

# Berlin Group **open**Finance



---

**An open API Standard for  
the Financial Industry**

---

# Why **open**Finance?

PSD2 XS2A set the regulatory reference for consent-driven data access and enabling third parties to trigger a payment. One of the main intentions of PSD2 was to foster innovation and competition in the European banking market. While a first step has been made, more is needed to truly achieve this objective.

Upon customer consent, PSD2 ensures access to datasets on a bank customers' payment account. The defined roles for payment initiation and account information allow to provide basic payment services. Compared to other payment means, these will not allow to unleash the full innovation potential.

**open**Finance aims to expand the access of customers' financial data to broader data sources and additional account types, such as e.g. savings, loans, investments. This offers enhanced views on customers' data and will empower bank customers to actively choose the best value products and services they need. Further it helps to improve the basic credit transfer with additional functionalities (e.g. flexible execution and document handling) and enables the creation of new payment and credit services. The **open**Finance services will attune to the ambitions of the European Central Bank and European Commission's Digital Finance Strategy and to any relevant API Access Scheme definition. The services also allow new business models and optimisation of existing processes.

**open**Finance will affect how future digital financial services are designed, built and distributed.



# Berlin Group **open**Finance

More than 75% of PSD2-mandated banks and hundreds of Third Party Providers (TPPs) have already decided to implement the Berlin Group NextGenPSD2 Framework and the standard has met strong adoption and support outside the PSD2-mandated countries as well. In unleashing the full

potential of the NextGenPSD2 API Framework technology, Berlin Group **open**Finance focuses on a broader and complementary perspective, beyond regulatory services, and adds standardised extensions that enable bank customers (consumer or corporate account owners), directly or via the TPP, to access bank accounts for commercial premium services and data.

THE *Berlin* GROUP

A EUROPEAN STANDARDS INITIATIVE



Leveraging the NextGenPSD2 technology and infrastructure investments, **open**Finance allows banks and TPPs to offer enhanced services, products and information, that will benefit market participants and will further improve customer experiences.

In a unique partnership, participants in Berlin Group **open**Finance are working together with the common vision that open and harmonised **open**Finance interface standards for processes, data and infrastructures are the necessary building blocks of an open, interoperable market. True interoperability is an essential component of competitive **open**Finance services and will contribute to further progress towards the European Single Market and benefit the payments industry in general and European consumers and businesses in particular.

Berlin Group

**open**Finance | The next evolution in Banking Services



OFFICES



ONLINE BANKING



MOBILE BANKING



PSD2 OPEN BANKING

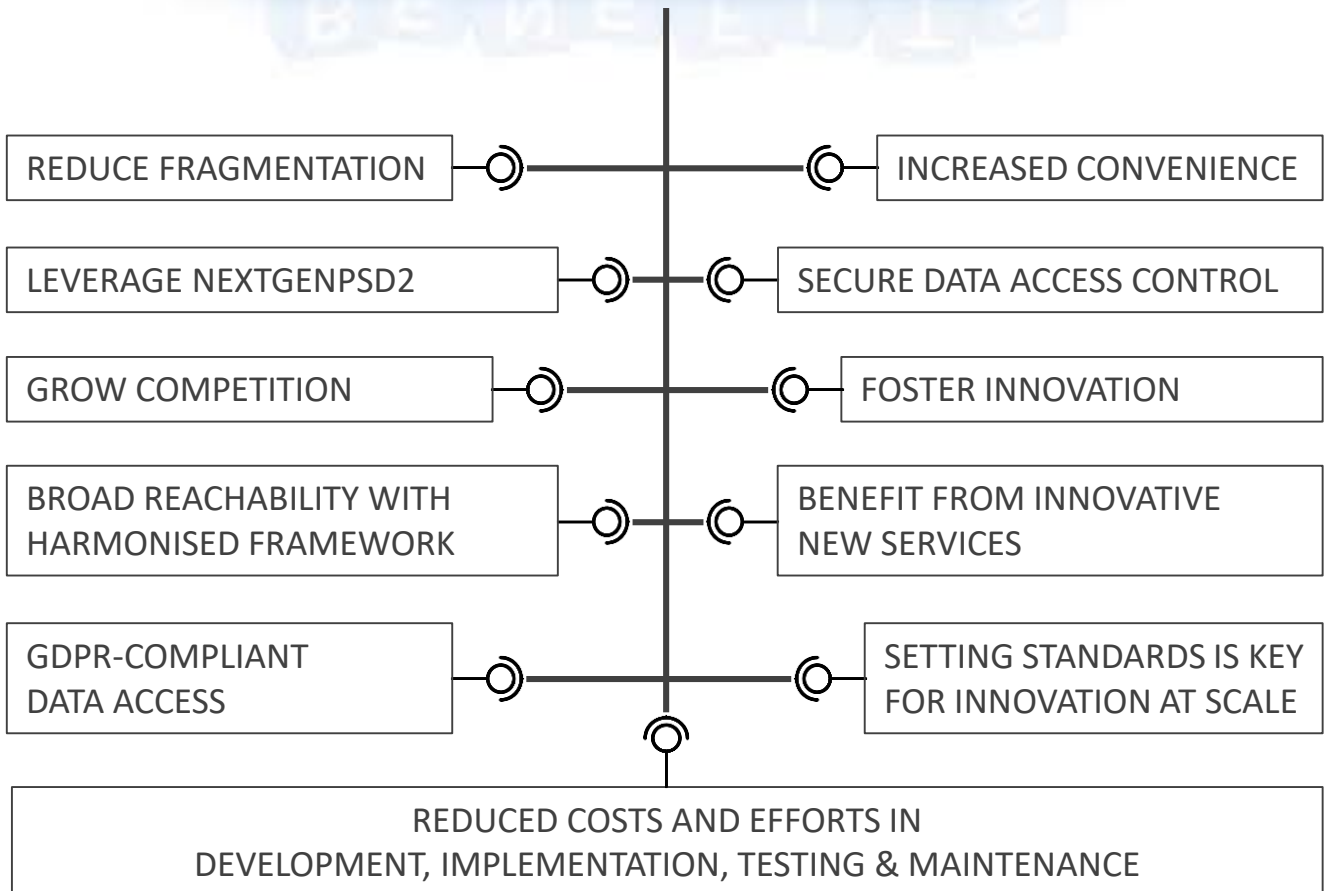


**OPEN**FINANCE



## Why rely on the **open**Finance API Framework?

- **COMPREHENSIVE:** covering as much as possible the market needs of both users and providers
- **FLEXIBLE:** covering a diverse range of Strong Customer Authentication means
- **EFFICIENT:** re-using existing banking standards and building on PSD2 investments
- **MODERN:** based on newest technologies, such as REST, JSON, etc.
- **COVERAGE:** based on NextGenPSD2 - already implemented in more than 25 countries
- **SECURE:** using secure identification based on eIDAS
- **SIMPLE:** a clear layered model where each actor can choose the parts relevant to him
- **PAN-EUROPEAN:** actors from all over Europe (and beyond) contribute to the framework
- **OPEN:** publicly available under Creative Commons Licence 
- **EXTENSIBLE:** new services will be added upon market requirement



## Berlin Group

The Berlin Group is a pan-European payments interoperability standards and harmonisation initiative with the primary objective of defining open and common standards in the interbank domain. The Berlin Group has been established as a pure technical standardisation body, focusing on detailed technical and organisational requirements to achieve this primary objective. Other standards that have been delivered so far are in the area of card payment processing, Mobile P2P Interoperability and PSD2 Access to Bank Accounts (NextGenPSD2). Decisions on the implementation of the standards delivered by the Berlin Group are left to individual market participants.

Participants to Berlin Group standardisation are from the market supply-side (the providers) and from the market demand-side (the users). More information and a full list of participants can be found on <https://www.berlin-group.org>

## openFinance services

- |  |   |
|--|---|
| Account Information extensions           | <ul style="list-style-type: none"><li>• Basic AIS Service (Core PSD2)</li><li>• Push AIS Services</li><li>• Extended Consent Management (GDPR)</li><li>• Additional Account Types: e.g. Savings, Loans, Securities</li><li>• Premium AIS Services</li></ul>   |
| Payment extensions                       | <ul style="list-style-type: none"><li>• Basic Payments (Core PSD2)</li><li>• (Recurring) Reservation of Funds</li><li>• (Partial) Deferred Payments</li><li>• (Multiple) Recurring Payments</li><li>• Request to Pay</li><li>• Verification of Payee Service</li><li>• Pay by Loan (integrated Consumer Loans)</li><li>• Mandate Service for Direct Debits</li><li>• Integrated ID Data service</li></ul> |
| Trade extensions                         | <ul style="list-style-type: none"><li>• Mortgage/Loan Management</li><li>• Securities Ordering</li><li>• Trade Finance</li><li>• Document Services</li><li>• Direct Access for Corporates and Wallets</li></ul>   |
| API Management                           | <ul style="list-style-type: none"><li>• Discovery API (Bank Parameter)</li><li>• Client Parameter API</li></ul>   |
| Administration and Registration services | <ul style="list-style-type: none"><li>• Pricelist API</li><li>• Digital Contract API</li><li>• Admin Services</li></ul>   |

## Technical Characteristics

- |                                     |   |
|-------------------------------------|---|
| Transport Protocol                  | <ul style="list-style-type: none"><li>• HTTP version 1.1</li><li>• TLS version 1.2 or higher</li></ul>                      |
| Applicative Protocol                | <ul style="list-style-type: none"><li>• REST with HAL support</li></ul>   |
| Client (PSU) Authorisation Protocol | <ul style="list-style-type: none"><li>• redirect/OAuth2, decoupled, embedded</li><li>• Signatures (direct access)</li></ul> |
| Characterset                        | <ul style="list-style-type: none"><li>• UTF-8</li></ul>   |
| Data formats                        | <ul style="list-style-type: none"><li>• JSON &amp; XML</li></ul>  |
| Data model origin                   | <ul style="list-style-type: none"><li>• ISO 20022</li></ul>   |
| Identifier naming convention        | <ul style="list-style-type: none"><li>• ISO 20022 extended names</li></ul>  |

## Interface Characteristics

- Third Party Provider access beyond PSD2
- GDPR compliant consent model beyond PSD2
- Support of Direct Access for PSUs / Corporates
- eCommerce support
- Discovery service to obtain the specific implementation details
- Multilevel SCA/Corporate Banking support

## Security Features

- |                              |   |
|------------------------------|---|
| Transport Layer              | <ul style="list-style-type: none"><li>• Mutual TLS</li></ul>  |
| Access Client Identification | <ul style="list-style-type: none"><li>• <b>Transport Layer (mandatory)</b><ul style="list-style-type: none"><li>• QWACS eIDAS certificates</li></ul></li><li>• <b>Application Layer (optional)</b><ul style="list-style-type: none"><li>• QSEALS eIDAS certificates</li><li>• Corporate Seal certificates</li></ul></li></ul> |
| API Provider Identification  | <ul style="list-style-type: none"><li>• Based on TLS</li></ul>  |
| Signatures                   | <ul style="list-style-type: none"><li>• Sign http messages (maintain)</li><li>• JSON Web Signature (JWS)</li></ul>  |
| Client (PSU) authentication  | <ul style="list-style-type: none"><li>• All SCA methods of the client</li></ul>   |
| Data encryption              | <ul style="list-style-type: none"><li>• Based on TLS</li><li>• JSON Web Encryption (JWE)</li></ul>  |
| Fraud detection              | <ul style="list-style-type: none"><li>• Based on PSU device related data</li><li>• Further mitigation measures will be published by security bulletins</li></ul>  |

## Documentation