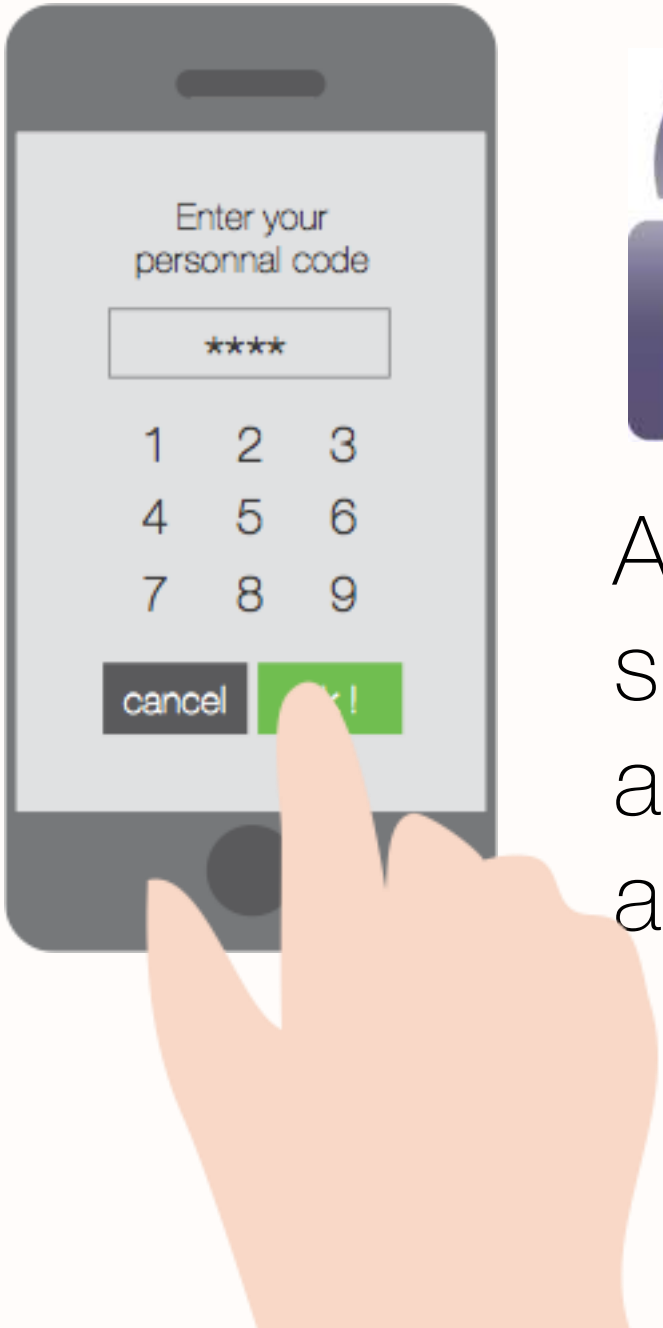


mobile connect

A universal, simple and safe authentication service

Orange | Innovation Marketing & Technology
Décembre, 2014

Digital ecosystem challenges … and pains

- Our everyday digital experience is made of
  - Using webservices for many different purposes (facebook, amazon, leboncoin …)
  - Buying from the internet in the more possible secured way
  - Accessing governemental portals (tax paying …)
  - Accessing Operator's self-care portals

But all stories always starts with the same ritual : authenticating !

- Then the « authenticating dilemma » and the 2 possible choices :
  - « I want it simple » :
    - Always the same password (rather trivial, most of the time), and same ID
    - Great to log in, but risky and with dramatic consequences once i'm hacked
  - « I want it safe » :
    - Different (complex) passwords (and possibly different IDs) for each service
    - I fear nothing anymore now … but i often juggle with the « send me back my pasword » option !

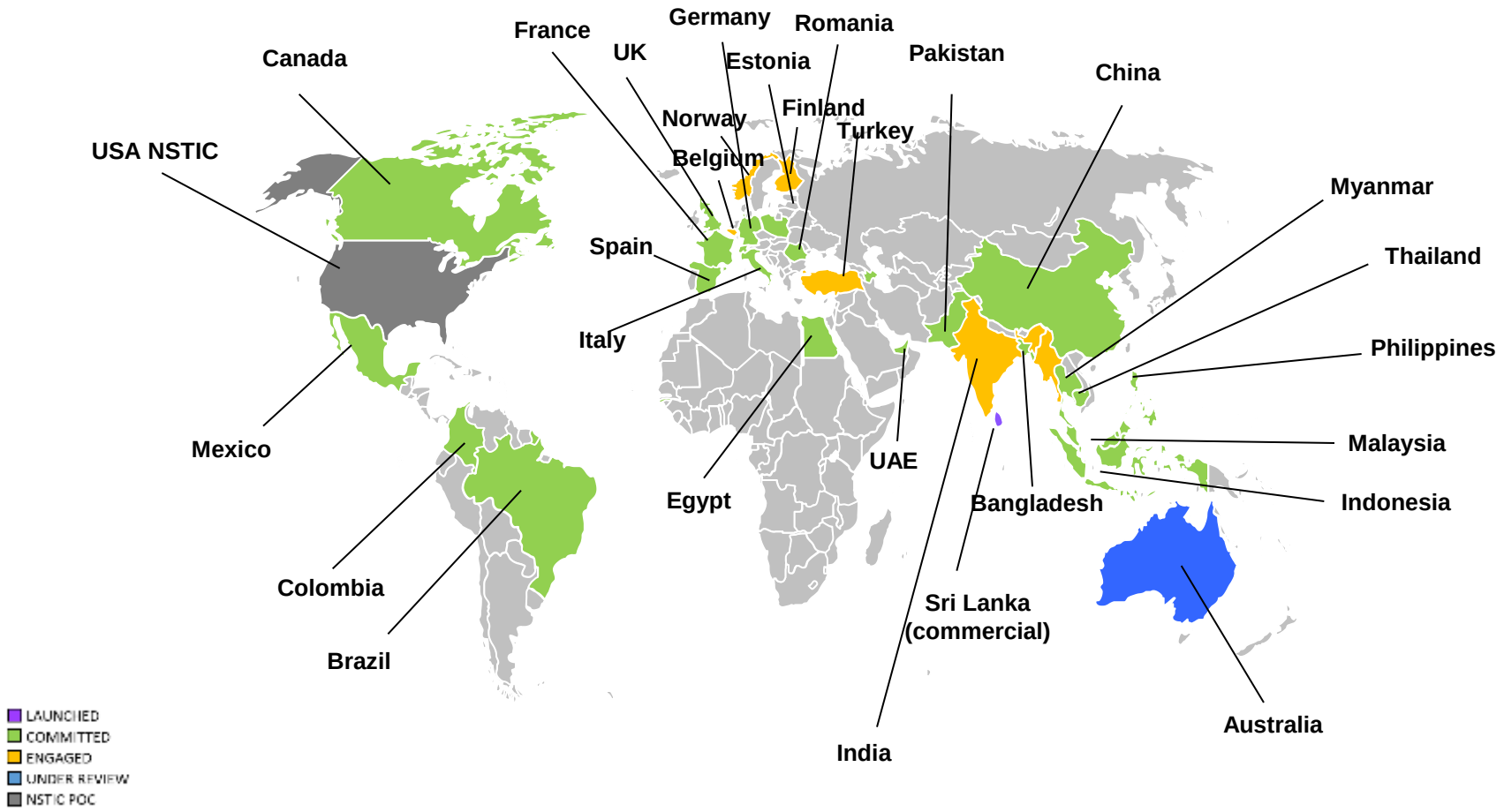
- Why couldn't we make it simple and safe at the same time ?

That's what Mobile Connect was designed for

Mobile Connect

A multi-MNOs proposal, under GSMA governance

Markets engaged with Mobile Connect 2015/16



Mobile Connect and security factors

	log-in & reassurance					Signature
Mechanism	**Username & password**	**Seamless Login (2G-3G auth)**	**SIM confirmation (Click 'OK')**	**SMS Push OTP**	**SIM Enter PIN**	**SIM PIN (PKI with certificate)**
Strength	Single factor: What I know	Single factor: What I have	Single factor: What I have	Single factor: What I have	Two factor: What I have + What I know	Two factor: What I have + What I know
Security						
Channels						

[NEW]
Mobile Connect

What is Mobile Connect?

- Mobile Connect is a new end-user authentication and authorisation method
- More convenient than any other authentication method, yet secure
- Based on secure SIM card applet and customer individual 4-digit PIN code
- Simplification: no logins, no different passwords to be remembered
- Authentication always related to current user transaction
- Using 2-factor authentication (Enter PIN mode) complies with EC PSD2 requirements
- Safe from many types of attacks

- Two authentication modes:

Click OK Enter PIN

Mobile Connect

Strenghs

Mobile Connect strenghs: security and simplicity combined

Mobile Connect is simple because:

- The customer always has his mobile phone with him
- It only relies on a 4 digits code, chosen by the customer (could be the same as the one for the credit card or the SIM PIN code).
- It allows a single end-user experience when accessing to all MC service providers all over the world
- It requires very little effort to implement for Service Providers, and does not need any pre-existing ecosystem (compared to NFC, for instance)

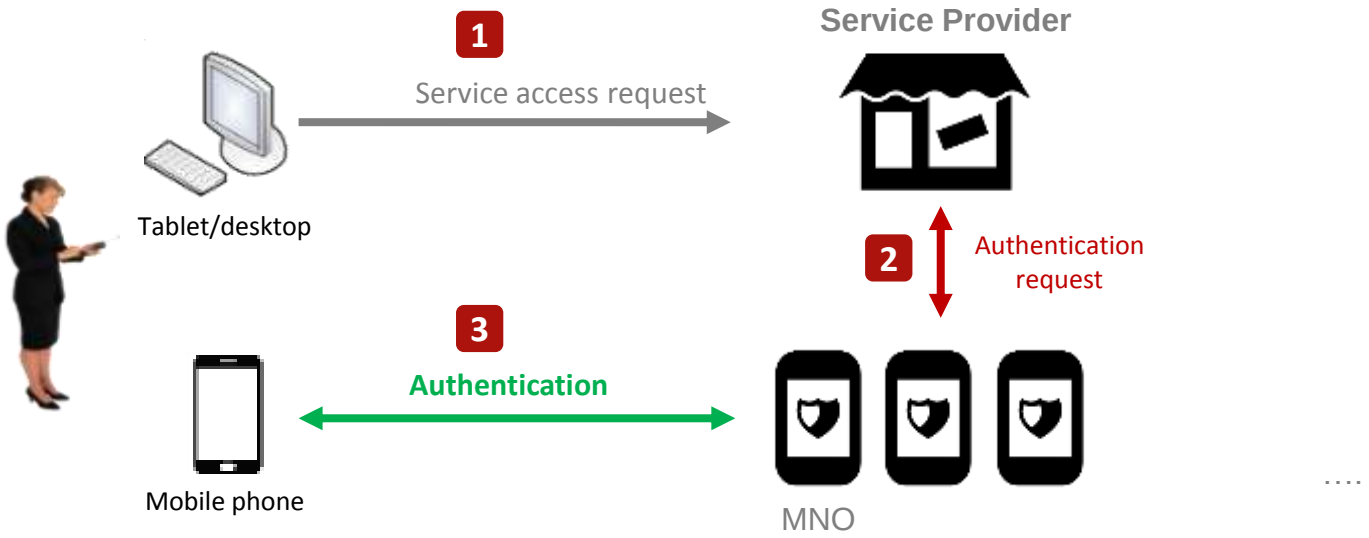
Yet, Mobile Connect is safe since :

- Password is safe not because of its complexity nor length but due to the fact that …
  - Pwd is only stores in 1 place in the world : the customer's SIM card
  - Pwd is encrypted, and SIM card is by nature very well protected against attacks
  - Pwd never transists over the network, even the MNO does not know it.
- Mobile Connect relies on an (SIM) applet which means :
  - An app totally independant from feature phones or smartphones Operating Systems → very difficult or impossible to attack though high level apps.
  - The applet remains under full control of the MNO, and is installed only by MNO (no « App Store » and thus no possibility to provide a fake app to the customer)

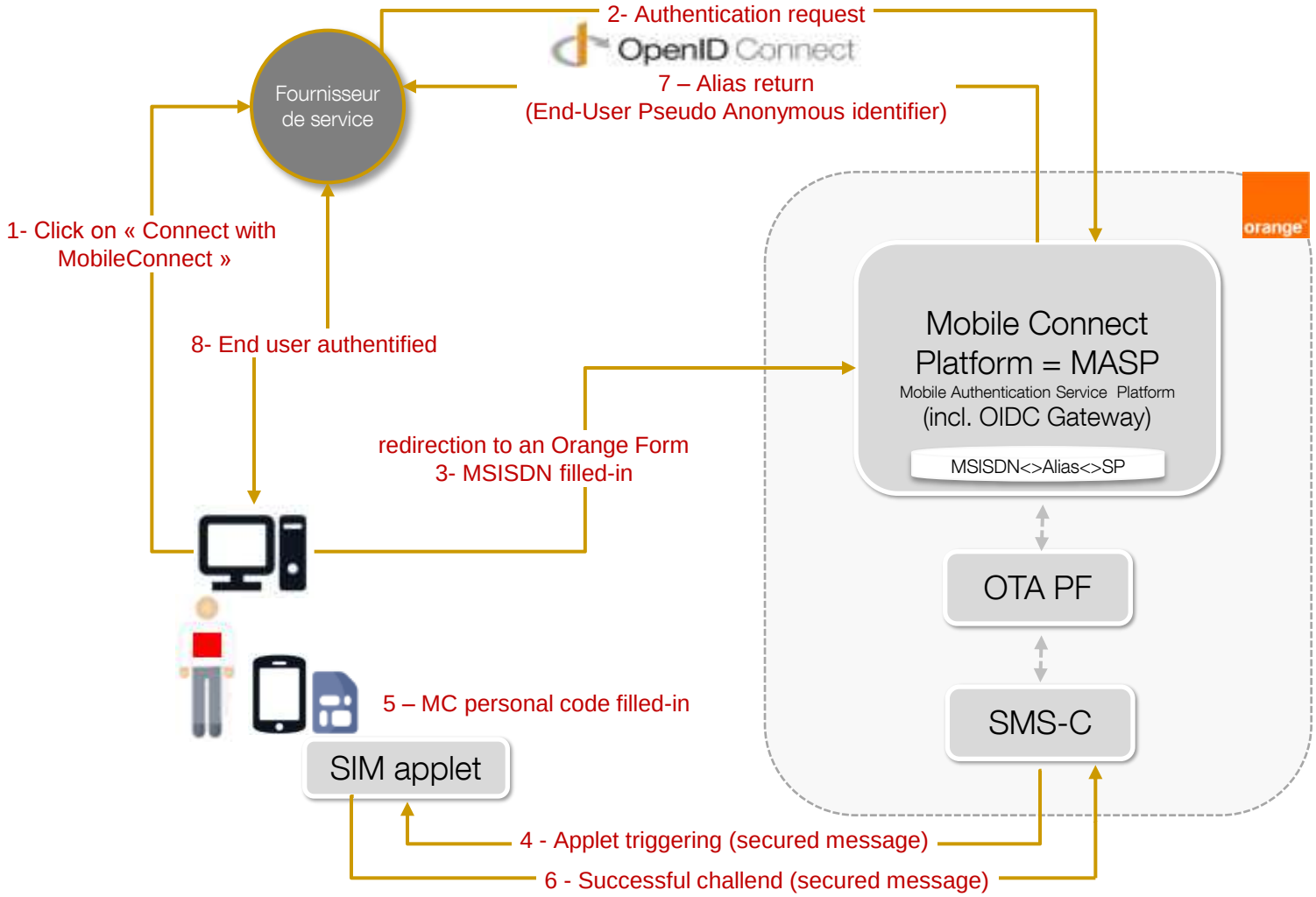
Mobile Connect

High level architecture and comparison with SMS OTP

Mobile Connect : main architecture and flows

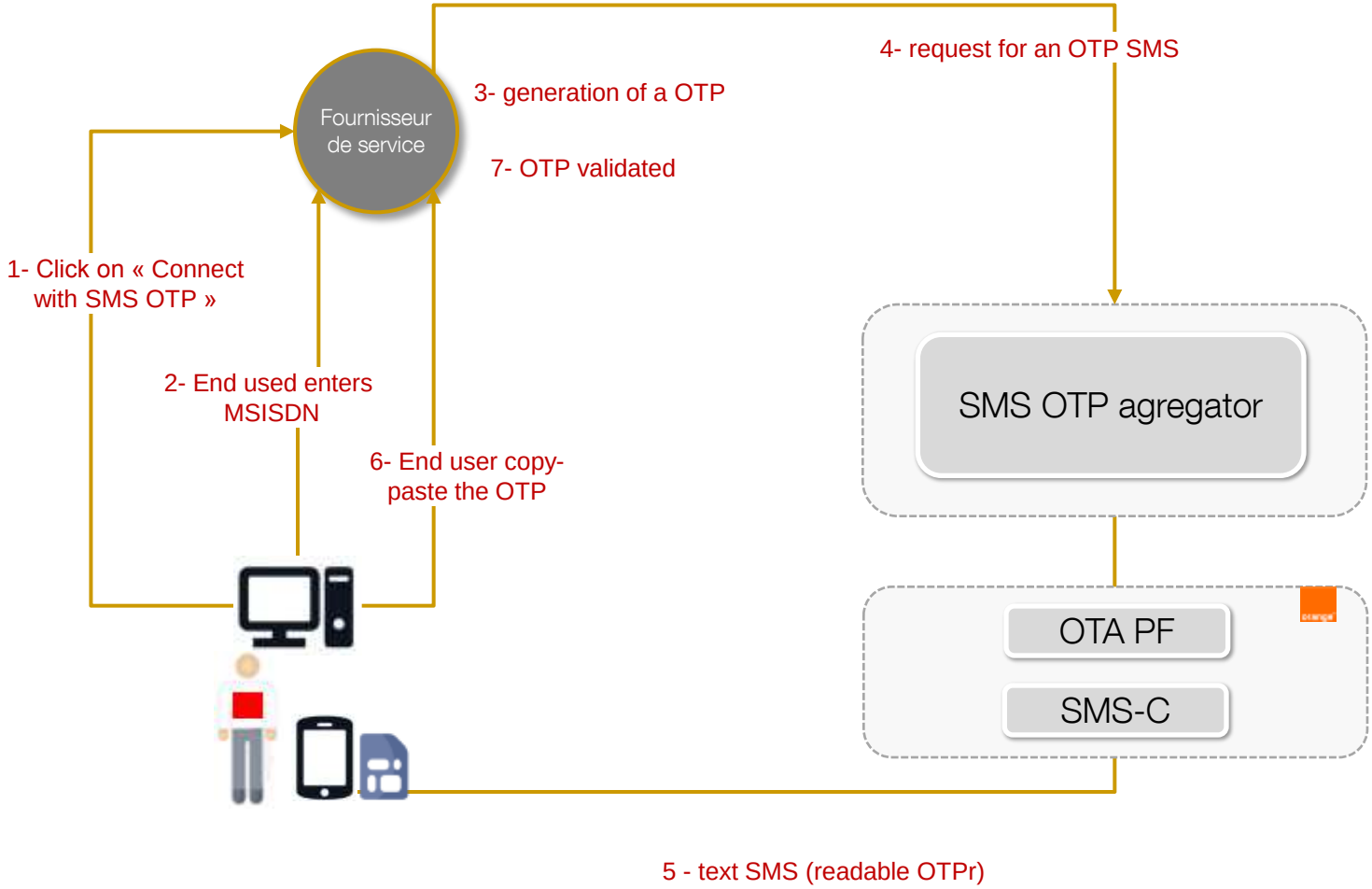


Mobile Connect : main architecture and flows



Customer's MSISDN is not seen by Service Provider which receives instead an alias or ACR (Anonymous Customer Reference) from MC platform.

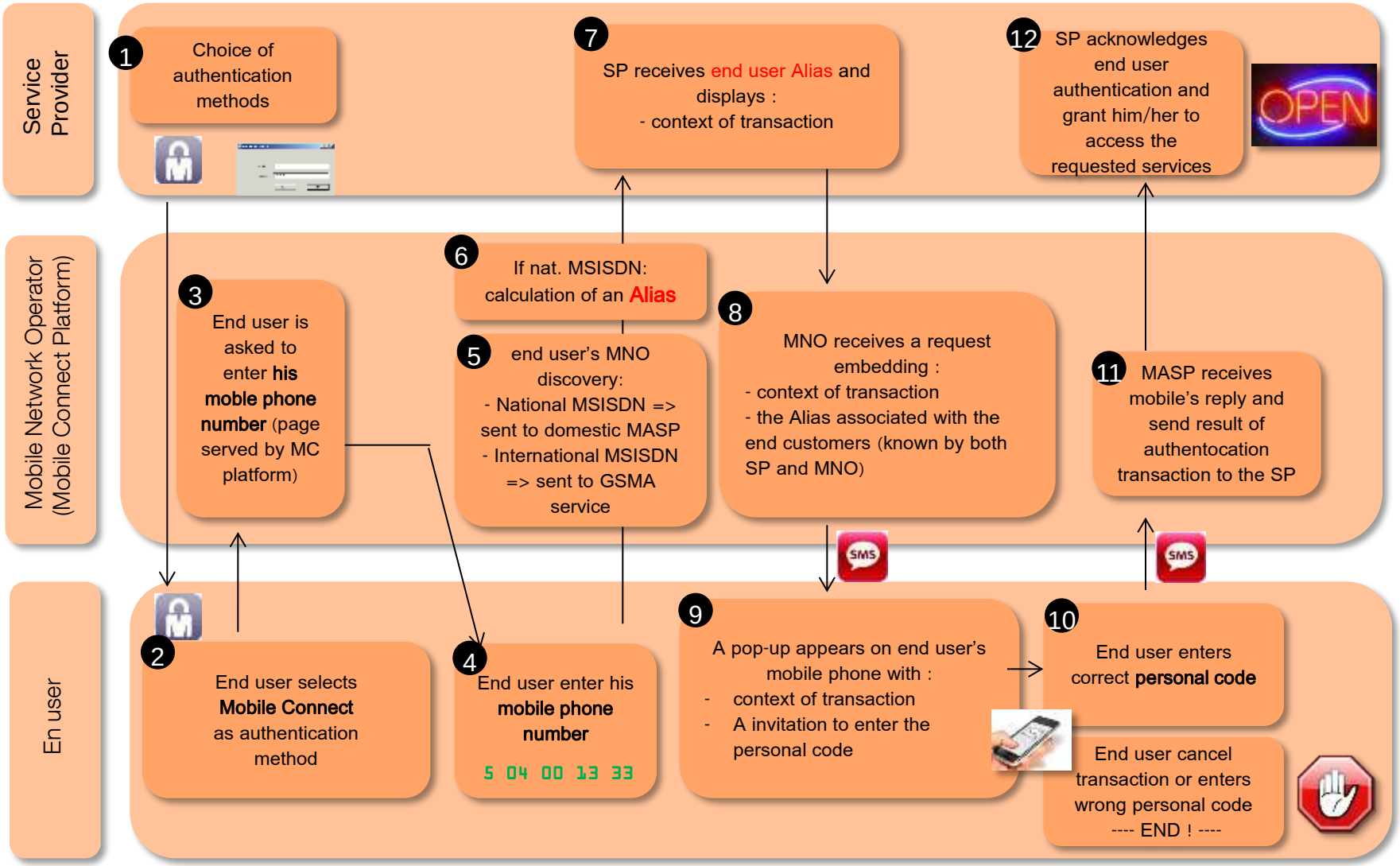
OTP : main architecture and flows



SP has to know custmer's MSISDN.
OTP code is transmitted without protection over the netword through a SMS code (and stored within the phone).

MC user journey, flows and confidentiality

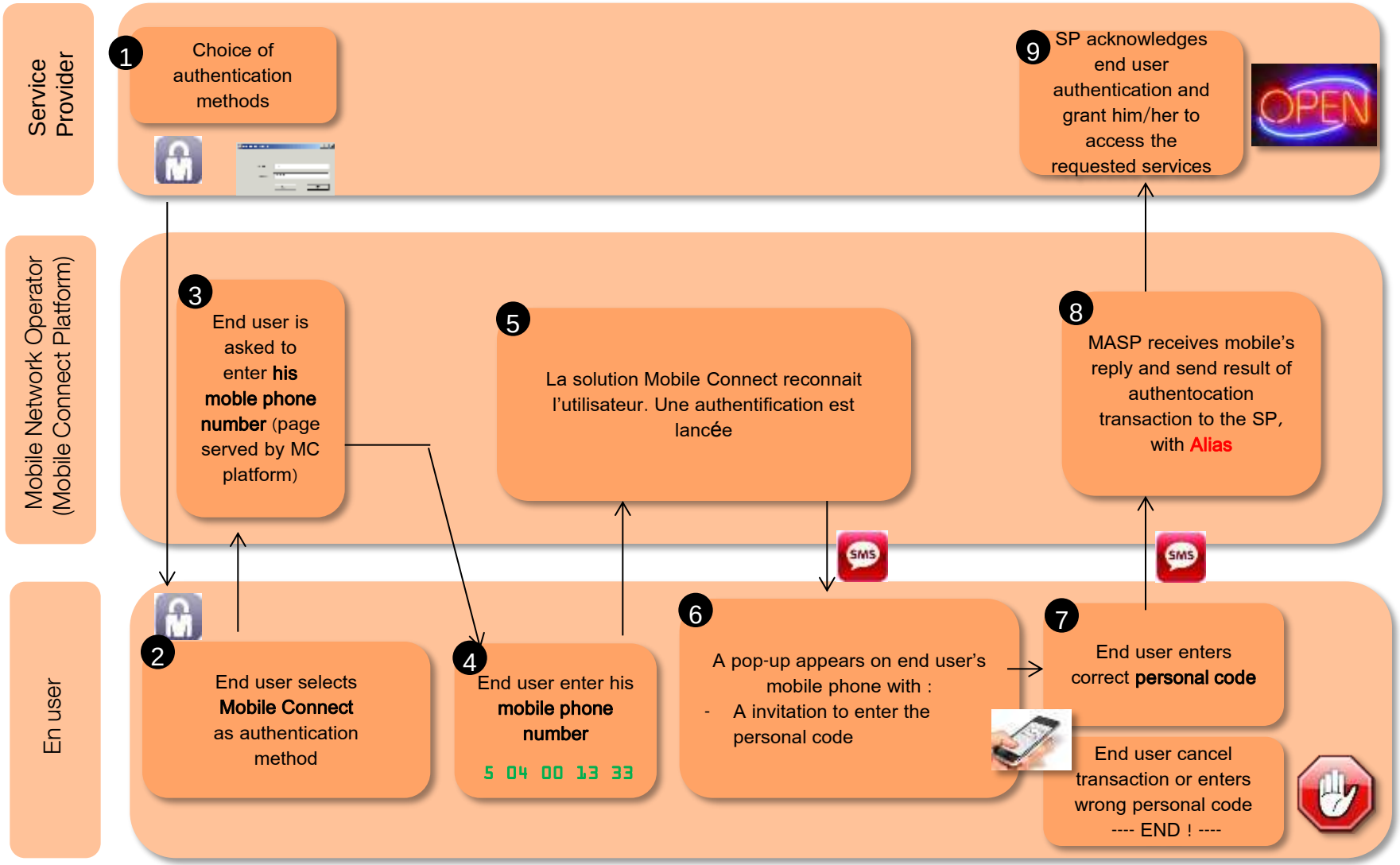
MC used for the first time



No personal information is shared with SP :
the MSISDN entered onto MC platform is transformed into an alias for SP

MC user journey, flows and confidentiality

Every other time



Mobile Connect : Who knows what ?

Customer knows :	SP Identifier	Personal code	/	MSISDN
SIM card knows :	/	Personal code	/	MSISDN
Mobile phone knows :	/	/	/	/
MNO knows :	/	/	alias	MSISDN
Service Provider knows :	SP Identifier	/	alias	/
Over the air without protection	SP Identifier except if session over HTTPs	/	/	/