

OPEN BANKING

Helping ASPSPs implement PSD2 and take advantage of Open Banking

January 2019

Version 1.36



We make it easier for ASPSPs to implement PSD2 and take advantage of Open Banking

We have developed a comprehensive suite of Standards and services in partnership with nine of Europe’s largest financial institutions. This has been achieved with extensive input from ASPSP and TPP communities, PSD2 and consumer stakeholder groups.

A proven standard

Our Standards are open to all ASPSPs and, during 2018, have been implemented across 90% of the UK payment accounts market, with circa 100 regulated TPPs and ASPSPs enrolled in the ecosystem, a number that is growing fast.

Through this process we have learned the importance of good implementation. We have therefore developed a suite of Conformance Tools and Implementation Services to support our Standards. We believe this approach can enable regulatory compliance and provide a strong foundation for an innovative and successful market that you can take advantage of.

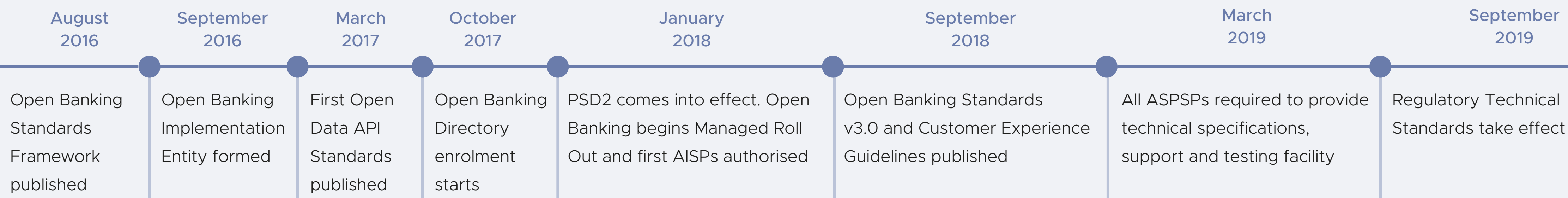
Supporting PSD2 compliance

ASPSPs can be confident that if they implement our Standards correctly they should be PSD2 compliant. The Standards map to EBA guidelines and are supported by Conformance Tools and a Certification option. These are designed to simplify the application for an exemption from the contingency mechanism.

Driving adoption

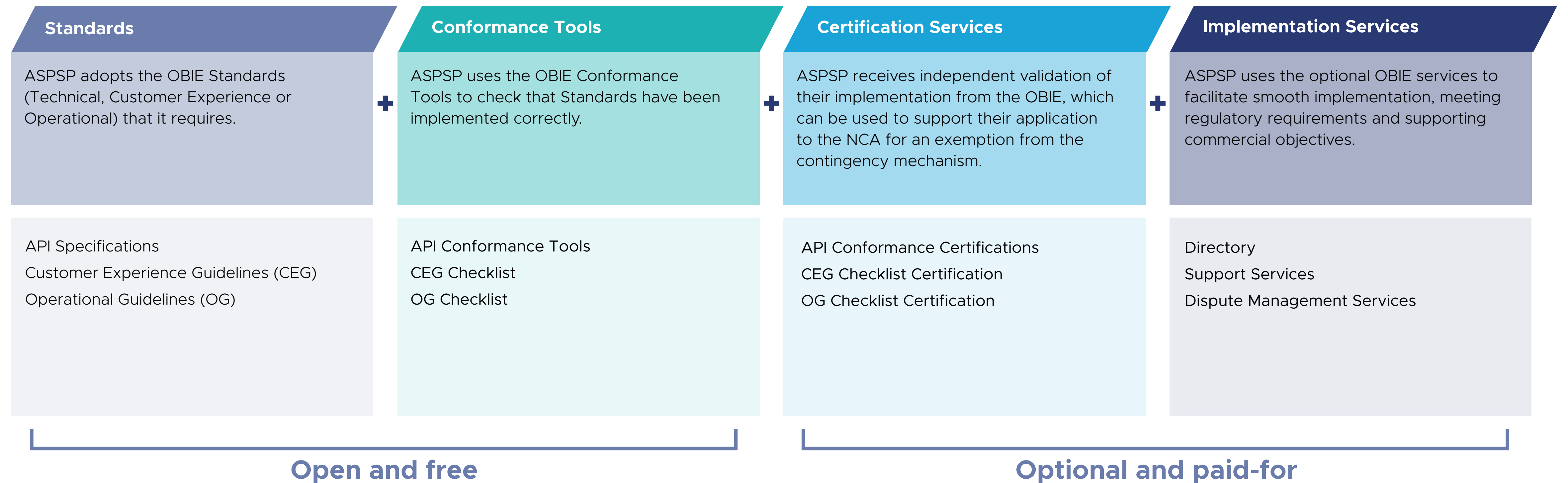
Our optional Implementation Services facilitate the secure and smooth running of the PSD2 ecosystem. For example, the OBIE Directory provides participants throughout the EEA with the ability to easily connect, identify and validate each other, without creating an obstacle for TPPs.

The Open Banking journey

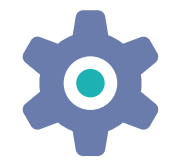


Our end-to-end proposition helps ASPSPs comply with PSD2

We believe API Specifications alone will not deliver a functioning PSD2 ecosystem. Our end-to-end proposition of Standards, Conformance Tools, Certification and Implementation Services are designed to help ASPSPs implement PSD2 with confidence and provide high quality APIs for TPPs. The components are modular. Some are open and free, others are optional and paid-for.



Our Standards are extensible, enabling PSD2 compliance as well as supporting commercial success



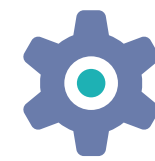
Regulatory Standards



Our Standards are designed to ensure any European ASPSP can meet their PSD2 and RTS requirements, supporting their application for an exemption from the contingency mechanism.

These market-enabling Standards are built in an optional modular format to most effectively meet consumer and market needs.

These Standards go beyond simple Technical Specifications and also include Customer Experience Guidelines and Operational Guidelines.



Commercial Standards

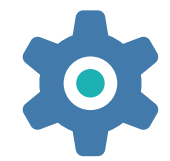


We recognise market demand for additional functionality and have created Standards for optional APIs that go beyond PSD2 requirements. These market-enhancing Standards enable TPPs to develop more compelling propositions, while encouraging ASPSPs to add functionality that can provide smoother, richer and more profitable customer experiences. Commercial APIs may allow ASPSPs to earn a return on their PSD2 investment.

Unlike the Regulatory Standards, the Commercial Standards may involve a contract between the ASPSP and TPP. Examples of Commercial API Standards will include options such as additional information fields (e.g. location or merchant category codes), as well as access to mortgages and savings accounts and the ability to initiate 'customer not present' payments.



Our Regulatory Standards map directly to PSD2 and RTS requirements and are made up of three components.



API Specifications

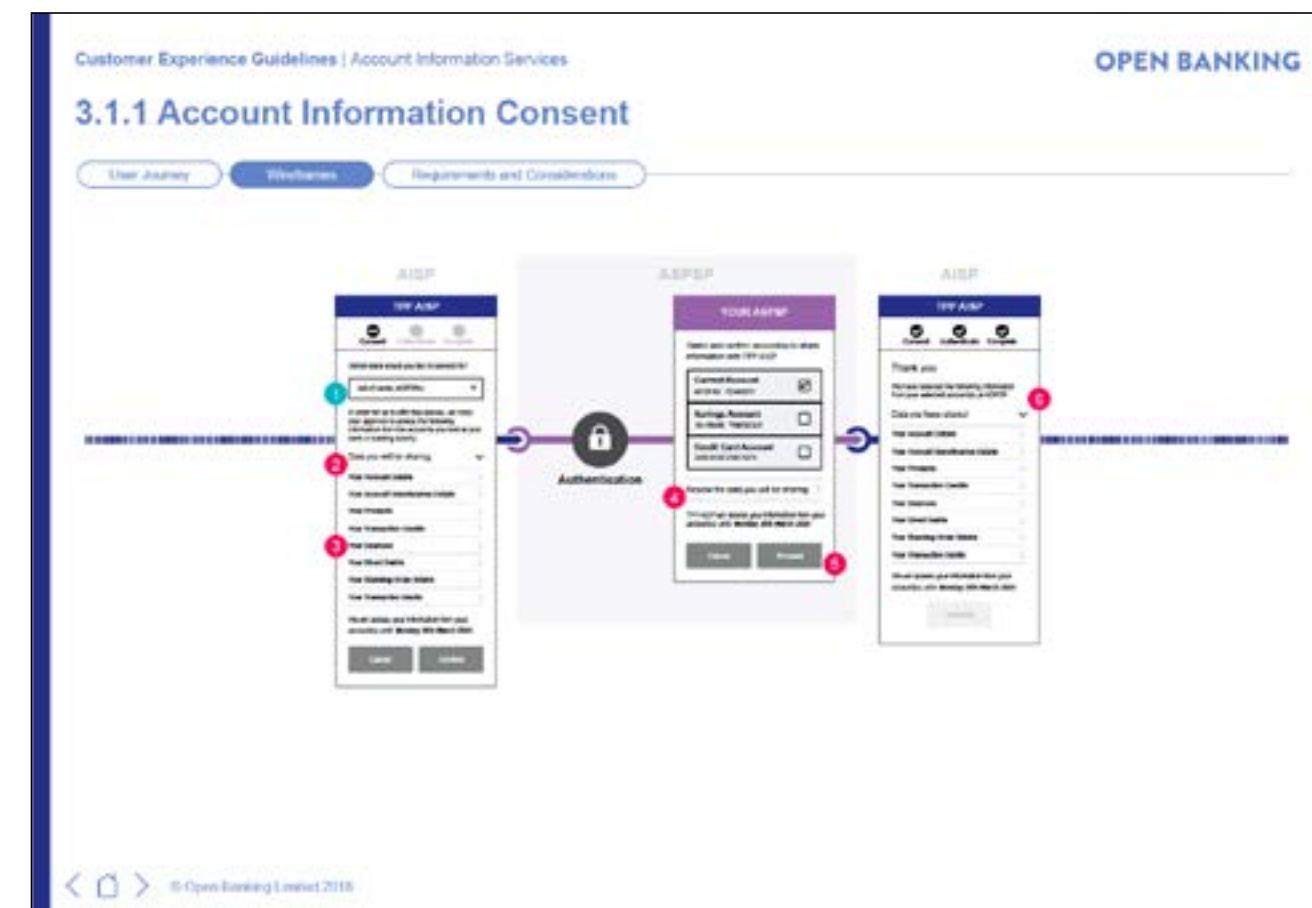
Our API Specifications include documentation, usage examples and swagger files for Account and Transaction Information, Payment Initiation, Confirmation of Funds, Event Notification, and MI Reporting.

We have partnered with the Open ID Foundation to develop security profiles for re-direct flows, decoupled flows, and TPP on-boarding. These include the Financial Grade API (FAPI), Client Initiated Backchannel Authentication (CIBA) and Dynamic Client Registration (DCR) profiles.



Customer Experience Guidelines

The Customer Experience Guidelines ensure that customer journeys deliver a great customer experience and avoid any unnecessary delay or friction as required under PSD2.



Journey Wireframes

ASPSP refers to the relevant journey which is accompanied by CEG Checklist requirement markers ² that demonstrate the mapping to PSD2, RTS and CX considerations ²



Operational Guidelines

Our Operational Guidelines have been designed to support ASPSPs in meeting relevant operational and service requirements, thereby facilitating regulatory compliance with obligations relating to performance and availability, design and testing, problem resolution and management information.

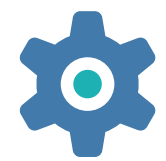
These Standards are open and can be used individually or combined as determined by the ASPSP:

www.openbanking.org.uk/providers/standards/



ASPSPs can use our Conformance Tools to check they have implemented the Standards correctly

We provide a suite of clear, accessible tools to help ASPSPs check they have correctly met our standard implementation requirements.



API Conformance Tools

Our experience shows these tools contribute significantly to seamless integration with TPPs.

Functional Conformance Tools

These allow an ASPSP to test functionality and data elements of their API implementations to ensure conformance with the Technical Specification for each of Account and Transaction API, Payment Initiation API and Confirmation of Funds API.

Security Profile Conformance Tools

These allow an ASPSP to test their API implementation for conformance with OpenID Foundation security profiles for redirect (FAPI profile), decoupled (CIBA profile) and TPP onboarding.



Customer Experience Guidelines Checklist

Our comprehensive checklist ensures that the Customer Experience Guidelines have been implemented correctly. Checklist questions are tracked back to Regulatory References to give ASPSPs and NCAs full transparency. See an example below.

CEG Checklist Requirements	Priority	CEG Checklist	Version	Implementation	CEG Considerations
1. The ASPSP provides the PSU sufficient information to enable the PSU to make an informed decision. For example, when the provider or when the user will be asked to provide consent, the user will have access to the information, functionality and other data that is requested and where the user can revoke consent at any time.	High	3.1.1	1.0	Not Implemented	1. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.
2. The ASPSP provides the PSU with a description of the information requested using the provider and language requirements in OASIS. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.	High	3.1.1	1.0	Not Implemented	2. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.
3. The ASPSP provides the PSU with a description of the information requested using the provider and language requirements in OASIS. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.	High	3.1.1	1.0	Not Implemented	3. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.
4. The ASPSP provides an application for PSD to ensure the user has sufficient information to make an informed decision. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.	High	3.1.1	1.0	Not Implemented	4. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.
5. The ASPSP provides the user with a description of the information requested using the provider and language requirements in OASIS. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.	High	3.1.1	1.0	Not Implemented	5. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.
6. The ASPSP provides the user with a description of the information requested using the provider and language requirements in OASIS. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.	High	3.1.1	1.0	Not Implemented	6. The provider must ensure that the user is aware of the information requested and that the user can revoke consent at any time.



Operational Guidelines Checklist

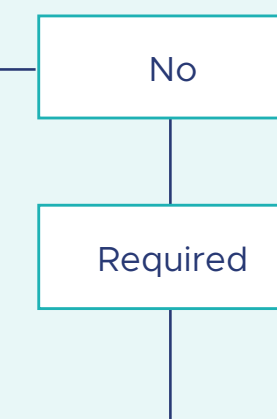
Our comprehensive checklist ensures that the Operational Guidelines have been implemented correctly. Checklist questions are tracked back to Regulatory Requirements to give ASPSPs and NCAs full transparency. The checklist supports ASPSPs in meeting required service levels for performance, availability, testing, problem resolution and management information.

Each requirement on the Checklist Requirements table links to the relevant question on the Customer Experience Checklist, an example of which appears below.

Example question

At any point during the Open Banking customer journey, do you ask the PSU for consent for the TPP to access account information or initiate a payment?

Answer must be
Open Banking Implementation Requirements



Regulatory reference(s)

EBA Opinion paragraph 13
EBA Draft Guideline 5.2 (c) and paragraph 34 (c)
RTS Art. 32(3)
FCA Approach Document paragraph 17.48



Certification Services allow ASPSPs to demonstrate independent validation of their implementation by the OBIE

Our Certification Services help ASPSPs demonstrate how they have met our implementation requirements. This enables an ASPSP to provide the NCA with an independent validation against a recognised market initiative when they request an exemption from the contingency mechanism.

Features of the OBIE Certification process:

Defined process

Clearly documented end-to-end process for certification can support an application for exemption.

Modular certificates

ASPSPs can choose to demonstrate their adherence to the Standards by obtaining certificates for individual aspects of the OBIE Standard.

Ongoing engagement

Continued dialogue throughout the implementation process helps ASPSPs certify successfully.

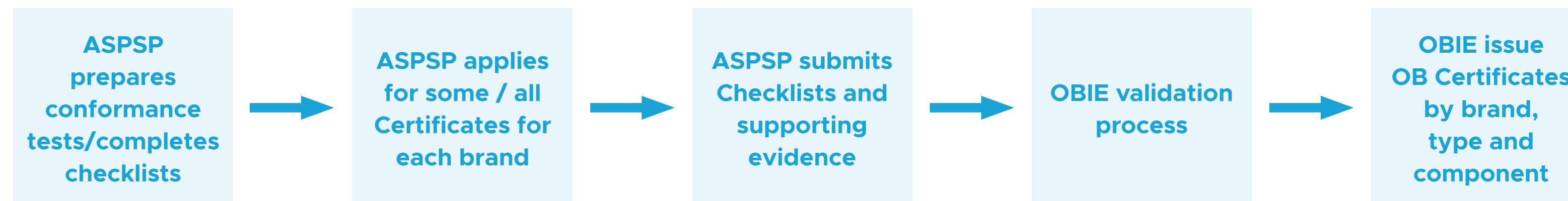
Clear information

Certificates allow all participants to fully understand the extent to which an ASPSP conforms to Standards.

Compliance checks

Caters for changes to Standards and supports ongoing wishes for ASPSPs to showcase improvements.

OBIE Certification Process



Implementation Services are designed to facilitate smooth implementation and market adoption

We have learned from experience how important good implementation is to ensuring PSD2 and open banking is a success for the ASPSP, TPP and TSP ecosystem.

This led us to develop a suite of Implementation Services that help all participants lower the cost and risk of implementation and deliver better end-user experiences. **All our implementation services are optional**, which means they can be used with or without the OBIE Standards, Conformance Tools or Certification Services.



Directory

An identity and access management platform which provides additional optional capabilities to make it easier and more secure for TPPs to onboard with ASPSPs, and to reduce the risk and cost for ASPSPs in validating identity and regulatory status of a TPP.



Support

Participants can benefit from our team providing market leading business, technical and communications expertise, both during the onboarding process and on an ongoing basis.



Dispute Management

A streamlined communication platform that helps end-user and market participants raise and manage enquiries, complaints and disputes in a way that's clear, consistent, transparent and ethical.

Directory

We facilitate a vibrant, connected ecosystem through a comprehensive directory already used by circa 100 participants. The Directory will be fully compatible with PSD2/RTS eIDAS requirements and offers the following functionality:

Organisation Authorisation Validation

Checks regulatory status of organisations in real time, across 31 National Competent Authorities.

Software Identity

Allows organisations to create identities for multiple brands and ensures these are visible to PSUs under the correct brand name, which will enable better adoption and reduce the volume of PSU queries.

Sandbox

Gives participants confidence in the onboarding and integration of open banking tools.

API Endpoint Directory

Accessible, consolidated place to help organisations easily find the API endpoints that an ASPSP supports through both Regulatory and Commercial APIs.

Security Management

Allows organisations to support their multiple brands by easily creating and managing multiple software statements, and facilitating re-cycling of keys, which provides significant security enhancements.

Discovery and Notification

Central address book of contact details which enables ASPSPs and TPPs to discover each other, and facilitates a central notification service.

Standout functionality for a stronger infrastructure

eIDAS lookup	✓
Regulatory Status check	✓
Trust Service Provider (alternative to eIDAS)	✓
Software Identity Management	✓
Software Identity Self Service Management	✓
Identity Self Service Management	✓
Participant Operational Information	✓
Participant Contact Information	✓
Regulatory Status Call / Cache capability	✓
Regulatory revocation notification	✓
Test version of the Directory	✓
Testing capability for unregulated entities	✓
Supports functionality beyond regulatory needs	✓





Support

We manage service desks and offer expert, impartial advice to ensure smooth implementation and integration between ASPSPs and TPPs. Our objective is to help all participants take full advantage of open banking opportunities.

Business support

Expert support for open banking services, reducing time to market, cost and ensuring a more mature engagement.

- Live access to experienced support team
- Enrolment support
- User Access
- Buddying connections
- Launch support
- API downtime reports

Technical support

Close collaboration with ASPSPs and TPPs to enable rigorous testing and seamlessly resolve any problems related to technical standards.

- Best in class testing platform
- Issue tracking and ecosystem engagement
- Building and implementing standards
- Onboarding to Directory

Communications support

Helps participants promote their open banking activities to a wider audience through extensive public relations expertise.

- Press release support
- Communication strategy
- Stakeholder engagement
- Events
- Communication and engagement processes





Dispute Management Services

Our optional Dispute Management Services help all participants efficiently and effectively deal with end-user complaints and work in the best interest of the customer.

Dispute Management

The Dispute Management System (DMS) is a communication process for ASPSPs and TPPs that helps organisations manage PSU enquiries, complaints and disputes among themselves, fairly and effectively.

It's a voluntary system built around best practice standards that enables:

- Requests for information or exchange of information
- Requests for a redress repayment (for example, where a party has paid out in response to a complaint or dispute, but believes the liability lies with another party)
- Complaints forwarding

The DMS is a streamlined communication platform that helps participants manage these issues in a way that is clear, consistent, transparent and ethical. It provides:

- An open communication process for ASPSPs and TPPs
- Codification of end user complaints to enable these to be addressed efficiently
- A solution to allow two or more previously unknown parties to engage with each other
- Support to ASPSPs and TPPs in the collection of information from other necessary parties
- Support to ASPSPs and TPPs in delivering an improved customer experience
- Governance around management of payment initiation and account information service transaction-related enquiries, complaints or disputes

The Open Banking Standards can help you implement PSD2 and take advantage of Open Banking

Facilitate your exemption process

Our Regulatory Standards and Conformance Tools can help implement PSD2 in a compliant way whilst minimising the cost and risk of rework. Our Certificates can become supporting evidence for your application from an exemption from the contingency mechanism.

Create opportunities

Our Commercial Standards can help you monetise your PSD2 investment by offering commercial APIs to TPPs.

Nine reasons to partner with Open Banking to facilitate PSD2 compliance

- ✓ Standards can be used by any ASPSP across Europe
- ✓ Goes beyond technical requirements to offer the world's most extensive Standards
- ✓ ASPSPs can 'pick and choose' from Standards that are most relevant to them
- ✓ Commercialise API opportunities with the UK's world leading and globally innovative FinTech sector
- ✓ Built with backing from major international financial institutions
- ✓ Engagement with governing bodies all around the world is helping to create a truly international network
- ✓ Comprehensive user experience considerations to provide standout customer engagement and market adoption
- ✓ The first market initiative to launch open banking in Europe
- ✓ Live ecosystem since January 2018 now with circa 100 participants

To join the OBIE ecosystem, get involved in shaping our Standards, or simply get more information contact us at:

<http://www.openbanking.org.uk/contact-us/>

A woman with curly hair and glasses, wearing a light-colored shirt, is smiling and looking at a laptop screen. A man with glasses and a beard, wearing a checkered shirt, is sitting next to her, also smiling and looking at the screen. They are in an office environment with a window in the background showing a cityscape.

Together we can make PSD2 a regulatory and commercial success

© 2019 Open Banking Limited

Published by Open Banking Limited, a company limited by guarantee
and incorporated and registered in England with company number 10440081
whose registered office is at 2 Thomas More Square, London E1W 1YN, UK