www.pwc.at/psd2

The communication between Third Party Providers and Banks.

What will the impact of technology be?

PSD2 in a nutshell

2

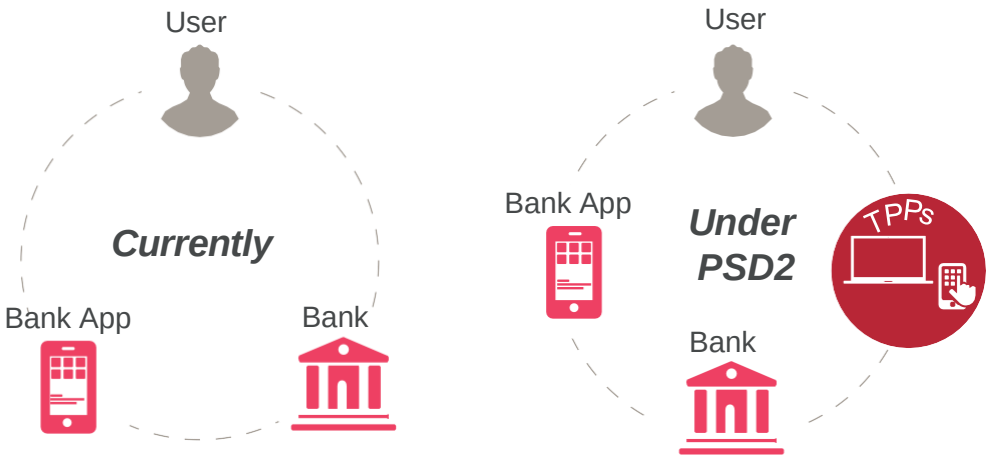
pwc

Summary

The banking system is at a turning point, under the pressure of the market and of emerging operators, who introduce a strong technological push; in this context, Banks will have to decide whether to compete in order to maintain a direct relationship with its customers or to limit their role as to provider of banking services.

The new **Directive on payment services** (PSD2) introduces the possibility for users that use an online banking account to make payments or to access their Bank statements through software developed by authorised third parties (PISP and AISP).

The new players, if authorised, will operate on the Bank accounts of the final users, clearly introducing the risk of disintermediation between Banks and their clients.



This openness towards the market allows the development of new services for customers through the integration and cooperation with other parties in the ecosystem, taking advantage of the interface that Banks will need to make available for customers to access their current accounts.

The **increased complexity** in the payments process chain and the need to ensure **greater security** to payers are the fundamentals that the Directive requires to add:

1. **Secure standards for the dialogue between Third Party Providers and Banks**
   Service payment providers authorised by final customers must enable the access to online accounts through interfaces that are easy to integrate. The principle of the new regulatory framework represents both a market opportunity and a matter of great concern for more traditional Banks, which risk disintermediation from their customers.

2. **Harmonisation and strengthening of the authentication processes**
   The use of strict safety standards, in compliance with the ECB provisions, becomes mandatory and it requires identity verification through two or more authentication tools, strengthened by the use of dynamic links which certify the uniqueness of the transaction.

Focus on secure standards for the dialogue between TPPs and Banks

The most significant impact on a technical level is the request by the Directive to facilitate the operations to access the accounts from external providers, in order to collect information or process a payment.

Contrasts among the potentials deriving from the development of a common language between Banks and third parties involved in payment operations are evident, and the risk of defining too rigid standards that create barriers for future innovation.

In order to allow for the dialogue between the parties with uniform and certified criteria, the task was assigned to EBA to address the requirements for a standard communication that allows innovation, through the publication of Regulatory Technical Standards.

In this regard, the final version of RTS in the field of "Strong Customer Authentication and Secure Communication" will be released by January 13th, 2017, while a Consultation Paper is expected in August 2016.

Whatever technology will be adopted to define the standard conversation between the parties, the choice that every Bank will take is about the project approach. It will be necessary to decide whether to wait for the regulatory and market changes (Reactive Approach) or anticipate them interpreting the Directive as an opportunity to develop the business (Proactive Approach).

Reactive

The project approach oriented towards obtaining mere regulatory compliance, could result in waiting for the final version of the Regulatory Technical Standards to be issued, and only then decide to implement the most effective and rapid adoption of the solutions identified by competitors and Fintech.

Banks that decide to adopt this approach risk that competitors get an advantage that will be difficult to bridge as well as a possible disintermediation towards their customers.

What happens if (or when) one of the bigger players active on social networks integrates payments as one of its services?

If every customer were to enter their IBAN code on its own social media account, the majority of customers using online payment services will be immediately active, potentially creating one of the largest networks amongst final consumers.

Proactive

The technological openness for the banking system addressed by the Directive will facilitate the creation of new services and products and maximizes the contribution that the Fintech community is demonstrating can be obtained.

The technological choices will increasingly have to be coordinated and directed by the strategic business goals.

Acting as a first mover requires projects to verify the architectural design of their software systems, making sure they are truly service-oriented and supported by an application system ready to sustain the growing business needs and to simplify internal processes.

The application architectures already in place to manage multi-channel applications over the Internet (eg. APP) will be assessed from perspective of the open-use that the new Directive requires.

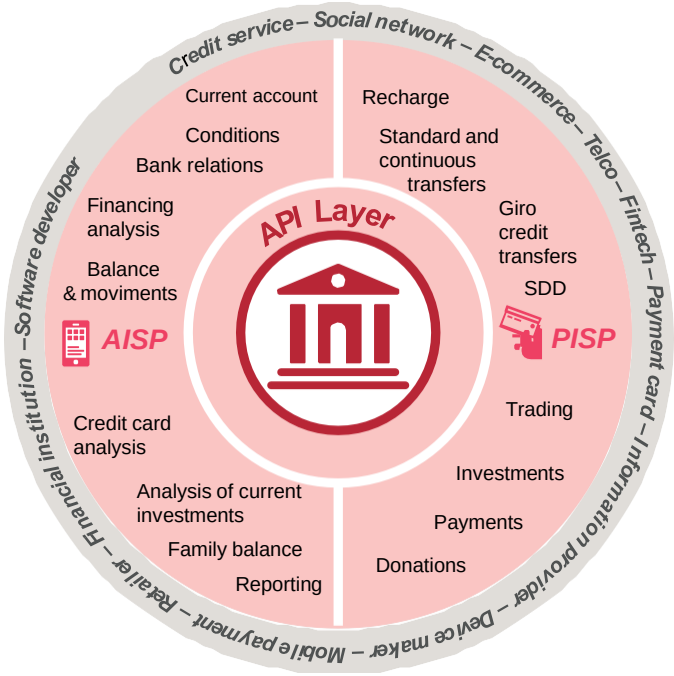
APIs, a way to implement

The legislation does not show the technology that the Banks must adopt to dialogue with third parties, delegating the task to EBA. The latter intends to orientate their indications in order to preserve innovation and cooperation, avoiding the introduction of unnecessary rigidity. On the other hand, the definition of a standard, addressed either by the regulator or the market, will have to be introduced, in order to not disperse unnecessary energy of the industry that attempt to reconcile the different interfaces implemented in autonomy by the different Institutes.

Even in the presence of these areas of uncertainty it is the common view, among financial institutions and Fintechs active in the sector, that the API may be a desirable technology to adopt.

APIs represent a specific architectural approach that ensures scalability, security and code reusability. This solution would allow Banks to reduce integration costs, increasing speed and making an innovation platform also available to developers and Fintechs.

Most of the initiatives related to the digital market are technologically based on APIs, used to open the systems to the parties included in the ecosystem by increasing the value of the service for the final customer. For example, the main players active in the field of social media and marketplace have adopted the APIs to make functionalities and modular design available to third parties, while creating value and a dependence on their systems.



Third parties access to current accounts is already a practice!

If the change required by the Directive, which requires opening to the market, seems excessive, consider that already today third-party applications that allow users to access their Bank accounts exist.

This takes place for example via screen scraping, a technique which allows to simulate the behavior of the client, linking to his banking homepage, in order to handle operations or request information.

This introduces several risks, not least the one related to the integrity of customer credentials, whose mitigation (through regulation and the implementation of secure methods to access their Bank accounts) is among the main objectives of the Directive.

Banks may not know if their customers are already authorising third-party access to their Bank accounts.

Focus on harmonisation and strengthening of the authentication process

The need in all Banks to harmonise the implementation of strict criteria for security (Strong Customer Authentication) represents the other main innovation of the Directive, confirmed and anticipated even by the 16th update of the Circular 285 of the Bank of Italy.

The user identity must be verified by two or more authentication tools classified as:

- knowledge (something that only the user knows, such as a PIN)
- possession (something that only the user has, such as Token)
- inherence (something that only the user is, such as a digital fingerprint)

The 16th update to Circular no. 285 of May 17th, 2016 "Supervisory Provisions for Banks" introduces the new Section VII "Organisational principles for Banks related to specific activities or risk profiles" that makes it mandatory for Banks to implement the requirements set out in the "Guidelines on the final of the Internet payment security" issued by EBA December 19th, 2014.

The Banks are required to document the adoption of strong authentication measures to strengthen the verification of the identity of the customers with regard to the security of transactions via remote channels. The alignment to the legislation should take place by September 30th, 2016 and by October 30th, 2016 Banks will be asked to share with the ECB or the Bank of Italy, a report on the work carried out on the organisational structures and information systems.

EBA, in order to limit the risk of compromising the authentication requirements, is detailing the issue of the interdependence of the individual elements to avoid that the violation of one credential affect the others.

The directive also anticipates that the payment operations with increased security thanks to mechanisms of "dynamic linking" that contain at the minimum an amount and a specific beneficiary. In fact, the goal is to ensure that authentication for a remote transaction is not used for any other purpose than the one originally foreseen by the payer.

There are also ongoing assessments about possible synergies between the authentication procedures we referred to above and the standards for digital identity adopted by the government and directed by international (e-IDAS) and national (SPID) standards which require compatible requirements.

The possible adhesion to SPID could benefit Banks, including potential opportunities of obtaining a wider customer base and increasing the offer of services to final users.

It is clear that there is a need to align the requests of making authentication and security policies strict and homogeneous to the need of the market of making online payments fluid and flawless, including also the relevant exemptions offered by the legislation.

Blockchain e Strong Customer Authentication

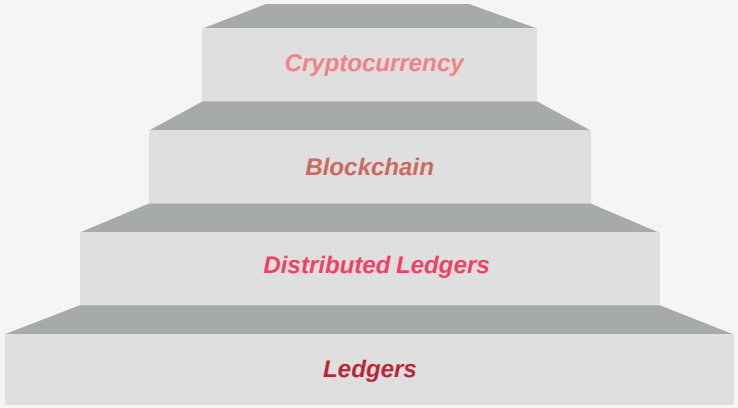
DLT, which stands for Distributed Transaction Ledger, is a technology that foresees the replication of a ledger which manages assets across multiple peer entities, enabling them to carry out transactions in trustless context without the need for intermediaries.

Blockchain is a variation of DLT that links together transactions in block and that give the ledger a characteristic of immutability, which guarantees greater transparency and safety.

Many Blockchain technologies manage the authorisation of transactions through an infrastructure in which every public key is associated an asset and the related private key allows you to validate the transaction. The process is very similar to that of the digital signature, without the obligation to use an accredited Certification Authority and allows the use of a self-generated KeyPair, solely stored on a Mobile Device.

In this way, it offers the possibility of considering the device as an ownership element to which only the user has access, just like the OTP devices currently in use.

For example, it is possible to implement the possession factor “something that only the user has” of the Strong Customer Authentication, using the Blockchain technology to bind a particular user to a specific mobile device.



www.pwc.at/psd2

Christoph Obermair

Partner
+43 699 10871262
+43 1 501 88-3629
christoph.obermair@at.pwc.com

Stefan Moser

Senior Manager
+43 699 16305012
+43 1 501 88-1156
stefan.moser@at.pwc.com