The communication between Third Party Providers and Banks
What will the impact of technology be?

PSD2 in a nutshell

2

www.pwc.com/cz/psd2

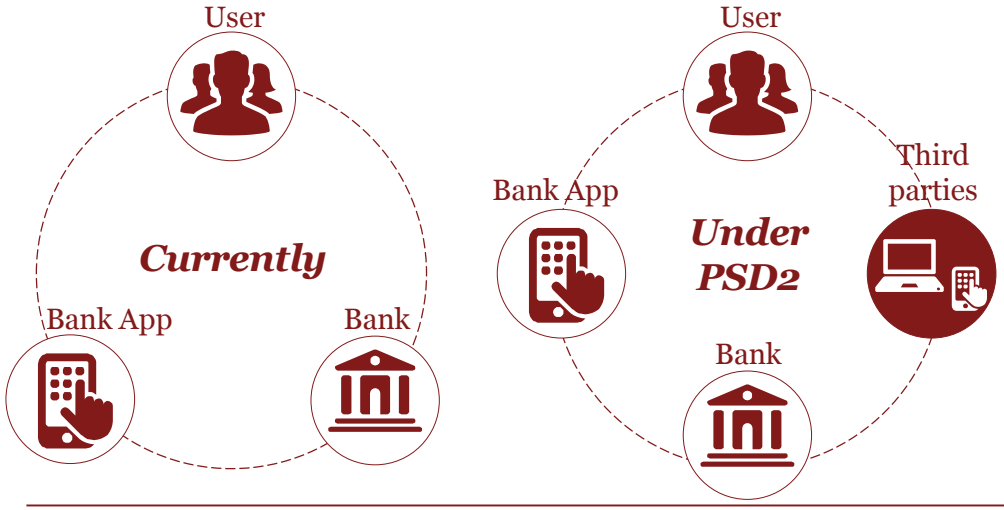
pwc

Summary

The banking system is at a turning point. It is under pressure from the market and emerging operators who have introduced a strong technological push; in this environment, banks will have to decide whether to compete in order to maintain a direct relationship with their customers or to limit their role to that of just a 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 in the Bank accounts of the final users, clearly introducing the risk of disintermediation between Banks and their clients.



This openness towards the market allows for 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 third party providers.

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

1. **Secure standards for the dialogue between Third Party Providers and Banks**
   Service payment providers authorised by final customers must enable 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 operations that access accounts from external providers, in order to collect information or process a payment.

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

EBA was assigned the task of creating standard communication that allows innovation which will be published in Regulatory Technical Standards (RTS). This will allow for dialog between parties with the uniform and certified criteria.

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

Whatever technology is adopted to define the standard conversation between the parties, the choice that every Bankwill 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 competitors getting 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 their own social media account, that would create a huge payment institution that would have a dominant position in the market.

Proactive

The technological openness for the banking system addressed by the Directive will facilitate the creation of new services and products and maximise 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 that projects 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.

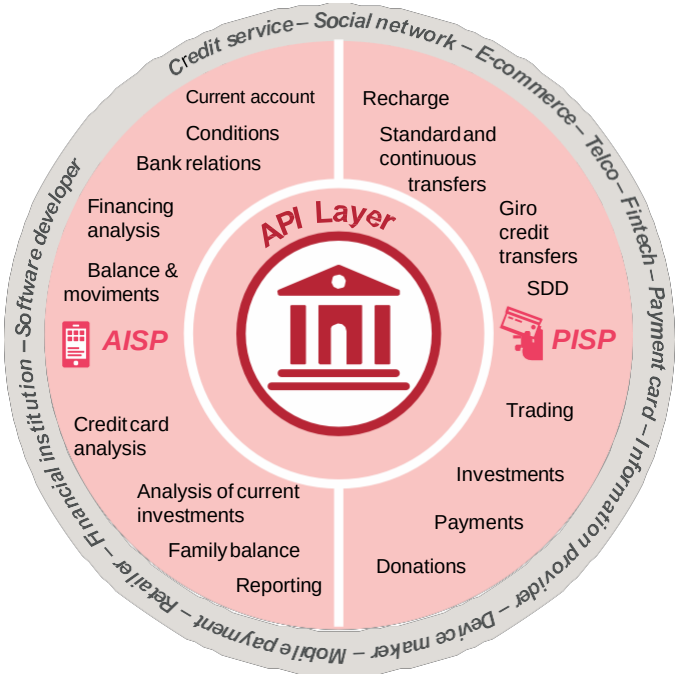
The application architectures already in place to manage multi-channel applications over the Internet will be assessed from perspective of the open-use that the new Directive requires.

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 attempts to reconcile the different interfaces implemented autonomously 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 systems to 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 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!

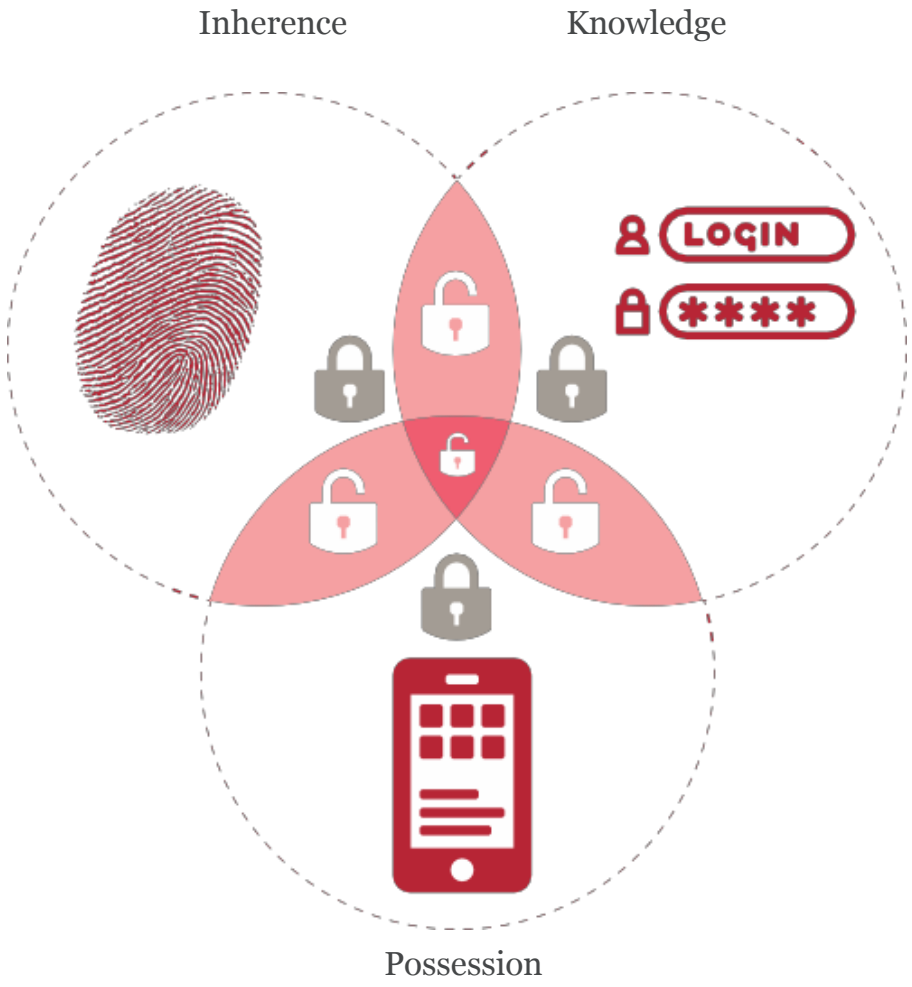
If the change required by the Directive, which requires opening to the market, seems excessive, consider that today third-party applications that allow users to access their Bank accounts already exist.

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

This introduces several risks, not least of which is 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 harmonising and strengthening 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 PSD2.

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)

EBA, in order to limit the risk of compromising the authentication requirements, is focusing on the issue of the interdependence of the individual elements to ensure that the violation of one authentication does not affect the others.

The directive also anticipates that the payment operations with increased security thanks to “dynamic linking” mechanisms will contain at least 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.

Focus on harmonisation and strengthening of the authentication process

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 call for compatible requirements.

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

Blockchain & 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 a trustless context without the need for intermediaries.

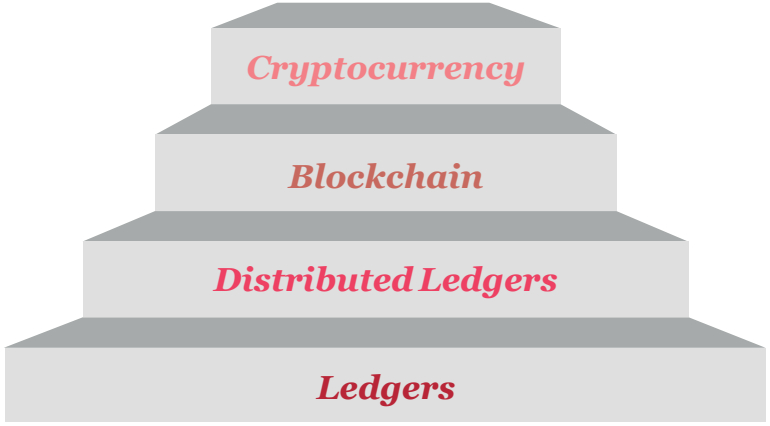
Blockchain is a variation of DLT that links together transactions in blocks and that give the ledger a characteristic of immutability, which guarantees greater transparency and safety.

Many Blockchain technologies manage the authorisation of transactions through an infrastructure in which every public key is associated to adevice 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 to be 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 Strong Customer Authentication, using the Blockchain technology to bind a particular user to a specific mobile device.

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



Contacts

www.pwc.com/cz/psd2

Mike Jennings

Partner | Financial services
+420 603 280 371
mike.jennings@cz.pwc.com

Martin Vurm

Senior Manager | Financial services
+420 775 011 014
martin.vurm@cz.pwc.com

Vincent Santamaria

Manager | Regulatorics
+420 733 612 785
vincent.santamaria@cz.pwc.com

Radoslav Ratkovský

Senior Manager | Financial services
+421 903 450 128
radoslav.ratkovsky@sk.pwc.com

Looking forward to our future collaboration