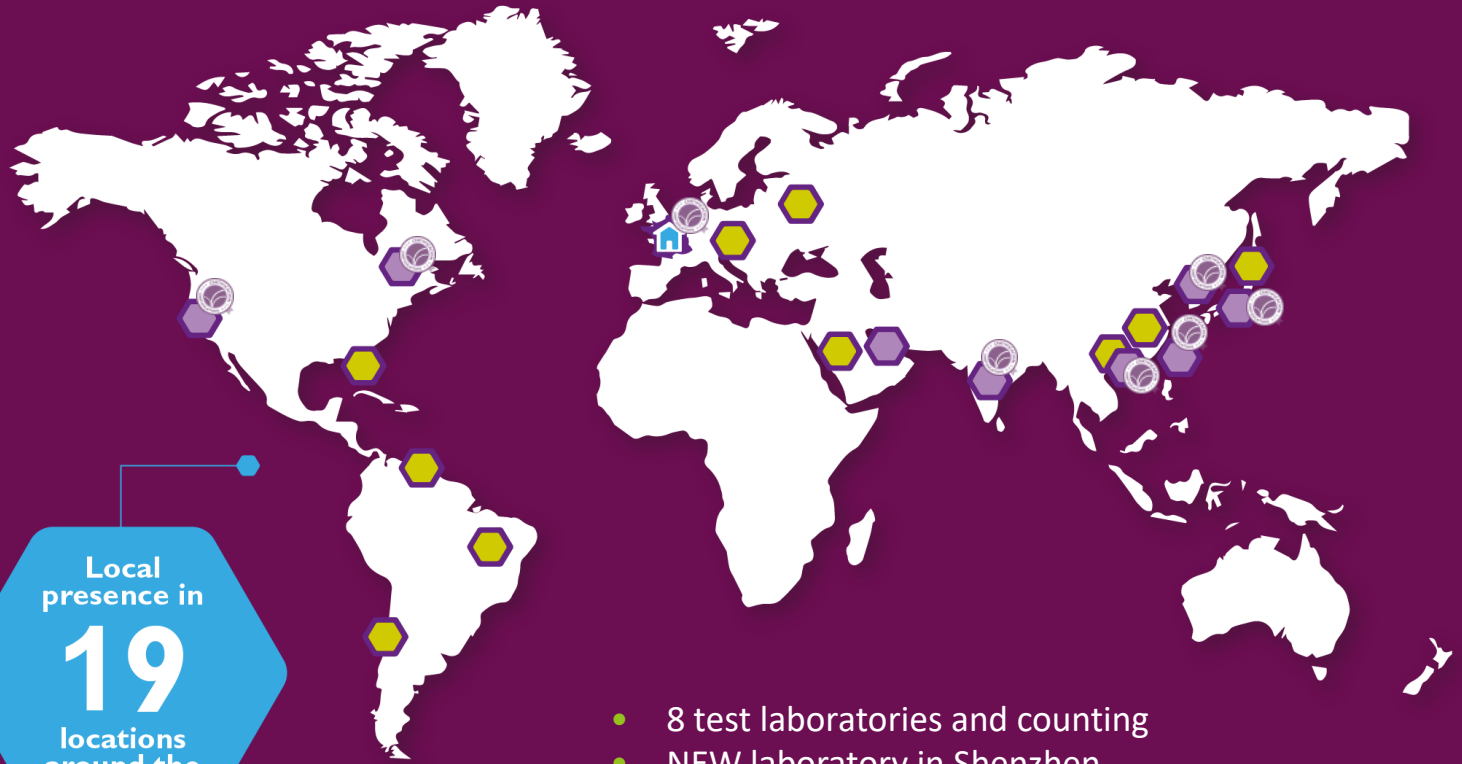
FIME®

One Action. **A billion transactions.**

Open Banking API validation

fime.com

Global reach



FIME LABS

MONTREAL • CAEN
SAN JOSE • BANGALORE
SHENZHEN • TAIPEI
SEOUL • TOKYO

FIME OFFICES

FIME DISTRIBUTORS

Local presence in **19** locations around the world

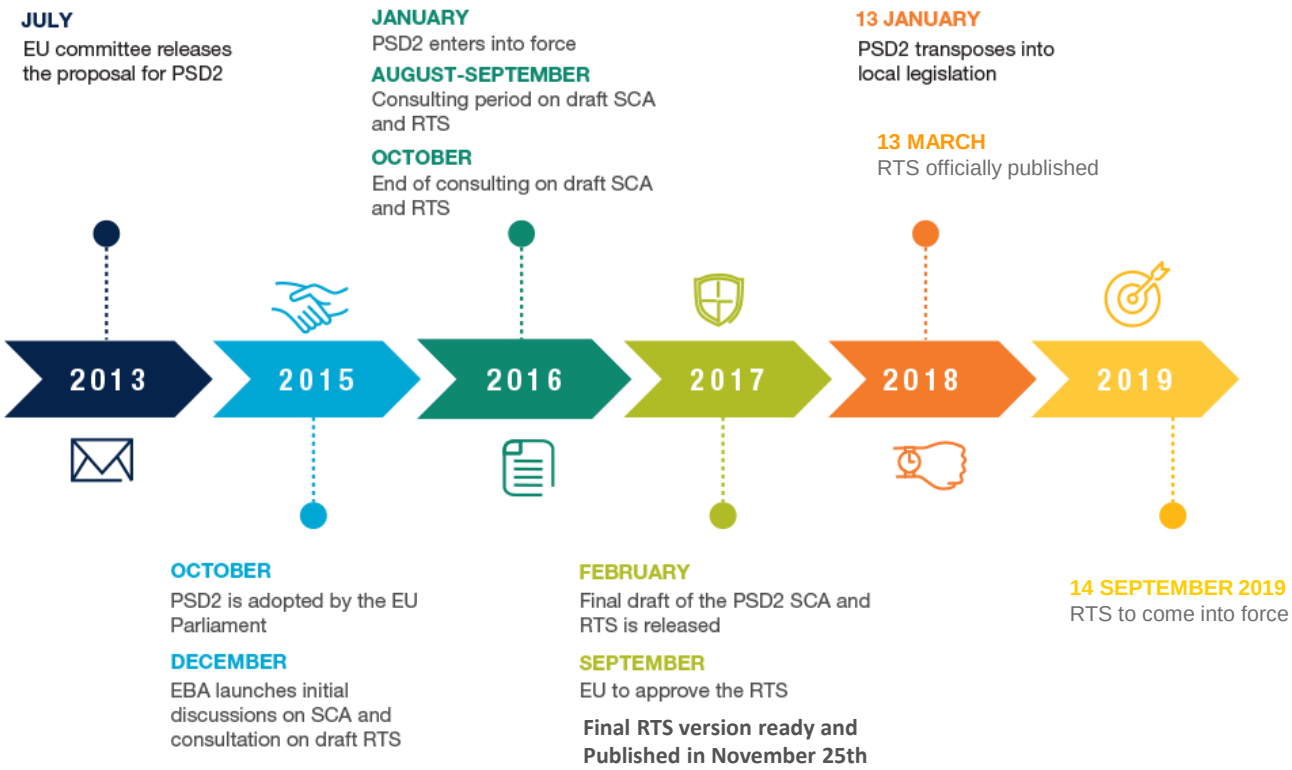
- 8 test laboratories and counting
- NEW laboratory in Shenzhen
- Customers in 180+ different countries

Once upon a time there was PSD2….

- PSD2 defines requirements for ASPSPs to share account holder information with person's explicit consent
- PSD2 limits the regulatory scope to payment accounts
- PSD2 defines the scope of data to be shared

- Regulatory Technical Standard provides strict guidelines
- EBA deliberately decided not to define standardised specifications for the interfaces to be developed in the RTS
- PSD2 brings testing & security requirements under EU law in the RTS

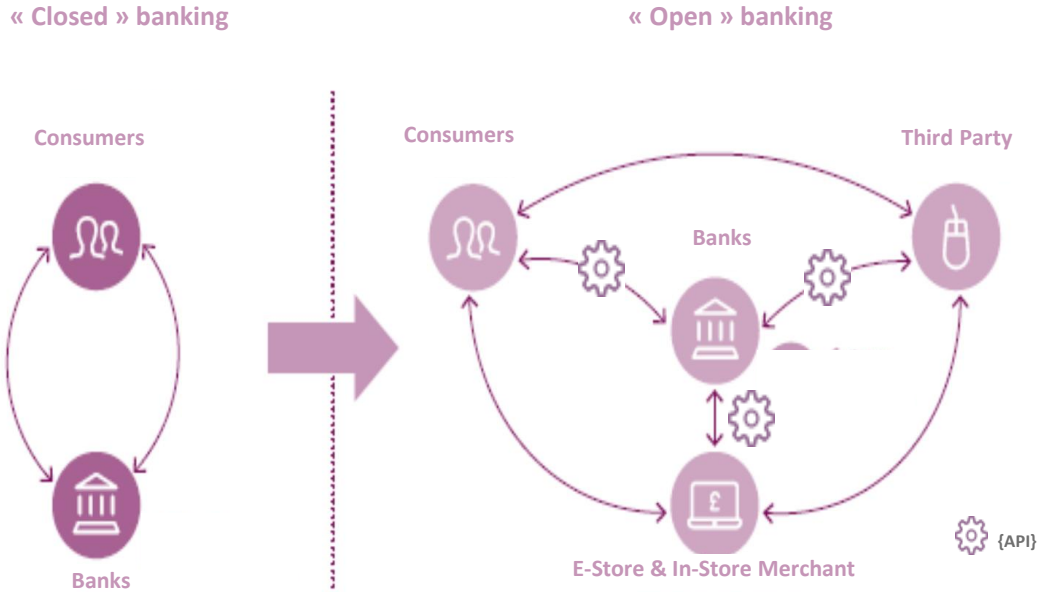
The deadlines of PSD2 regulation

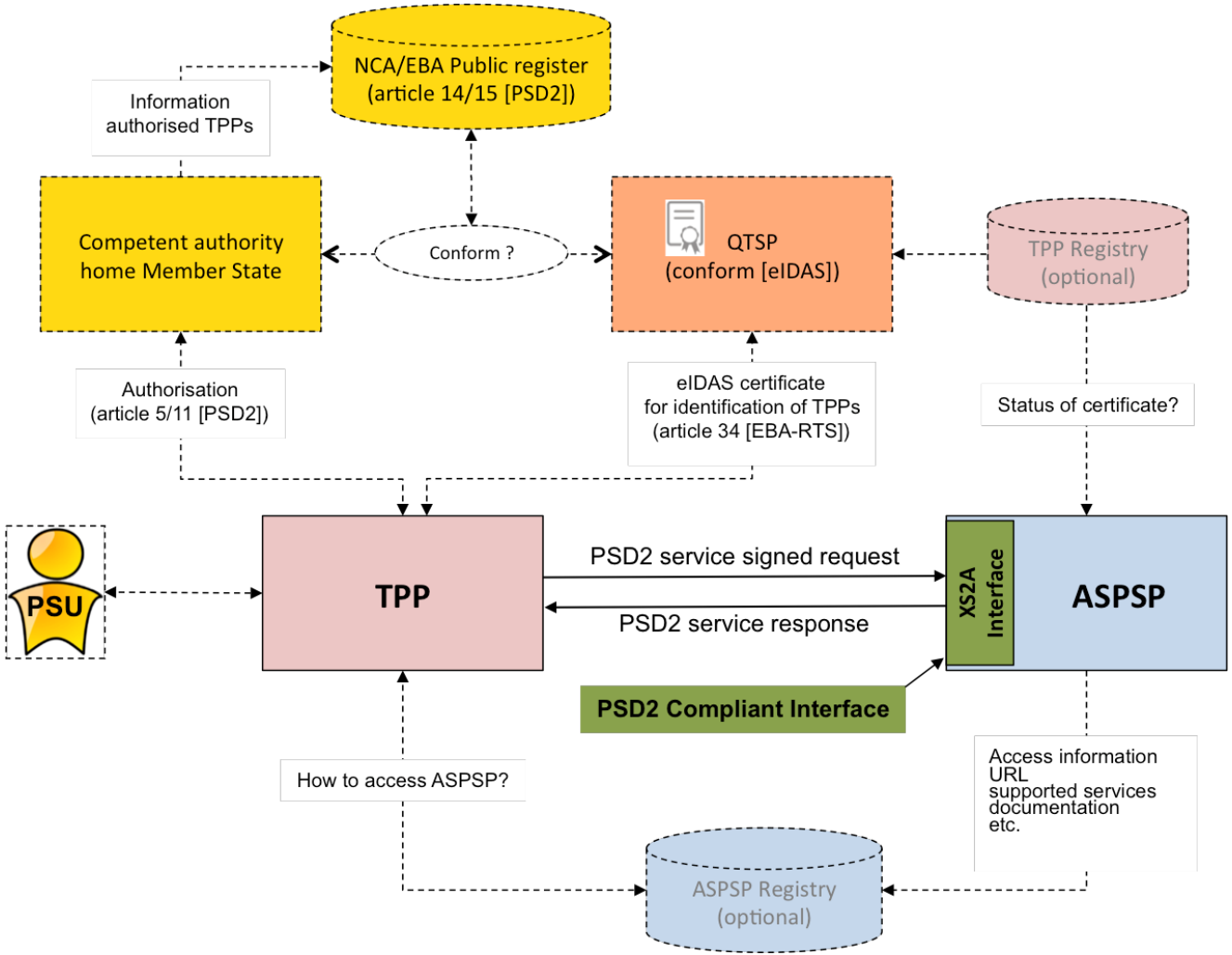


Open Banking Ecosystem

- Opening up of bank-held customer account data to third Parties

- Banks & third parties exchange Financial messages through APIs




NCA/EBA Public register
(article 14/15 [PSD2])
Information
authorised TPPs
Competent authority
home Member State
Conform ?
QTSP
(conform [eIDAS])
TPP Registry
(optional)
Authorisation
(article 5/11 [PSD2])
eIDAS certificate
for identification of TPPs
(article 34 [EBA-RTS])
Status of certificate?
PSU
TPP
PSD2 service signed request
PSD2 service response
XS2A
Interface
ASPSP
PSD2 Compliant Interface
How to access ASPSP?
Access information
URL
supported services
documentation
etc.
ASPSP Registry
(optional)

Open Banking is driven by regulation

Regulation is pushing

- In **Europe PSD2** came into force on 13 January 2016
- In **Poland PSD2** is transposed into law

Banks are developing APIs

- **1400 banking** APIs already exist in Europe
- **Banks digitalization strategy**

Third parties are standardising APIs

- **The Berlin Group** provides guidelines for API interface
- **The Polish API standardization** provides banking specification
- **Digital hub such as KIR in Poland** standardizing API

TESTING before July 14th 2019

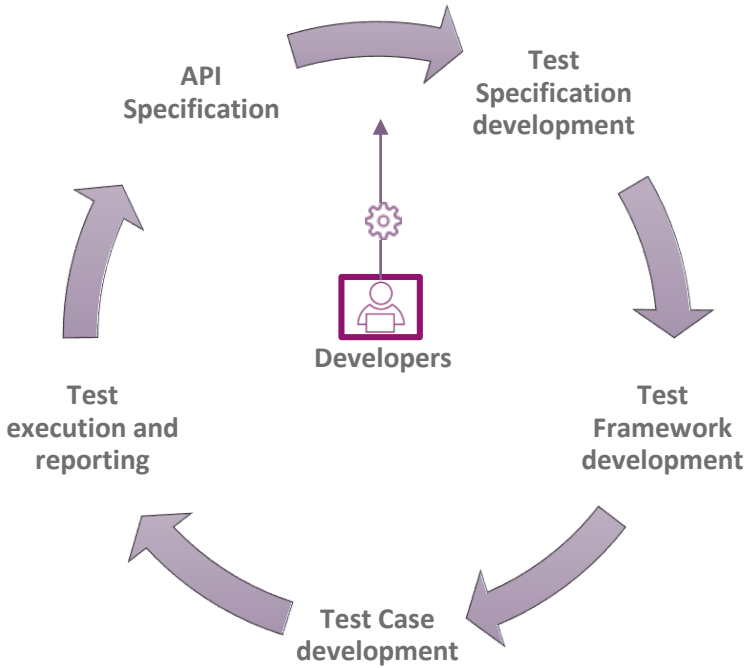
Testing Open Banking API (1)

What is tested?

- **Functionality** of Open Banking API to be validated against API's standards
  - Berlin Group : guidelines
  - Polish API – Poland

- **Security** through penetration testing to determine the main threats and vulnerabilities to which payment service providers are currently exposed

How it is tested?

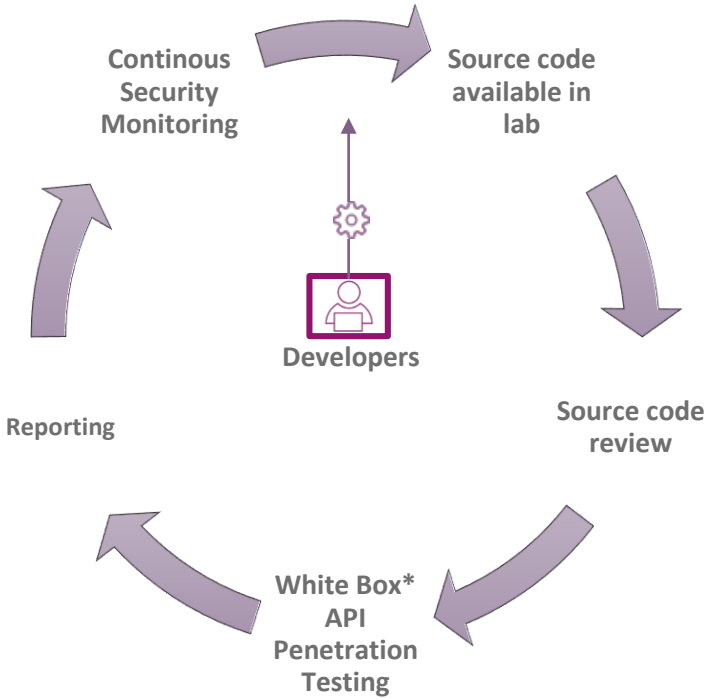


Testing Open Banking API (2)

What is tested?

- **Functionality** of Open Banking APIs to validate against technical standards
  - Berlin Group Germany
  - Polish API
- **Security** through penetration testing to determine the main threats and vulnerabilities to which payment service providers are currently exposed

How it is tested?



Testing Open Banking API (3)

When?

► Every time the payer accesses his **payment account online**, initiates **electronic remote payment** or **remote channels transactions**

►Under European PSD2 regulation **PSPs require STRONG AUTHENTICATION** to avoid bad transactions

What?

Knowledge
Something the user **knows**
E.g. static password, PIN

Ownership
Something only the user **possesses**
E.g. Token, smart card

Inherence
Something the user **is**
E.g. such as a fingerprint

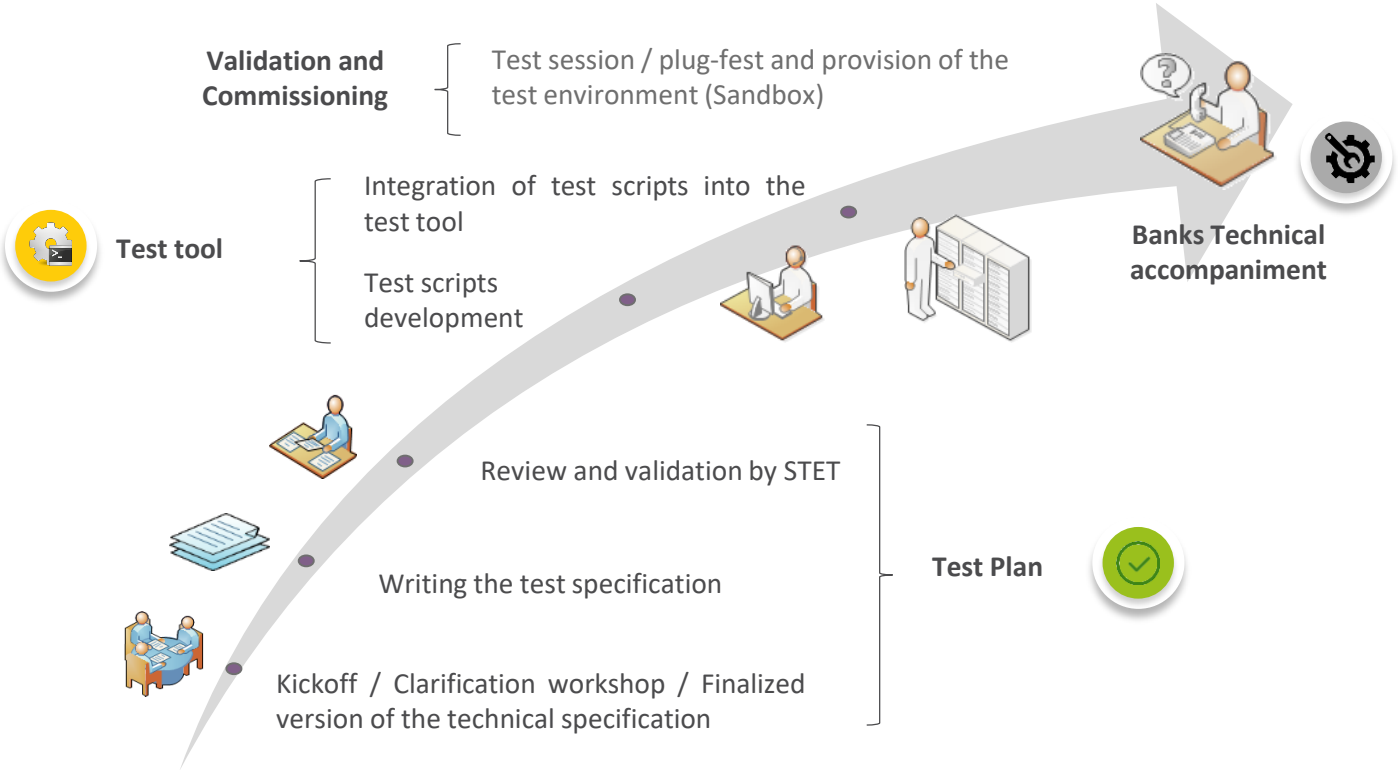
How?

► **Tokenization**–One-time authorization (via “tokenization”) prior to payment (e.g. ApplePay)

► **Embedding** –User is redirected to known Bank interface (e.g. iDEAL)

► **Overlaying** –Third party provider providing one user interface across multiple banks (e.g. SOFORT)

CASE STUDY | STET



Contact FIME

Nigel.reavley@fime.com
www.fime.com

One Action. **A billion transactions.**

Thank you