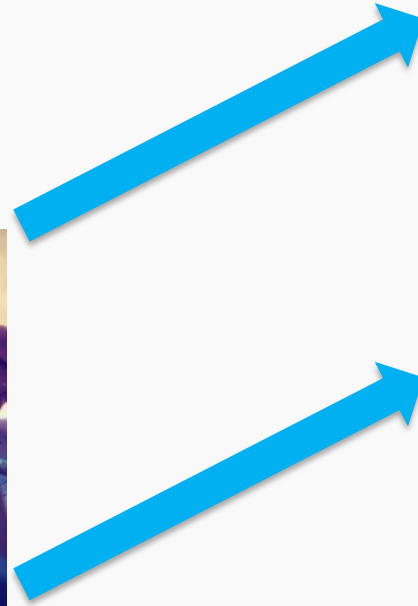


From Open Banking to Open Finance

BACKGROUND & STRATEGIC CONTEXT - STATUS UPDATE - FUTURE OUTLOOK



The Berlin Group in a nutshell



- ◆ Name derives from the first meeting in Berlin in October 2004
- ◆ Pan-European payments interoperability standards and harmonisation initiative

Objectives

- ◆ Meet and complement the SEPA (Single Euro Payments Area) aims and vision of the European Central Bank, the European Commission, the ERPB (Euro Retail Payments Board) and the EPC (European Payments Council)
- ◆ Contribute to SEPA unbundling by defining open and common scheme- and processor-independent standards, fostering open market access, increased competition, more innovation and efficient SEPA services
- ◆ Focus on technical and organisational requirements, independent from payment schemes and business arrangements

- ◆ Implementation decisions left to individual market participants
- ◆ More information: www.berlin-group.org

Outline



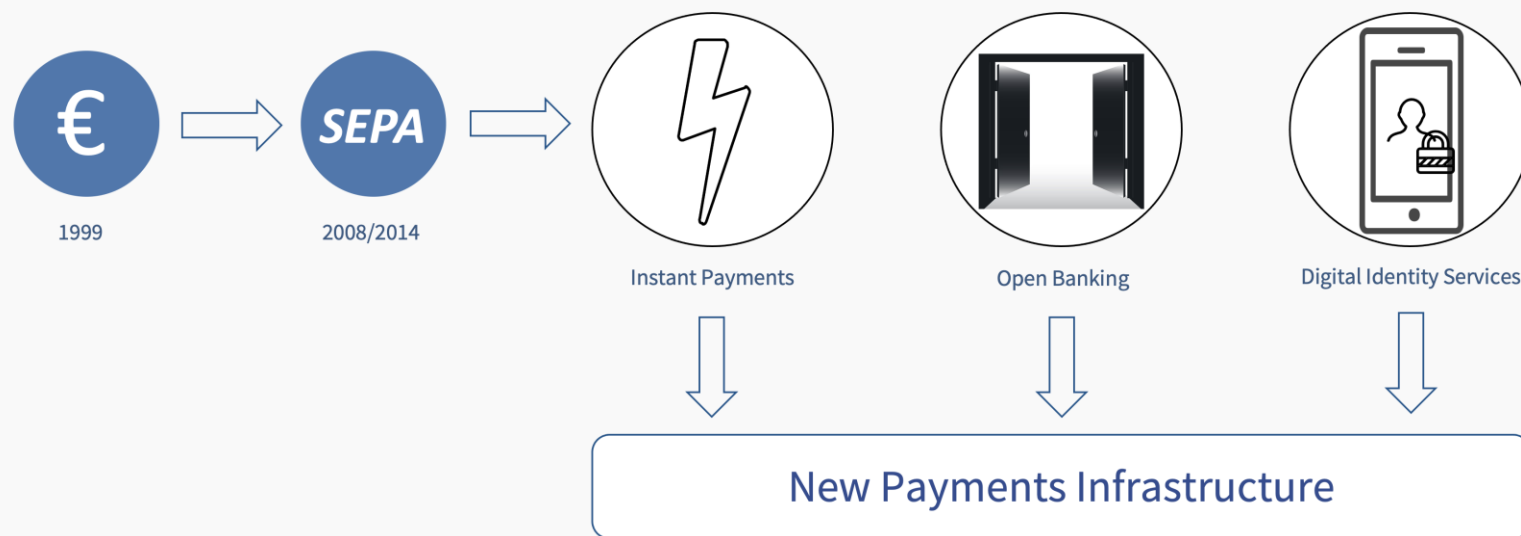
BACKGROUND & STRATEGIC CONTEXT

STATUS UPDATE

FUTURE OUTLOOK

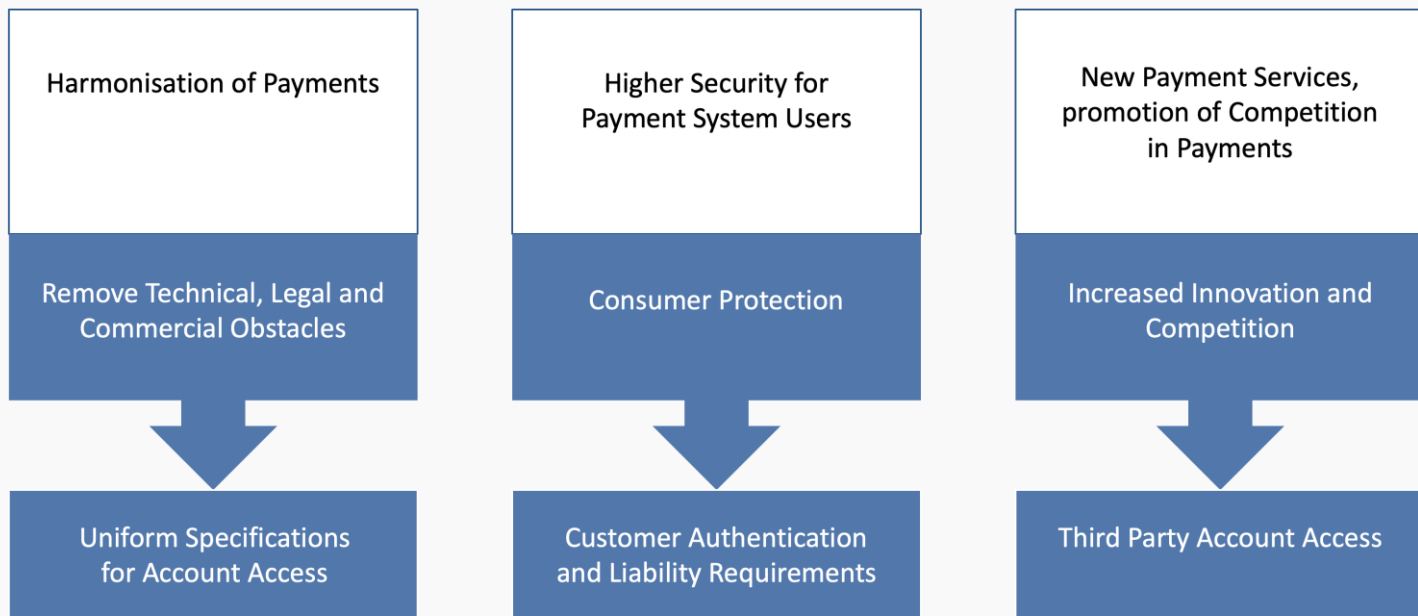


Europe | Preparations towards the “Digital Economy”



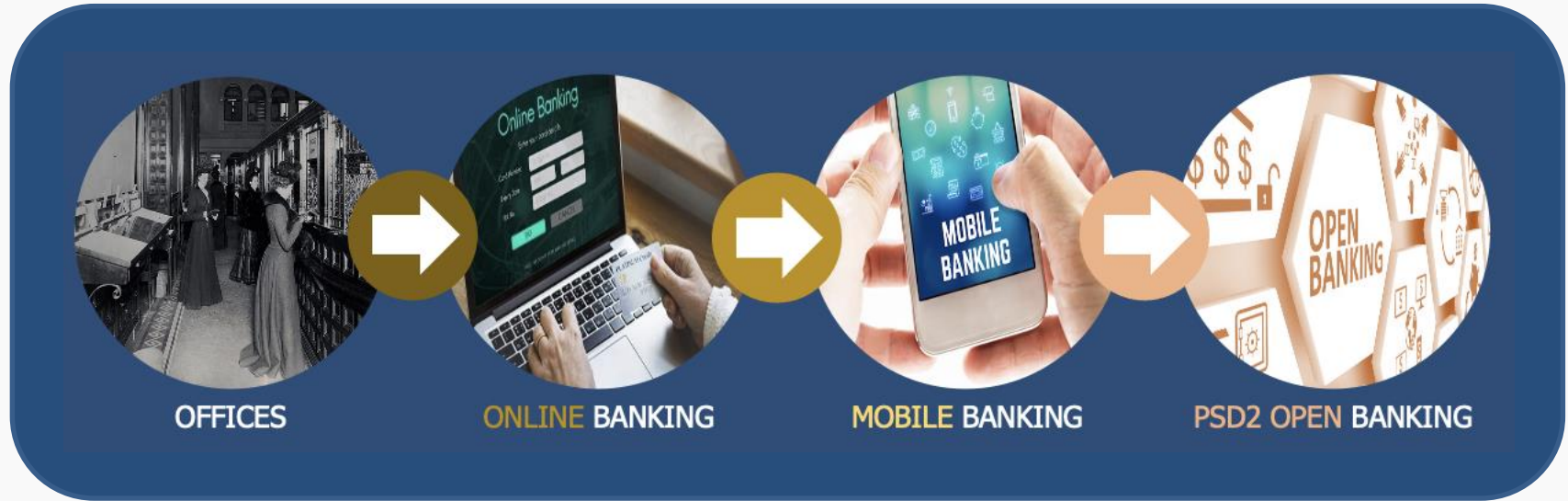


Open Banking | What is it all about? (PSD2 Objectives)



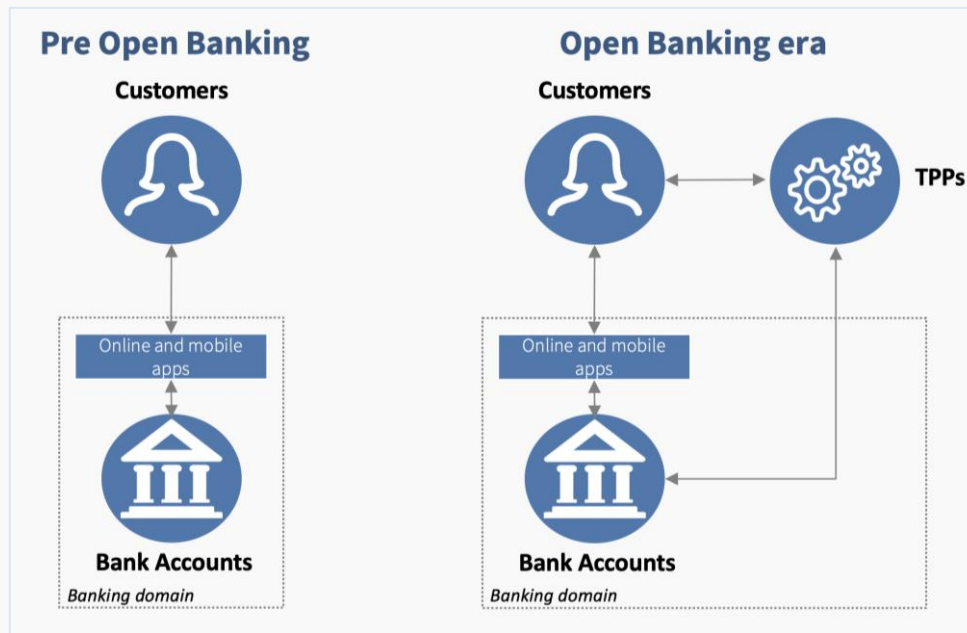


Open Banking | The next Big Shift in Banking Services





Open Banking | Impact on payments value chain





Open Banking | Regulatory Requirements

◆ Subset of most relevant articles in PSD2 and EBA RTS

Requirement	Article		
Enabling CBPIIs, AISP and PISPs to access the necessary data from payment accounts accessible online	Articles 65, 66 and 67 PSD2 Article 30 RTS	Allowing AISPs and PISPs to rely on all authentication procedures issued by the ASPSP to its customers	Article 97(5) PSD2 Article 30(2) RTS
Conforming to (widely used) standard(s) of communication issued by international or European standardisation organisations	Article 30(3) RTS	Enabling the AISP to access the same information as is accessible to the individual consumer and corporates in relation to their designated payment accounts and associated payment transactions	Article 67(2)(d) PSD2 Articles 30(1)(b) and 36(1)(a) RTS
Allowing the payment service user (PSU) to authorise and consent to a payment transaction via a PISP	Article 64(2) PSD2 Article 30(1)(c) RTS	Enabling the ASPSP to send, upon request, an immediate yes/no confirmation to the PSP (PISP and CBPII) on whether or not there are funds available	Article 36(1)(c) RTS
Enabling PISPs and AISPs to ensure that, when they transmit the personalised security credentials issued by the ASPSP, they do so through safe and efficient channels	Articles 66(3)(b) and 67(2)(b) PSD2	Enabling dynamic linking to a specific amount and payee, including batch payments	Article 97(2) PSD2 Article 5 RTS
Enabling the identification of the AISP/PISP/CBPII and supporting eIDAS certificates	Articles 65(2)(c), 66(2)(d) and 67(2)(c) PSD2 Articles 30(1)(a) and 34 RTS	Enabling the ASPSP to apply the same exemptions from SCA for transactions initiated by PISPs as when the PSU interacts directly with the ASPSP	Articles 18(2)(c)(v) and (vi), 18(3), 30(2) and 32(3) RTS
Allowing 90-day reauthentication for AISPs	Article 10(2)(b) RTS	Enabling SCA composed of two different elements	Article 4 RTS
Enabling the ASPSPs and AISPs to count the number of access requests during a given period	Article 36(5) RTS	Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII, mitigating the risk of any misdirection of communication to other parties	Articles 28 and 35 RTS
Allowing a change control process	Article 30(4) RTS	Ensuring security at transport and application levels	Article 97(3) PSD2 Articles 30(2)(c) and 35 RTS
Allowing the possibility of cancelling an initiated transaction in accordance with PSD2, including recurring transactions	Articles 64(2), 80(2) and 80(4) PSD2	Supporting the needs to mitigate the risk of fraud, have reliable and auditable exchanges and enable providers to monitor payment transactions	Article 97(3) PSD2 Articles 3, 22 and 35 RTS
Allowing error messages explaining the reason for the unexpected event or error	Article 36(2) RTS	Allowing traceability	Article 29 RTS
Supporting access via technology service providers on behalf of authorised actors	Article 19(6) PSD2	Allowing the ASPSP's dedicated interface to provide at least the same availability and performance as the user interface	Article 32 RTS



Open Banking | Regulatory Requirements

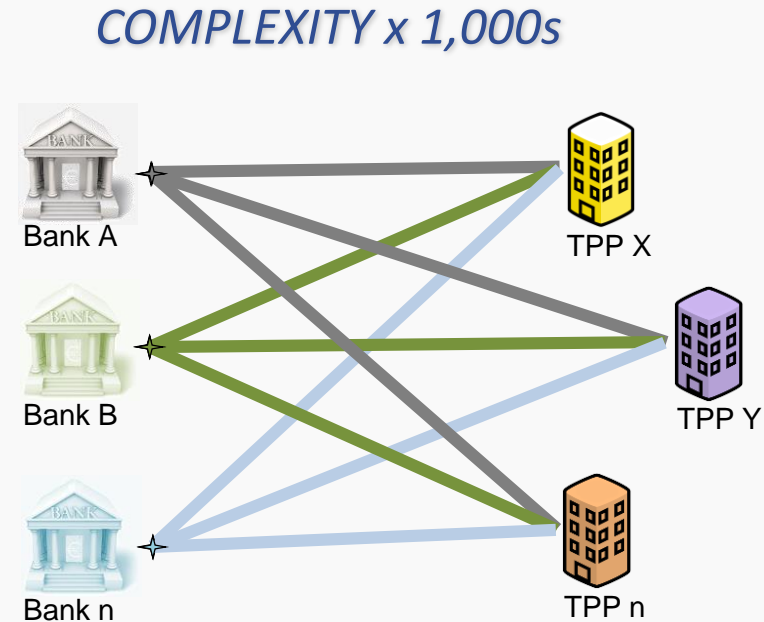
- ◆ Subset of most relevant articles in PSD2 and EBA RTS

Requirement	Article		
Enabling CBPIIs, AISP and PISPs to access the necessary data from payment accounts accessible online	Articles 65, 66 and 67 PSD2 Article 30 RTS	Allowing AISPs and PISPs to rely on all authentication procedures issued by the ASPSP to its customers Enabling the AISP to access the same information as is accessible to the individual	Article 97(5) PSD2 Article 30(2) RTS Article 67(2)(d) PSD2
Conforming to (widely used) standard(s) of communication issued by international or European standardisation organisations		Article 30(3) RTS	
security credentials issued by the ASPSP, they do so through safe and efficient channels	PSD2	payments	Article 5 RTS
Enabling the identification of the AISP/PISP/CBPII and supporting eIDAS certificates	Articles 65(2)(c), 66(2)(d) and 67(2)(c) PSD2 Articles 30(1)(a) and 34 RTS	Enabling the ASPSP to apply the same exemptions from SCA for transactions initiated by PISPs as when the PSU interacts directly with the ASPSP	Articles 18(2)(c)(v) and (vi), 18(3), 30(2) and 32(3) RTS
Allowing 90-day reauthentication for AISPs	Article 10(2)(b) RTS	Enabling SCA composed of two different elements	Article 4 RTS
Enabling the ASPSPs and AISPs to count the number of access requests during a given period	Article 36(5) RTS	Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII, mitigating the risk of any misdirection of communication to other parties	Articles 28 and 35 RTS
Allowing a change control process	Article 30(4) RTS	Ensuring security at transport and application levels	Article 97(3) PSD2 Articles 30(2)(c) and 35 RTS
Allowing the possibility of cancelling an initiated transaction in accordance with PSD2, including recurring transactions	Articles 64(2), 80(2) and 80(4) PSD2	Supporting the needs to mitigate the risk of fraud, have reliable and auditable exchanges and enable providers to monitor payment transactions	Article 97(3) PSD2 Articles 3, 22 and 35 RTS
Allowing error messages explaining the reason for the unexpected event or error	Article 36(2) RTS	Allowing traceability	Article 29 RTS
Supporting access via technology service providers on behalf of authorised actors	Article 19(6) PSD2	Allowing the ASPSP's dedicated interface to provide at least the same availability and performance as the user interface	Article 32 RTS



Open Banking | Standards Development

- ◆ High IT complexity and high costs when each bank develops, documents, tests, and maintains its own proprietary standard
 - ◆ High network complexity
 - ◆ High testing efforts and operational risks
 - ◆ High documentation efforts
 - ◆ Risk increase due to pan-European scale



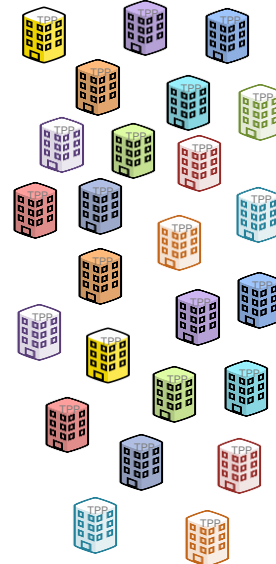


UNIFORM AND INTEROPERABLE
COMMUNICATIONS
BETWEEN BANKS AND TPPS

Banks



TPPs



THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

★ ★ ★
NEXTGENPSD2
FRAMEWORK
★ ★ ★

API*

**APIs have to comply to the standards and will
not be provided by the Berlin Group*

Outline



BACKGROUND & STRATEGIC CONTEXT

STATUS UPDATE

FUTURE OUTLOOK

Status Update

1



> 3,200 banks have implemented
NextGenPSD2



NEXTGENPSD2 TASKFORCE

64 organisations from **27** countries
coordinate the standards development



NEXTGENPSD2 ADVISORY BOARD

78 TPPs, FinTechs, IT providers, Merchants
counsel on future evolution

Status Update

.2



NextGenPSD2 | Taskforce



Status Update

..3



NextGenPSD2 | Advisory Board





NextGenPSD2 Framework | Key Characteristics

- ◆ An open standard for banks to implement a PSD2 compliant Open Banking interface
- ◆ Open for all TPPs to implement to connect to supporting banks
- ◆ Defines a mandatory minimum set of services with a number of optional services
- ◆ Modern 'RESTful' APIs using common internet technologies
- ◆ Data structures either as JSON or XML
- ◆ Data model origin in ISO 20022
- ◆ Identifier naming convention: ISO 20022 extended names
- ◆ HTTP/1.1 with TLS 1.2 (or higher) as transport protocol
- ◆ Four models for Strong Customer Authentication (SCA): redirect, OAuth2, decoupled and embedded
- ◆ Dedicated consent management API
- ◆ Optional session support (set of consecutively executed transactions)



NextGenPSD2 Framework | Supported Services

GENERAL

- Grouping transactions to signing baskets (*optional*)

ACCOUNT INFORMATION SERVICES

- Establish account information consent
- Get list of reachable accounts (*optional*)
- Get account details of the list of accessible accounts
- Get balances for a given account
- Get transaction information for a given account

PAYMENT INITIATION SERVICES

- Initiation of a single payment
- Initiation of a future dated single payment (*optional*)
- Initiation of a bulk payment (*optional*)
- Initiation of a recurring payment (*optional*)
- Cancellation of payments (*optional*)

PAYMENT INSTRUMENT ISSUING SERVICE

- Get confirmation on the availability of funds



NextGenPSD2 Framework | Specification Suite

- ◆ Published for free under Creative Commons (CC-BY-ND): www.berlin-group.org/psd2-access-to-bank-accounts



Outline



BACKGROUND & STRATEGIC CONTEXT

STATUS UPDATE

FUTURE OUTLOOK



Future Outlook | New challenges approaching fast



New Technologies



Customer Requirements



Regulatory Requirements



TPP and Retailer Requirements



Future Outlook | From Open Banking to Open Finance



openFinance | Shaping the future of financial services



Future Outlook | Open Finance in 2021

- ◆ Building on top of the robust NextGenPSD2 architecture and infrastructure investments

openFinance services

Account Information extensions

- Basic AIS Service (PSD2)
- Account Entry Push Notifications
- Extended Consent Management (GDPR)
- Additional Account Types: e.g. Savings, Loans, Securities

Payment extensions

- Basic Payments (PSD2)
- Reservation of Funds
- Deferred Payments
- Request to Pay
- Pay by Loan (integrated Consumer Loans)
- SEPA Direct Debit eMandates
- Integrated ID Data service

Trade extensions

- Loan business
- Securities business (list of stocks, certificates, ...)

API Management

- Discovery API (Bank Parameter)
- Client Parameter API

Administration and Registration services

- Pricelist API
- Digital Contract API



Open Finance | The next evolution in Banking Services



The 2021 Workplan will soon be available on <https://www.berlin-group.org/open-finance>



Summary | Challenges & Lessons learned

- ◆ Diversity of banking payment products and infrastructures across Europe
- ◆ Diversity of authentication methods and infrastructures across Europe
- ◆ Facilitate Retail and Corporate Business
- ◆ In general, banks are no longer considering PSD2 as 'just another compliancy effort'
- ◆ Banks are acknowledging the power of the API economy
- ◆ (est.) approx. 60% of banks adopt a TPP role as well
- ◆ Open Finance enables 're-bundling' of services, leading to new (profitable) customer propositions
- ◆ Sufficient scale and reachability requires industry-wide standardisation efforts

Open Finance allows new business models and customer-centric service propositions



Thank you very much for your attention





THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE



info@berlin-group.org | www.berlin-group.org