Konsentus

Confidence in open banking

A RegTech Company

PSD2 open banking for Small Banks and Credit Institutions

Implications and Requirements

Webinar January 2019

Konsentus
Confidence in open banking

David Parker, Advisor
& co-founder Konsentus

Please ask questions as we go along

Konsentus
Confidence in open banking

Regulatory challenge in the EU

In January 2018 the European Union Payment Services Directive (PSD2) came into force across Europe, delivering a consistent vision for open banking across all member states

End users will have a legal right to share their personal transactional account data from their financial institution with regulated third parties to enable better financial outcomes

Open Banking API Access

Konsentus
Confidence in open banking

Financial Institutions (FI) must provide regulated third parties (TPPs) access to end user transactional account data

FIs are being strongly encouraged by regulators to implement open banking APIs

If not they are mandated by regulation to deliver dedicated interfaces to support open banking

What FIs need to do to Respond

Konsentus
Confidence in open banking

Difference between Big Banks and other FIs

- There is none in terms of PSD2 open banking
- Yes in the UK the CMA9 under the implementation jurisdiction of the OBIE were just the 9 big bank
- The CMA9 will need to align their offering to meet the more extensive requirements of the PSD2 open banking
- Could be argued to be unfair but the EBA Regulatory Technical Standards makes no distinction, or timing allowance between large and small FIs
- So PSD2 open banking applies to all FIs, big or small, Emoney, or Payment Institution regulated

Konsentus
Confidence in open banking

So what is a transactional account

- PSD2 uses the term ‘Transactional Account’
- The FCA defines a transactional account in the FCA handbook as a ‘Payment Account’
- "Payment account" is defined in the FCA regulation 2 as:

"an account held in the name of one or more payment service users which is used for the execution of payment transactions"

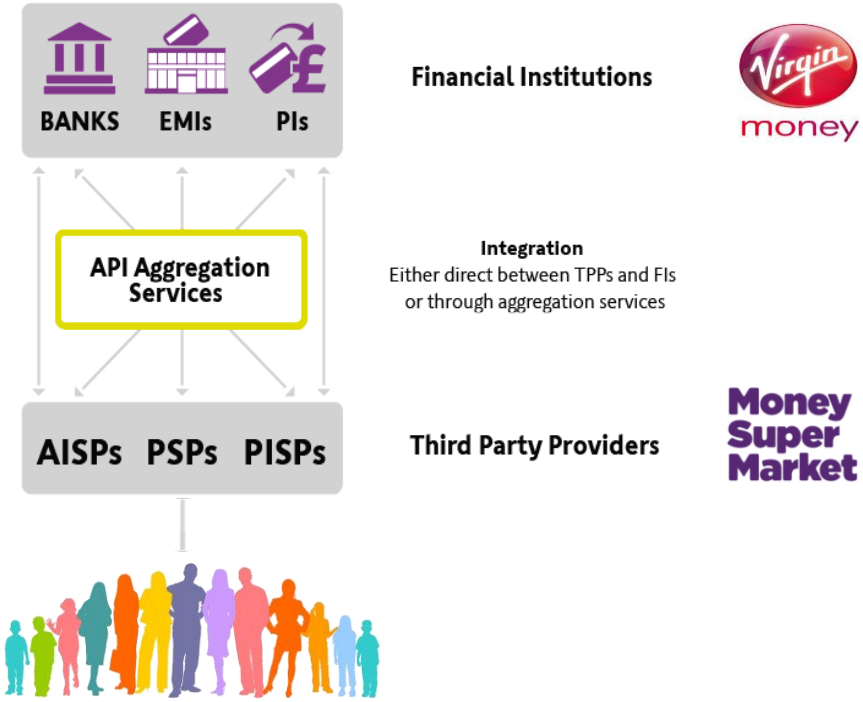
So who is covered, almost every account that is accessible vis an online interface (i.e. mobile / internet banking etc.):

- E-wallet Wallet
- Reloadable Prepaid Card
- Bank Current and Payments Accounts
- Account you can pay someone or a merchant from

Source: FCA Handbook PERG 15 Guidance on the scope of the Payment Services Regulations 2009

End user interaction

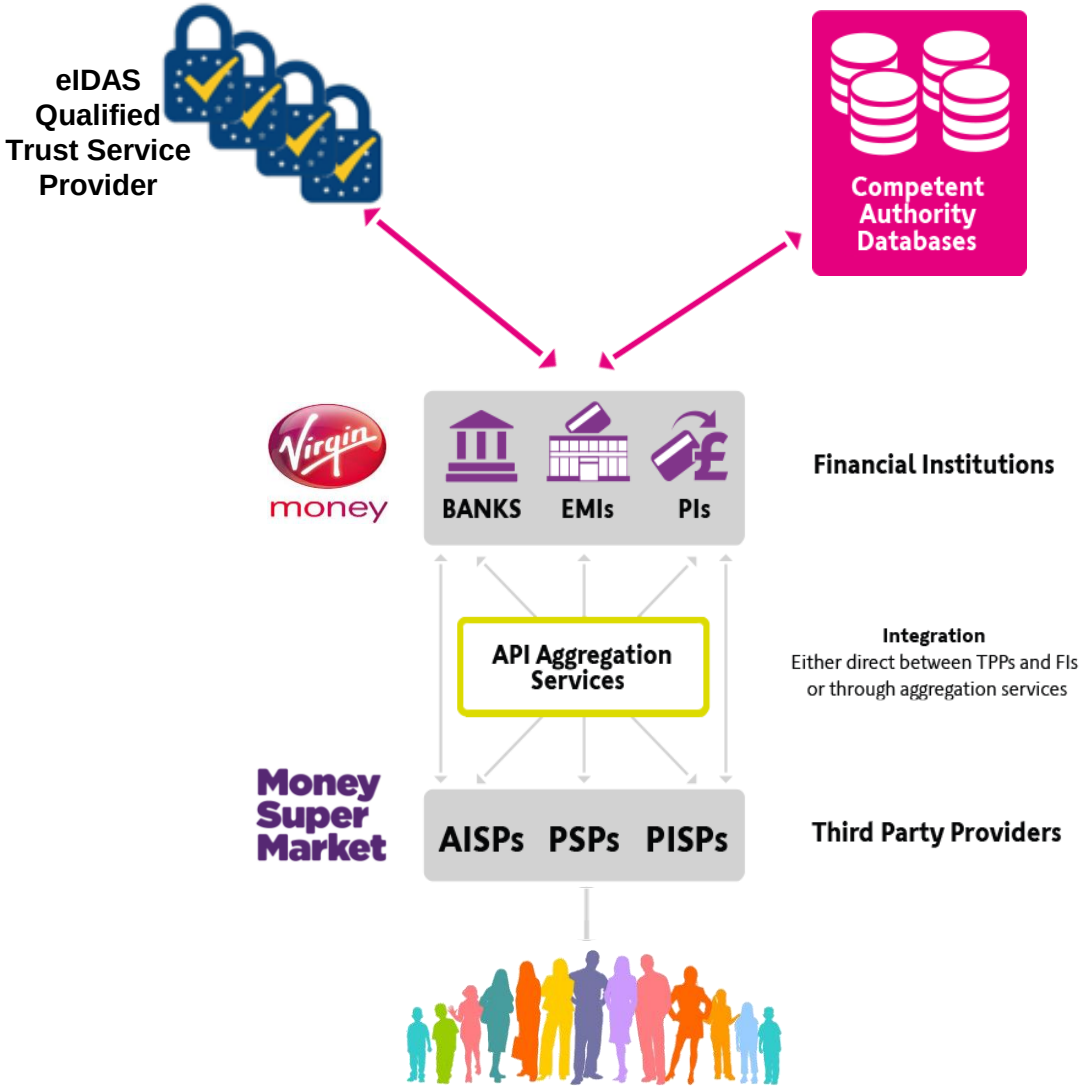
Third Party Providers and aggregators communication



1. End user requests TPP to access data from FIs
2. FI validates identity of TPP using its eIDAS Certificate to establish secure communication channel
3. FI collects end user Consents from TPP
4. FI performs Strong Customer Authentication (SCA) to authenticate end user

Konsentus
Confidence in open banking

Behind the scenes – TPP identification and validation



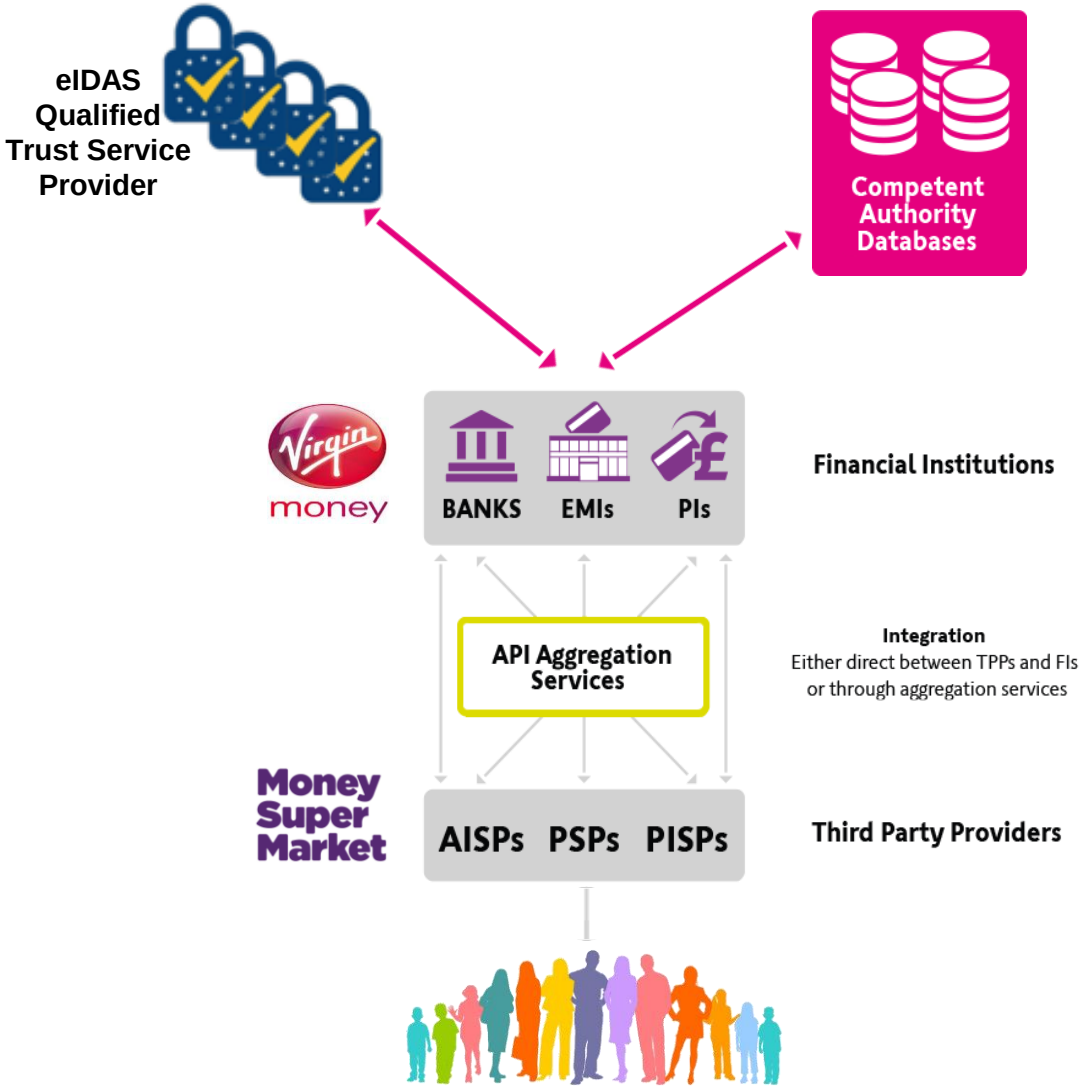
5. **FI validates TPP eIDAS Certificate via QTSP to confirm identity of TPP and associated National Competent Authority (NCA)**

6. **FI checks with NCA that TPP is regulated/approved**

7. **FI issues Access Token to TPP as appropriate (PSD2 schema)**

Konsentus
Confidence in open banking

Behind the scenes – Transaction processing



1. TPP requests access to end user account(s) from FI
2. FI validates TPP eIDAS Certificate via QTSP to confirm identity of TPP and associated NCA
3. FI checks with NCA that TPP is regulated/approved
4. FI validates Access Token checking that end user has not revoked Consent

Konsentus
Confidence in open banking

Is it just an API that FIs must offer

- FIs are required to put in place a fallback mechanism

- Unless FIs gain ‘exemption’ they must also offer a ‘dedicated interface’
  - A dedicated interface in English means online/app access via functionality like screen scraping

- Exemption certificates are issued by the NCA in consultation with the EBA

- TPPs must be able to access an FIs ‘dedicated interface’ if their API is unavailable for more than 30 seconds

- FCA have stated:

- *“We would encourage ASPSPs seeking exemption not to wait until this (sic March 14 2019) date to make these available. Stress testing will also need to be carried out by the ASPSP.*
- *The RTS does not allow us to grant a partial exemption. We will provide opportunities for ASPSPs to engage with us before submission of the exemption request. We also encourage timely requests for exemption as we will need time to make an exemption assessment.”*

Konsentus
Confidence in open banking

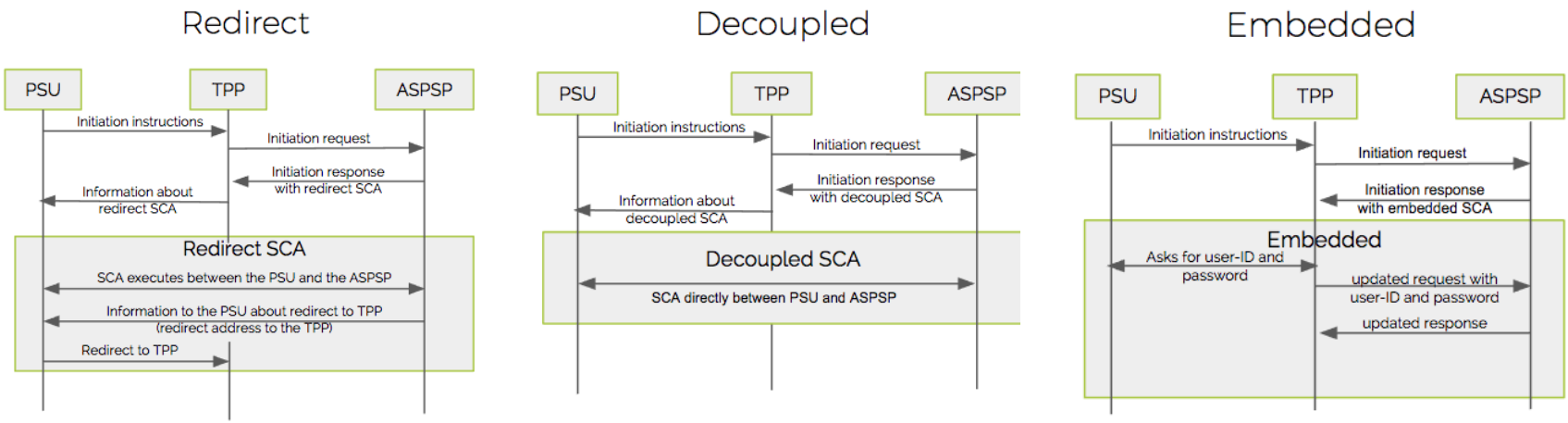
Can FIs not offer an API

- Yes

- If using the dedicated interfaces FIs must be able to ensure
  1. TPPs can be identified and checked for status
  2. Take the necessary measures to ensure they only access, store or process data the consumer has consented to
  3. Log the data they access and make it available to the relevant NCA if requested

Understanding SCA

- SCA = Strong Customer Authentication
- Each time a Payment Service User grants consents to a TPP an FI must carry out SCA
- They can use whatever method they want to perform SCA:



- The FCA has stated:

- *"That the use of redirection by an ASPSP is not automatically an obstacle; nor is there a requirement in PSD2 or the RTS for an ASPSP to provide more than one method of access."*

The use of SMS messages for SCA

- Questions had been raised in the industry about whether a One-Time Password sent via SMS to a mobile phone qualifies as an ownership factor (“something only the user possesses”)

- The EBA stated on the 5/10/2018:

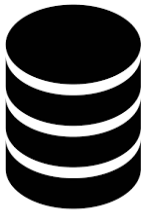
- *Paragraph 35 of the EBA opinion on the implementation of the Commission Delegated Regulation (EU) 2018/389 (RTS on Strong customer authentication and secure communication) clarifies that “For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device”.*

- *In this context, a one-time password sent via SMS would constitute a possession element and should therefore comply with the requirements under Article 7 of these RTS, provided that its use is ‘subject to measures designed to prevent replication of the elements’, as required under Article 7(2) of these RTS. The possession element would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number.*

Konsentus
Confidence in open banking

FIs must only provide data to registered/approved TPPs no matter how they access

How can FIs tell if a TPP is approved?



EBA Register

31 National Competent Authorities (NCA)

70+ Qualified Trust Service Providers (eIDAS)

Numerous PSD2 Schema

An FI needs to reference 100+ Databases, many not real time, machine readable

the **Problem**

Konsentus
Confidence in open banking

In summary TPP approval: The challenges

- EBA Register is not a machine readable, real-time, online accessible database
- Scheme Regulatory Databases (i.e. UK Open Banking) are not compulsory to register with
- National Competent Authority Databases are not Machine Readable
- National Competent Authorities have no legal obligation to notify Scheme Regulatory Databases other than a general published bulletin when they revoke a TPP
- National Competent Authorities have a 20 day SLA in place to notify passported NCAs when a TPP is revoked
- There are 70+ Qualified Trust Service Providers who issue eIDAS seal Certificates

So yes; It is a Challenge

Timings are mandatory, there is officially no wiggle room

- Regulatory Technical Standard published in OJEU March 2018
- Based on this the timings are:

March 14th 2019 FI's must have platforms available for external testing

Sept. 14th 2019 FIs must go live or face the risk of fines from regulators

- What is live today is the UK CMA9, this is UK Open Banking, not PSD2 open banking, though this will merge

Konsentus
Confidence in open banking

FCA are very clear:

Timings

- FCA issues clear guidance on PSD2 open banking and what it expects (edited).

- *"ASPSPs and TPPs should be aware that:*
  - *We encourage ASPSPs to provide dedicated access to TPPs using APIs.*
  - *From 14 September 2019 all ASPSPs will need to comply with obligations set out in RTS Articles*
  - *All ASPSPs will also need to make available technical specifications, and provide support and a testing facility by 14 March 2019."*

https://www.fca.org.uk/news/statements/eba-draft-psd2-guidelines-opinion-banks-others-involved-open-banking

Payment System User Management

- *Karina McTeague; PSU's must be able to manage consents through online channels as they do direct debits* *(EPA Pay 360 Speech)*

Konsentus
Confidence in open banking

EBA also clear:

- *"Ignorance of them can of course not be used to justify non-compliance."*
- *"Non-compliance amounts to a breach of law, with the resultant consequences for the legal entity."*

Konsentus
Confidence in open banking

What do FI's Need to Consider

Option 1 – API solution

1. API interface, live for six months prior to externally going live
2. Exemption certificate from NCA or fallback option
3. SCA solution
4. TPP regulatory checking
5. eIDAS Seal Certificate checking if operating in Europe
6. Access token issuance (including token duration e.g. 30 days, 90 days)
7. Management of Consents by PSU

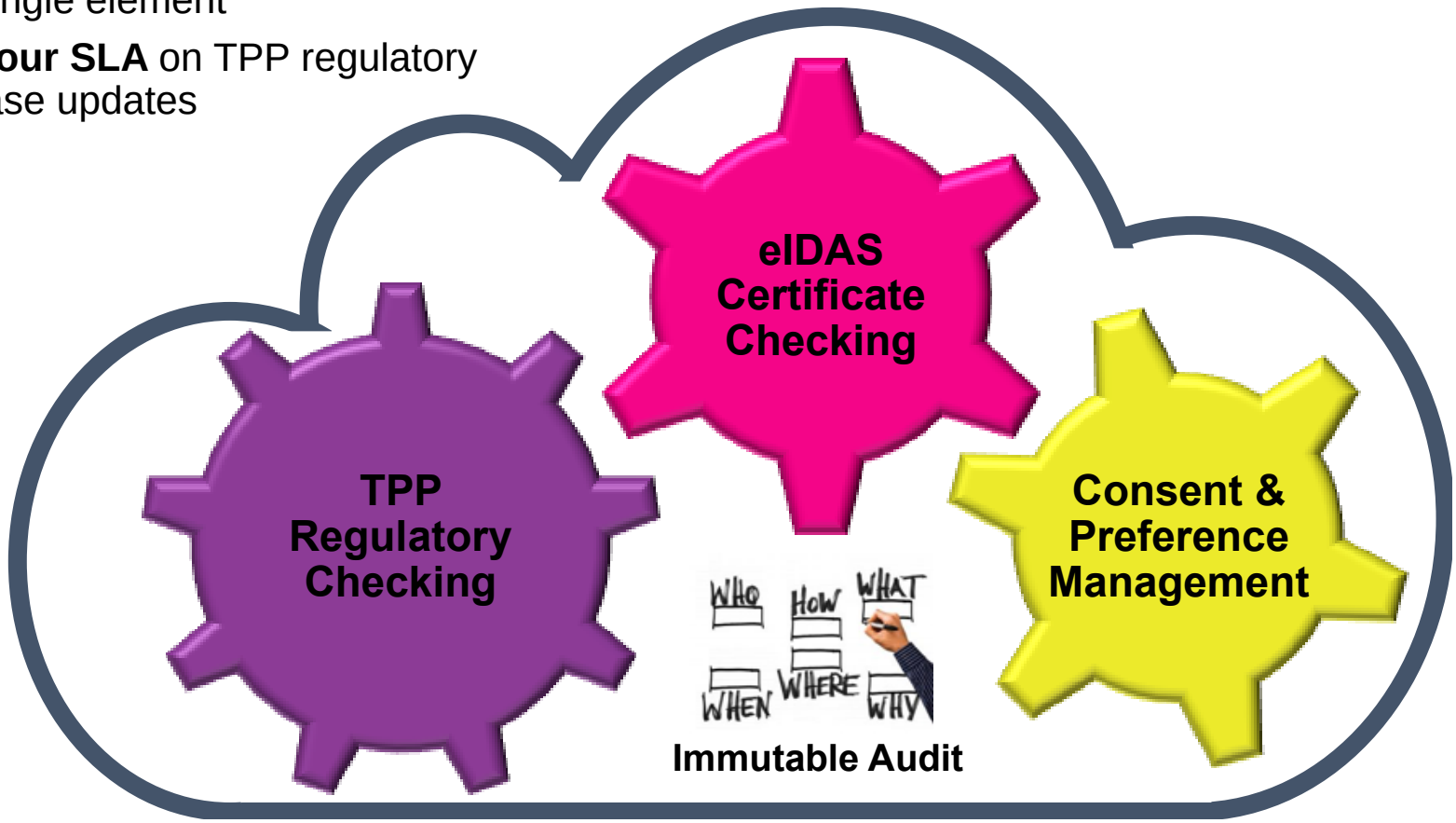
Option 2 – Dedicated interface: Not API

1. 4,5,6 also needs to be done from above to deliver
2. Take the necessary measures to ensure they only access, store or process data the consumer has consented to
3. Log the data they access and make it available to the relevant NCA if requested
4. Justify to the NCA, upon request, the use of the interface

Konsentus
Confidence in open banking

The Konsentus solution:

- FIs can purchase the complete solution
- Or a single element
- **One hour SLA** on TPP regulatory database updates



Konsentus
Confidence in open banking

What do FI's Need to Consider

Option 1 – API solution

1. API interface, live for six months prior to externally going live
2. Exemption certificate from NCA or fallback option
3. SCA solution
4. **TPP regulatory checking**
5. **eIDAS Seal Certificate checking if operating in Europe**
6. **Access token issuance** (including token duration e.g. 30 days, 90 days)
7. Management of Consents by PSU

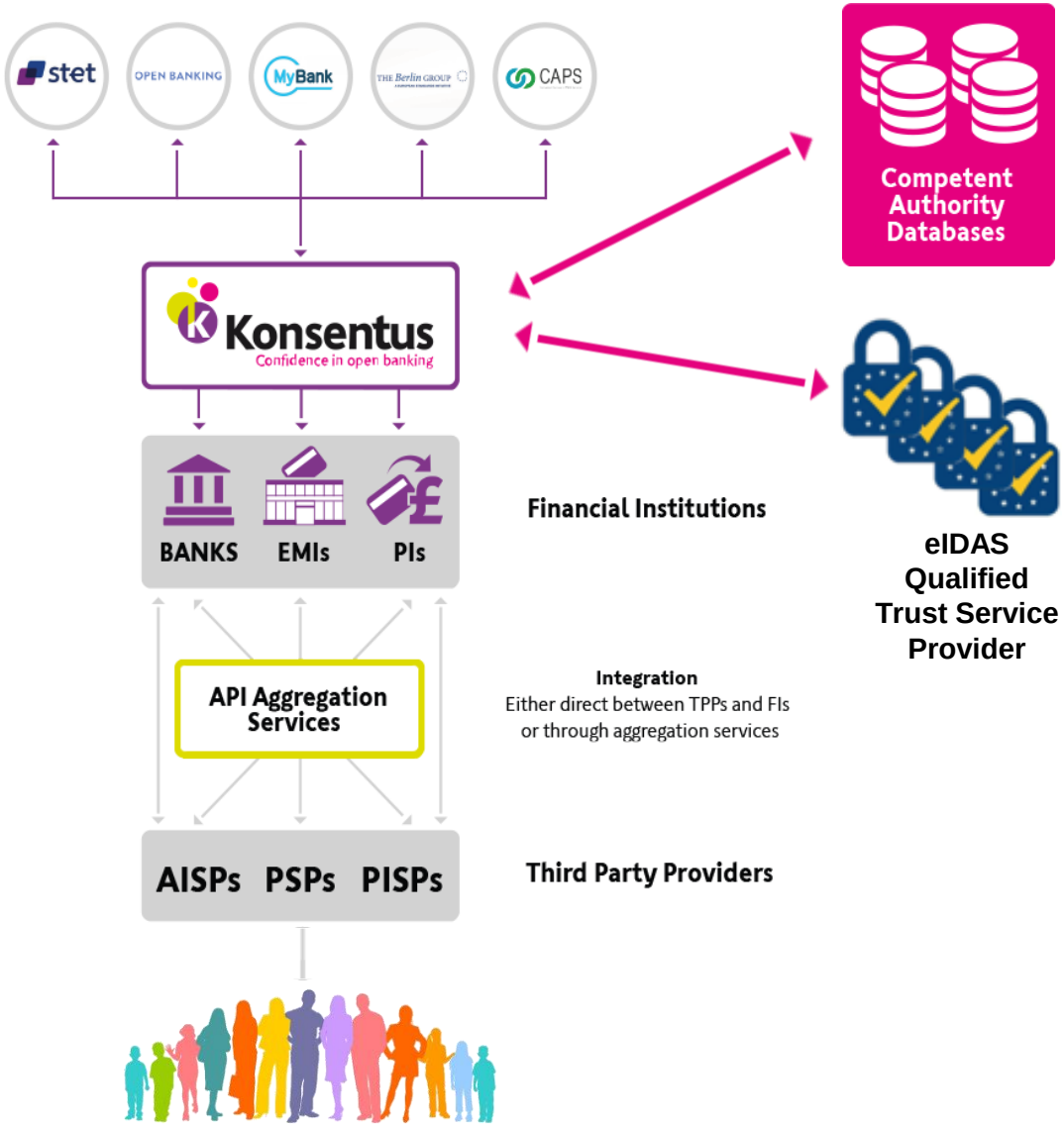
Option 2 – Dedicated interface: Not API

1. **4,5,6 also needs to be done from above to deliver**
2. Take the necessary measures to ensure they only access, store or process data the consumer has consented to
3. Log the data they access and make it available to the relevant NCA if requested
4. Justify to the NCA, upon request, the use of the interface

Konsentus Solution
Confidence in open banking

Konsentus
Confidence in open banking

Konsentus the TPP regulatory checking solution



Why use Konsentus

1. Konsentus is the only secure SaaS platform that provides online, real-time open banking regulatory checking services:
   - **Risk Management** – provides the most up to date information on TPP regulatory status, thus reducing the FIs risk of providing data to an unregulated third-parties
   - **Identity Management** – validate the identity of TPPs ensuring fraudulent TPPs cannot access FIs APIs
   - **Consent Management** – Tokenisation services to meet the requirements of PSD2 schema use cases
   - **Immutable Audit** – provides FI with a system of record of all activity and actions that can be presented to a regulator if a dispute arises
2. **Removal of complexity** – integration of RESTful APIs to deliver the above services, thus reducing significant costs for FIs to integrate to multiple regulatory and eIDAS databases
3. **Speed of implementation** - dedicated SaaS solution that can be quickly and easily deployed
4. **Performance** - service has been built to be deployed in a cloud based, micro services architecture to provide scalability, throughput and elasticity
5. **Reliability** – resilient system design to underpin maximum availability and fault tolerant, live-live distributed architecture

Konsentus the only complete solution

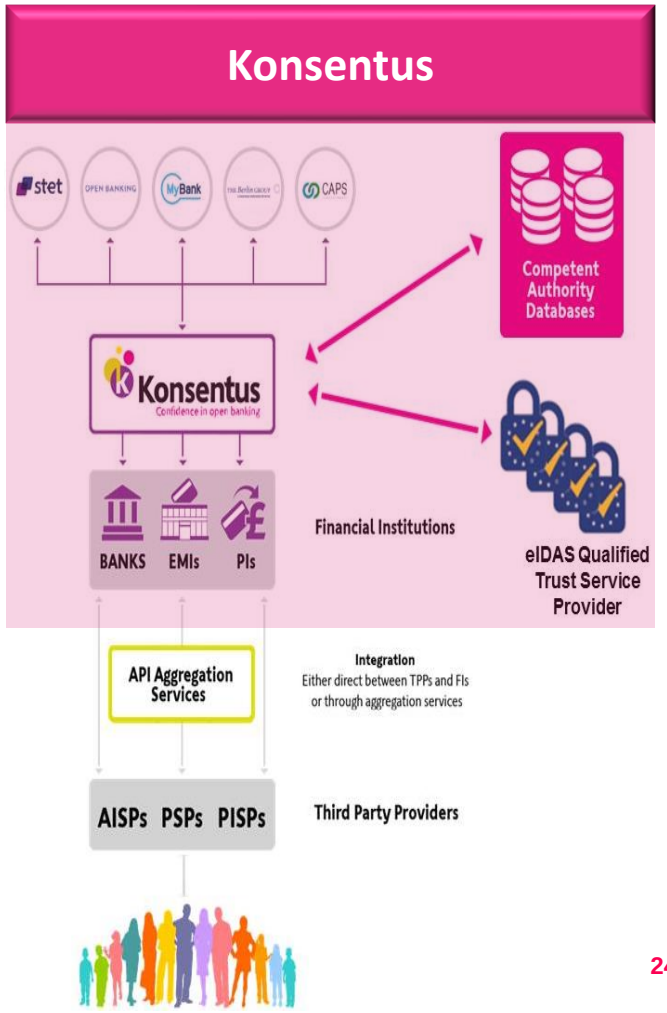
EBA & PRETA

- Central European register of all regulated parties
- Does not support online, real-time automated checking of TPPs
- Does not support eIDAS Certificate checking
- Does not support Consent and Preference Tokenisation Management
- No immutable audit log

LUXHUB

- Full service open banking provider (APIs, aggregation, AISP services)
- Provide a similar suite of regulatory checking services to Konsentus as part of overall offering
- Are not offering regulatory checking services as standalone service

- Konsentus is unique in offering the full regulatory checking services



Executive team

CCO
Brendan Jones
30+ years experience in the UK & international payments industry. Held executive positions in banking, payment & technology companies. Ex Giesecke & Devrient, Bank of America MBNA & Datacard. Developed the Konsentus business from concept to Entity.

CEO
Mike Woods
Ex CEO of Proxama, Board member at Proxama PLC. Ex CEO & founder of Aconite, a payments & technology software company that operates across USA and EMEA. Prior to this spent 17 years at Royal Bank of Scotland and Marks & Spencer.

Finance Director
David Jacks
Big Four Chartered Accountant with 30+ years experience in SME businesses including 15 years in FinTech. Ex FD of Proxama PLC and Aconite. Previous companies include Warner Music and Sega

Chief Product Officer
Paul Meadowcroft
Cyber-security, encryption and payments specialist with 30+ years experience in financial services. Past companies include Thales, Baltimore & Zergo. Paul's focus is security architecture design, secure delivery of data services, ensuring compliance with industry regulation.

Chief Architect
Peter Winfield-Chislett
Payments & technology specialist with 30+ years experience in the financial services industry. Held senior roles in technology, strategy planning and architecture at Visa Europe.

VP Partner Management
Carol Heath
25 years experience in the financial services industry, managing strategic partnerships. Held senior in partner management at Visa Europe managing debit and prepaid activities.

Advisory team

David Parker
CEO Polymath Consulting

Nick Caplan
Chairman of Faster Payments

Leeroy Pye
CEO Tag Nitecrest

Konsentus
Confidence in open banking

Brendan Jones
07785 388867
brendan.jones@konsentus.com

Mike Woods
07740 910227
mike.woods@konsentus.com

David Parker
07712079307
david.parker@konsentus.com