providers Large User Base from day one	**Recruitment via a first mass market service, Partnerships**
Cost	Competitive cost based on Transaction or Active User	**Design-to-cost, flexible pricing models**
Ergonomics	Simple enrolment & usage	Keep it simple. Favour online subscription and self-care
Security	3DSecure label EU qualified signature	Lobbying
Deployment	Minimal integration & deployment effort	Integrate through standard interface with existing ecosystems
SLA	Offer clear warranty on service availability, latency, retry policy	Business as usual

Solution architecture & value chain : financial services example

🇫🇷

10

- Service logic
- Risk Management
- Fraud detection, scoring
- Auth. method selection

Service **P**rovider (Bank)

2

- Broker (simplify)
- Advisor (influence)

Technical **I**ntegrator

4

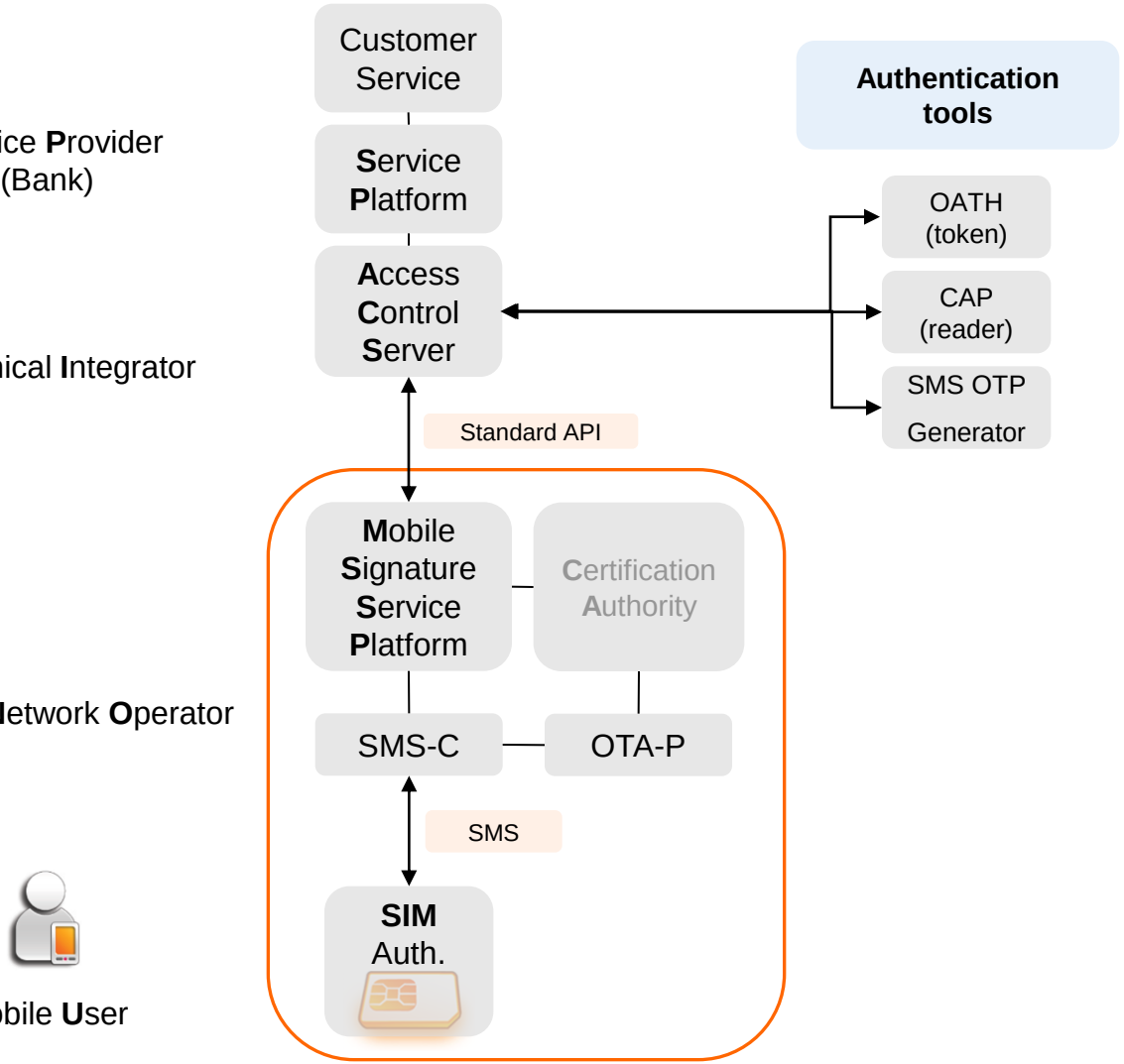
- Eligibility & enrolment
- SIM / PIN Management
- Secure communication
- Traceability & storage
- Message Customization
-Transparent Portability
- …

Mobile **N**etwork **O**perator

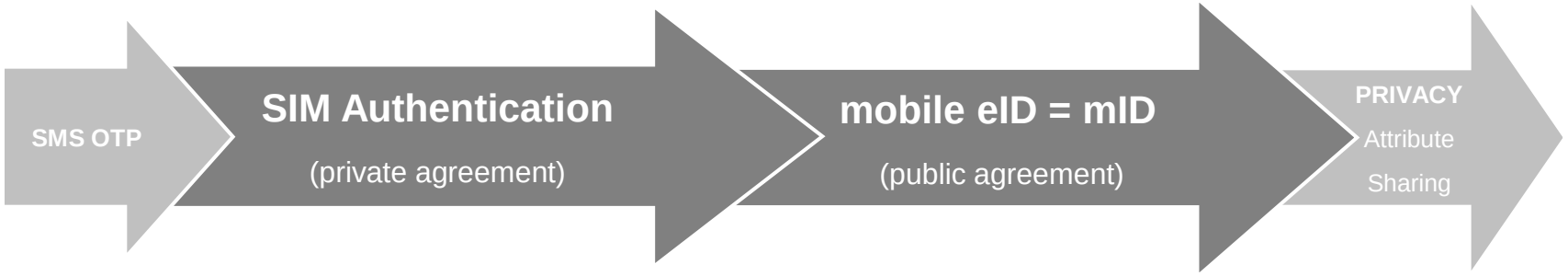
60M

- Personal Code & Device

Mobile **U**ser



Wrap-up



User input	▪ 4-digits personal code attached to a personal object : a stable user experience	
Services	▪ Access a web service ▪ Validate a transaction	▪ Sign a contract with legal value ▪ Prove your Identity
Technical	▪ (U)SIM, 5KB applet downloadable OTA	▪ (U)SIM, 50KB applet, EAL4+, crypto.
Process	▪ Remote enrolment & service association	▪ Strong enrolment in shop, ID check

Step by step service roll-out

End users	▪ Create a large user base & user habits leveraging on operators' services
Partners	▪ Recruit Service Providers & build a trusted ecosystem with Technical Integrators
Form Factor	▪ Position the SIM card early on as a preferred form factor
Brand	▪ Position Mobile Operators as trusted references for secure Authentication as a Service

First mover's assets



Olivier MASSIERE

Marketing

olivier.massiere@orange.com



Matthieu VERDIER

Technical

matthieu.verdier@orange.com



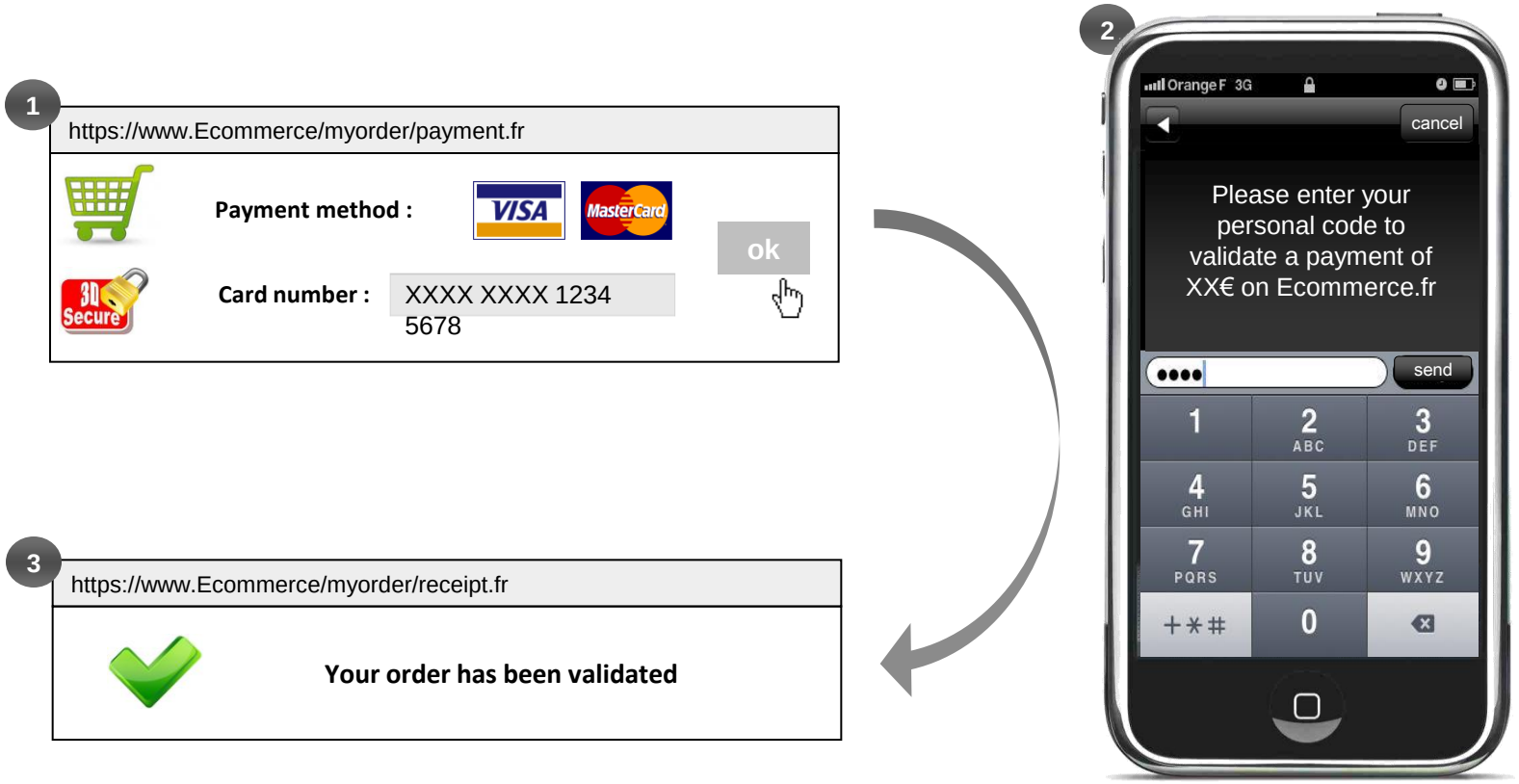
Thierry BARBA

Orange @ GSMA

thierry.barba@orange.com

thank you

Customer Journey on PC (similar for mID & SIM Authentication)



validation **request** generated from the web

[any **connected device**]

personal code **confirmation**

[**device with SIM**]

Customer Journey on mobile (similar for mID & SIM Authentication)

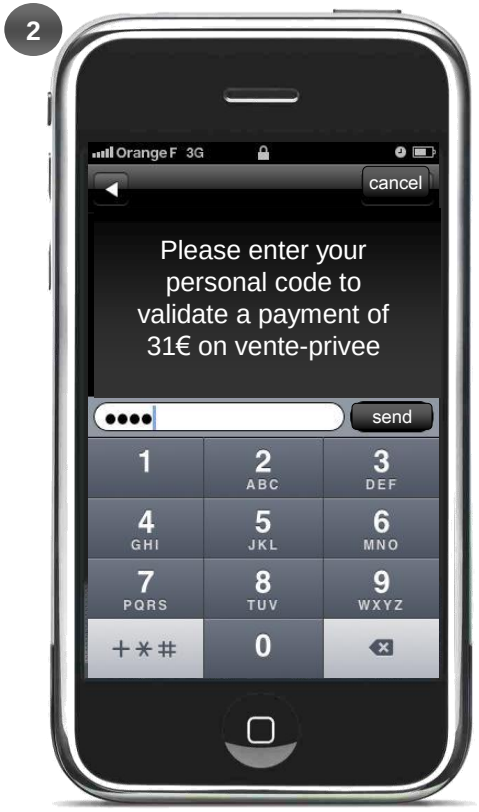
1



selection of a payment option (or authentication method for an access)

[Mobile Web browser]

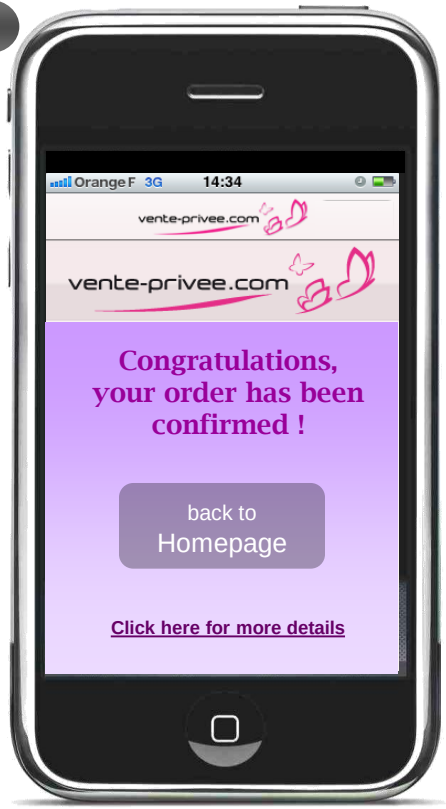
2



personal code **confirmation**

[SIM menu pop-up]

3



notification that the transaction was successfully carried out

[Mobile Web browser]