Guidelines for PSD2 Implementation

Helping banks explore API strategies and options

CONTENTS:

The PSD2 Directive is permanently changing the way banks interact with FinTechs and other partners. Encouraging greater choice and more innovative services for consumers, it aims to promote competition by levelling the playing field for digital newcomers. Under the directive, banks are obliged to provide an appropriate API interface for authorised third-party access to their customer account data. In this whitepaper, NDGIT outlines some of the key requirements and freedoms for APIs and explores how these impact strategic decision making and PSD2 implementation.

Shifting mindsets and expectations

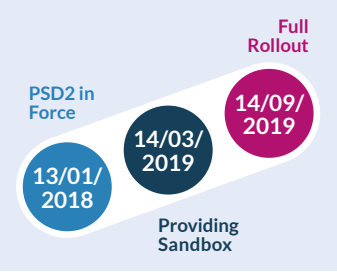
Pre-PSD2 banks had complete sovereignty over their customers‘ account data. Post-PSD2, they must give financial service providers with appropriate authentication and authorisation, the ability to access their customer account data and process their payments and transactions using bank APIs.

For customers, this means more choice, options and services in terms of how they pay, manage and monitor transactions, with the option to obtain consolidated views across their accounts. Banking will become more convenient, more secure and more compatible with other types of financial services. For new financial service providers, PSD2 unlocks the banking world by providing access to accounts (XS2A) and transaction tools to facilitate seamless payment transactions.

However, to make all of this happen, banks must facilitate the infrastructure that enables TPPs to obtain standardised access to requested data. There is a lot to do, timeframes are short and the clock is ticking.

No ‘ifs’ and ‘buts’, banks must act now

The final Regulatory Technical Standards (RTS) for strong customer authentication were published by the European Banking Authority (EBA) in March 2018. Now it’s up to EU banks to prepare for implementation in the form of a functioning interface for external companies.



From 14 March, 2019, banks and payment services must make the appropriate account information and payment release services available to other companies. Initially, this will be in a corresponding test environment with appropriate documentation, with live operation starting from 14 September 2019.

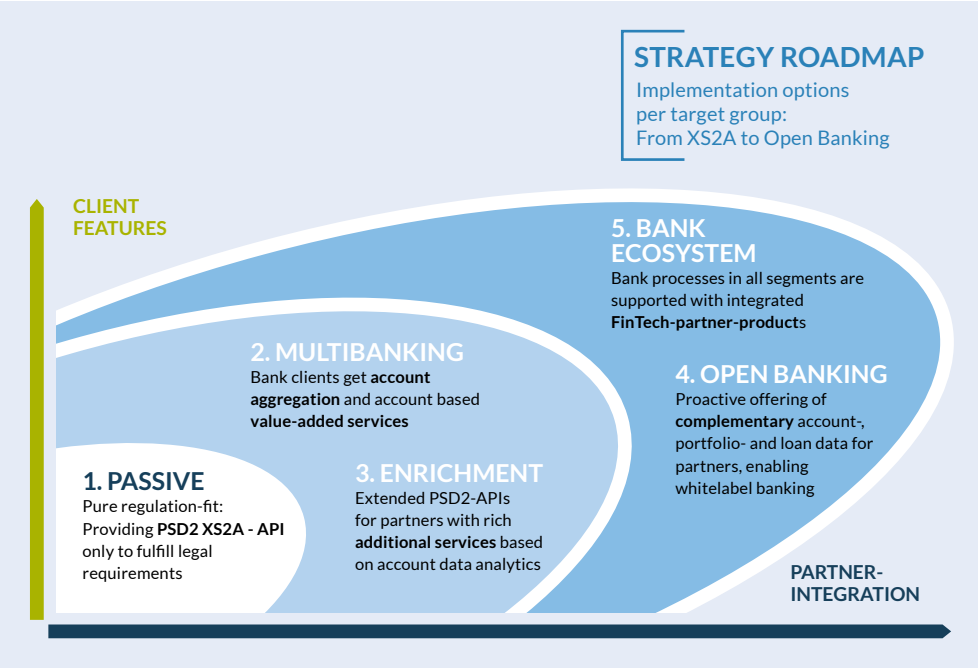
The challenge of choice

So what’s holding them back? One of the challenges facing banks is that the RTS doesn’t provide an established set of rules. Instead, the EBA and the standardisation bodies have set out a number of binding framework conditions and options based on market standards to act as a guideline for implementation.

On the one hand, this provides the advantage of allowing for different paths to technological implementation. On the other hand, banks and financial service providers will have to work out the design of items and workflows themselves.

Many details and use cases still remain open and will be determined soon. For many banks and TPPs this is an onerous task.

Top Five Strategic Considerations for PSD2 Implementation



Forward-looking banks implement an API infrastructure that allows Open Banking services“

So how can banks regain some clarity and simplify this process? Strategically, PSD2 raises a number of key questions and policy decisions that banks have to address before implementing PSD2. Here are NDGIT’s top five strategic considerations for PSD2 Implementation:

1. Invest for compliance or opportunity?

In principle, banks can opt for a minimal implementation of PSD2. This lowest common denominator – also called „compliance only“ – simply ensures that other companies can access a customer‘s account data and execute transactions via PSD2 APIs as required by the EBA.

Forward-looking banks, however, can choose to implement an API infrastructure that allows them to provide their own Open Banking services to digital partners e.g. investment products or loans. This can extend to Banking as a Service, where banks become the central provider of banking products or services for TPPs. In addition, banks have the opportunity to design ecosystems for their customers using open interfaces to deliver TPP’s value-added services, all conveniently filled with bank data.

2. Should we build or buy?

In the past, many companies have opted to develop their own applications and tended to internalise key components of their IT architecture. However, Open Banking platforms and PSD2 solutions present new and unique challenges that may be handled more efficiently using specialised providers with acquired expertise and a range of pre-built, fast to market solutions. With EBA deadlines rapidly approaching, banks should bear in mind that non-compliance can be sanctioned by BaFin or similar financial authorities.

It's unlikely that banks will be able to implement PSD2 without any kind of external support, particularly when it comes to the technological infrastructure and software required for the secure management of partners or automated statistics. Increasingly this will lead to 'hybrid' solutions where banks will use providers such as NDGIT to buy-in technology for the underlying Open Banking platform but will build the surrounding PSD2 framework themselves.

3. To host or not to host?

One crucial decision for banks is whether to host new PSD2-enabled services on-premise, in their own data centre, or to let the TPP implement services using SaaS and to host applications direct.

An on-premise solution requires the bank to regularly install updates and ensure the smooth operation of the underlying infrastructure. With a SaaS solution, the bank simply provides a VPN connection and system access for authentication/authorisation, account data query and payment release functions. All updates, modifications and patches are carried out centrally for multiple customers within a single, unified infrastructure. This greatly reduces the scope and burden of compliance, data protection and IT security, leaving them free to focus on their core business.

4. Can fallback be avoided?

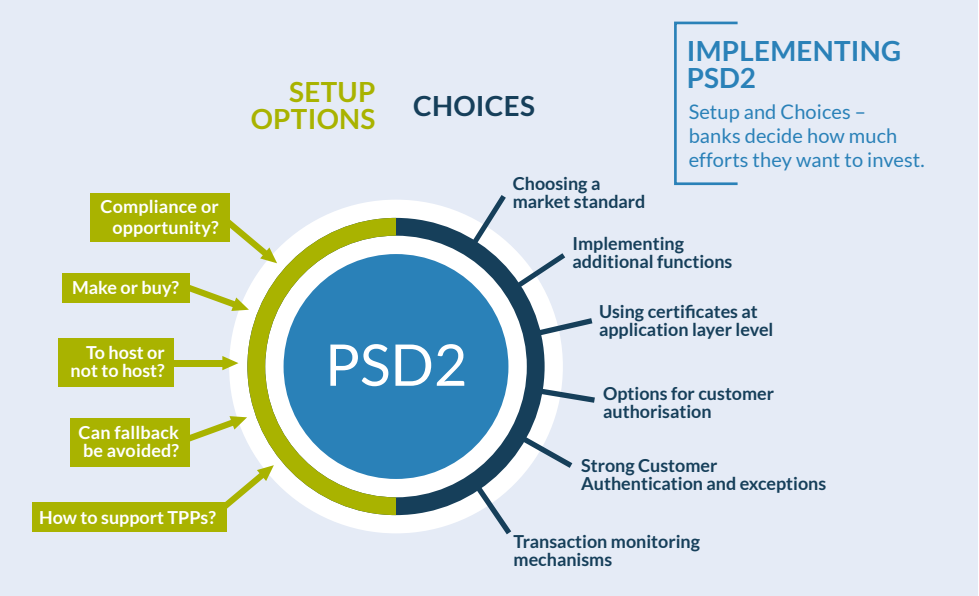
The legislator stipulates that every bank must provide a fallback solution in addition to its standard solution to ensure that even if the TPP's dedicated interface cannot be accessed, the end customer is not precluded from using the services. This fallback solution involves the traditional method of screen scraping an online banking interface, although in most cases the identification of the TPP per certificates is yet to be developed for this purpose.

With the approval of BaFin, it's possible to be exempted from the fallback requirement, if the bank proves to be sufficiently robust in terms of the availability and reliability of its dedicated interface for a period of three months. The exemption is possible from mid-June 2019, if the solution can demonstrate faultless performance right from the start. By avoiding the fallback requirement using a standard solution, helps banks to reduce costs.

To enable them to do this, it's advisable to work with a partner that can demonstrate a successful track record of providing and implementing a PSD2 solution for banks. If they try to achieve this in-house, they may run the risk of falling behind on the technical front and being unable to plausibly demonstrate to BaFin the lack of necessity for a fallback solution.

5. How to support TPPs?

Banks must offer comprehensive 24/7 support to every third-party provider either on their own or through a partner. Whether it's worth organising the support service independently is a matter for each institute to decide. However, it's clear that SaaS solutions from providers that serve many customers can deliver the scalability and cost savings required to make them much more commercially viable.



Implementation options: market standards, additional functions…

It's a plus for banks to provide TPP friendly authentication and optional extra services.“

Reinforcing PSD2's emphasis on freedom and openness, the EBA doesn't provide a concrete definition of PSD2 interfaces. It has explicitly left this up to the market and emerging standardisation bodies. The guidelines for PSD2 APIs are provided by a number of standardisation bodies. The NextGenPSD2 XS2A framework of the Berlin Group is the main standard used in Germany, STET is applied in France, and the UK follows the UK Open Banking Standard.

Here, NDGIT offers a snapshot of the parameters defining the design options of PSD2 APIs.

Choosing a market standard for APIs

In principle, a bank is not obliged to work with a standardised interface at all. However, using one is highly recommended as it's the only way for the financial institution to become a part of a growing industry network and benefit from developments in an ecosystem with common interests. Standardisation offers the bank the chance to join the integration and networking process and thus to share the benefit created.

While most banks choose one standard to follow, dedicated API providers, such as NDGIT, can combine several interface standards on request. This makes sense for large international corporations serving customers and banks in various countries. It also helps them to future-proof their business as PSD2 and RTS evolves, by accessing TPPs' continuously developing software to keep their banking interfaces up to date.

Implementing additional functions

As well as legally mandated account APIs, there are additional services that can be implemented voluntarily. These include forward transfers, mass payments, standing orders and support for multi-level authentication mechanisms in cor-

porate banking. Interface options for such features are already available. Again, many of the most innovative and commercially-savvy banks are seeking to differentiate and make these value-added services more competitive with the help of specialist FinTech providers.

Using certificates at the application layer

Certificates are a security function prescribed by the EBA enabling banks to authenticate third-party providers. The certificate reveals who the accessing partner is and whether they have the necessary permissions for a particular service. At the same time, local or central registers check whether the certificate owner is still in possession of valid TPP authorisation.

A bank already meets the requirements if it performs this certificate query at the transport layer. However, integrating the use of certificates at the application layer, in order to ensure the integrity of the transmitted data with signatures, is even more secure.

Options for customer authorisation

In terms of customer authorisation and access management, the standardisation committees have defined various options for dividing the task of checking authorisations between TPPs and banking software. Digital partners prefer „embedded" options as they ensure a high-quality user experience without confusing context changes. They do this by allowing banks to access credentials entered in the TPPs user interface . However, banks may be more inclined to a „redirect" approach, where customers enter their details directly into the bank interface. This maximises the bank's presence and control, but it may seem less elegant in terms of the user experience. Each bank must decide on the basis of its own corporate culture and its customer expectation which is the right way for them.

> ***Reinforcing PSD2's openness, RTS and Berlin group left a lot of choices to banks."***

Consent management

Consent management is the handling of a customer's access permissions granted to a TPP. The customer can define the level of authorisation and which data can be accessed by the FinTech application in connection with their account. Importantly, they can also delete or revoke permissions too. When it comes to organising consent management, a bank can decide how much control it wants to retain over access permissions and how much control it wants to hand over to the software partner. Read more on Consent Management here.

Strong Customer Authentication (SCA) and exceptions

Two-factor authentication (2FA) is an essential component of PSD2's SCA requirements. However, there are some exceptions where the second factor is not necessary. For example, if payments are made to known partners or secure recipients specified on a whitelist (family members, friends, etc.) or if the user is paying by contactless or using an unattended kiosk for a small, fixed amount e.g. parking fees. Banks have the option of either insisting on 2FA without analysing the transaction details or excluding those cases that are not seen as critical under the law as part of a rule-based risk assessment. The advantage of risk assessment lies in the simplicity for the customer and the improvement of convenience and user experience while maintaining the same level of security. Read more on SCA and exceptions here.

Transaction monitoring mechanisms

Within the framework of PSD2 requirements, there are a number of reporting obligations to national regulatory authorities for instance in Germany to the BaFin. Banks must provide regular information on how many transaction requests have been made, and at what rate, and also provide corresponding benchmarks. Another crucial aspect of this is fraud monitoring and reporting of fraud incidents that have occurred or been prevented. Banks can either do this independently or, in the case of a platform or cloud solution, have the necessary reports and audits carried out by their service provider.

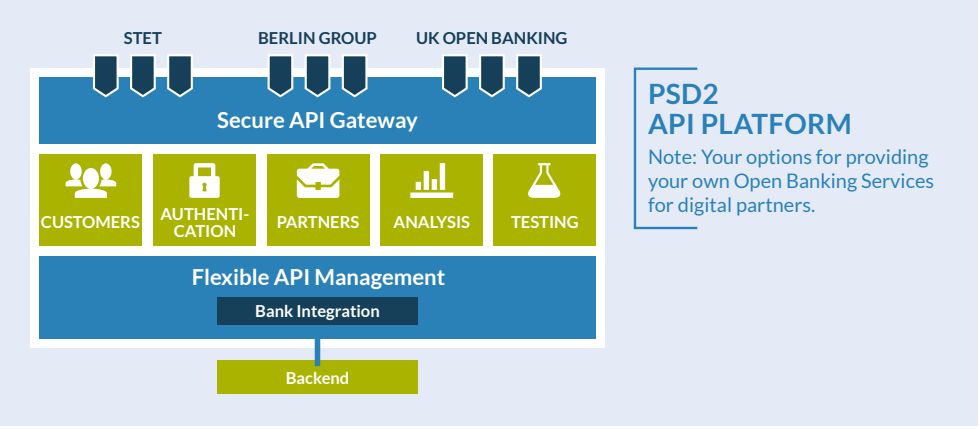
Setting the future course today

Commitment to succeed

The implementation of PSD2 is mandatory and the time frame for banks has been set. Banks must now decide for themselves to what extent and with how much investment and resource they wish to commit to implementing the obligatory PSD2 interface.

When making fundamental decisions that will determine the concrete roadmap, banks should not hesitate to bring external partners into the conversation. When it comes to costs, it's worth bearing in mind that trusting a standard software provider brings synergies based on past experience and proven know-how.

> ***Implementing PSD2 with a platform prepares for all cases, new digital strategies and eventually new regulatory.“***



How NDGIT helps

PSD2 API specialist NDGIT, for example can not only help create the necessary basic infrastructure but also the ability to monetise it through further services in the future. It's already providing banks with all the technical functions they need to implement the directive's requirements and more. Its 'out-of-the-box' solutions can link banking systems with minimal effort and provide a flexible platform to build new Open Banking developments.

NDGIT also delivers clear operational benefits. Its PSD2 APIs conform to Berlin Group, STET or UK Open Banking standards and support these with all the various authorisation approaches and continuous updates to meet any new requirements. NDGIT applications are made available securely to TPPs with the established API management platform and can be operated flexibly as SaaS or from the bank's data

centre. In addition, independent middleware allows updates and extensions to be performed without having to modify the bank interfaces. If required, NDGIT also provides full support for the TPP.

Staying ahead

Whatever implementation options are selected, PSD2 investment is set to influence banks' future commercial success and standing. Banks that see PSD2 as an opportunity to integrate customer-oriented services will opt for a solution that at least complies with the interface specifications of the Berlin Group and ideally also enables additional services thus enabling them to attract TPP partners. Banks that proactively offer such additional services and confidently cooperate with FinTechs will be better placed to drive innovation and accelerate services, make a lasting impression on the end user, reducing churn and growing their customer base.

Contact

info@nextdigitalbanking.com
www.nextdigitalbanking.com

NDGIT GmbH

Ridlerstr. 35a
D-80339 Munich

Tel.: +49 (0)89 1250155 60
Fax: +49 (0)89 1250155 69