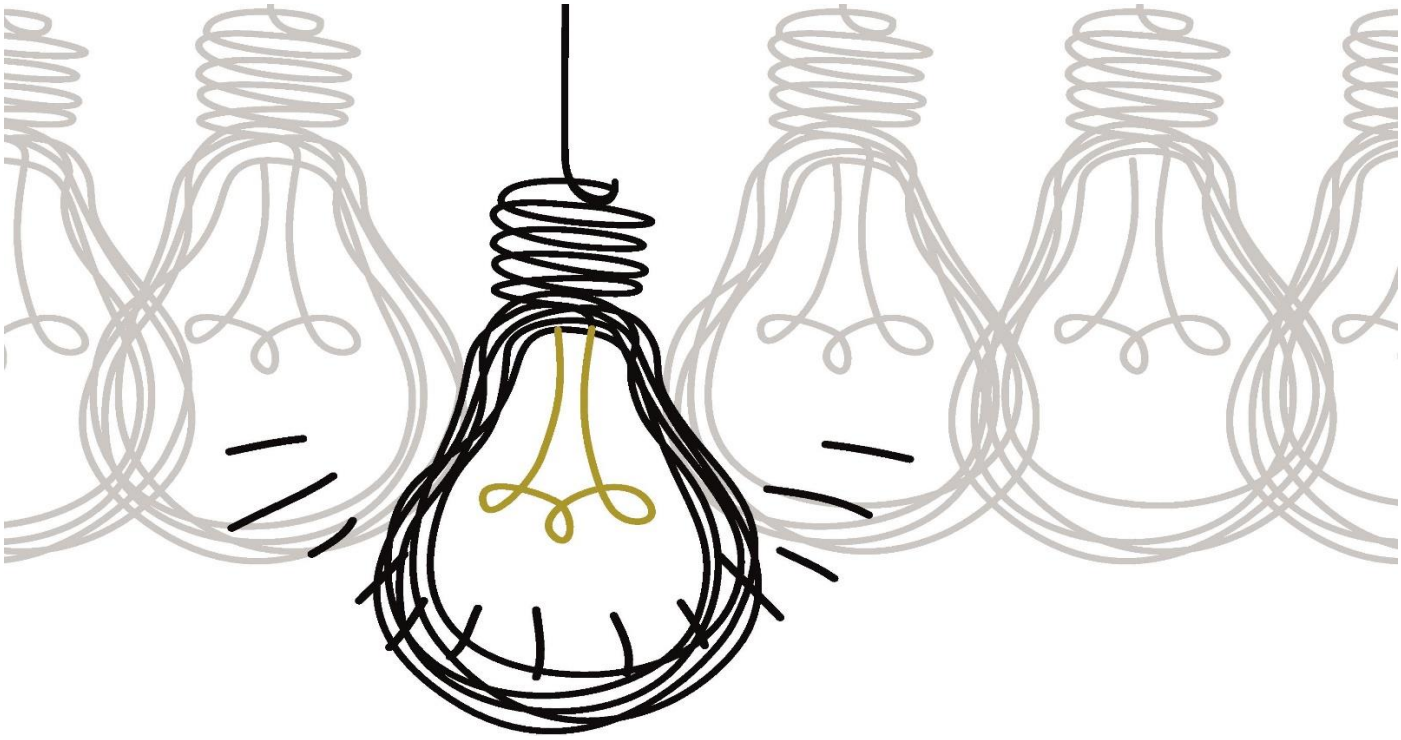


PSD2 and Open Banking

Summary of the most important lessons learned from the PSD2 workshop of June 22, 2018

On June 22, 2018, ICT Solutions Ltd. and Online Business Technologies held a joint international PSD2 workshop in Visegrád. This document summarizes the most interesting information and findings that have been made at the workshop.

Online
BUSINESS TECHNOLOGIES

Introduction

The **PSD2** and the so-called **open banking** is one of the most frequently discussed topics in the banking conferences today.

This is no coincidence: the evolution of information technology has enabled new business models to evolve in a number of industries, changed consumer habits, and these changes penetrated the financial services market through FinTech and BigTech companies. PSD2 facilitates this process from the regulatory side, since it allows FinTech companies to access banking databases to help promote the spread of financial innovation. Open banking is a collaborative model in line with the above changes, whereby banks try to provide higher quality and more versatile services to their customers by involving FinTech companies.

The aim of the PSD2 **workshop** of 22 June 2018 was to share deeper professional information related to PSD2 and Open Banking and to provide an opportunity to discuss these information.

The event gave a **360-degree picture** of PSD2 and Open Banking, addressing both **PSD2's regulatory issues**, **business opportunities**, as well as **IT implementation**. **Gijs Boudewijn**, Chairman of the Legal Support Section of the European Payments Council, presented the latest regulatory news, **Peter Gába**, the leader of the Erste Group's Open Banking Initiative, gave a review of the use of open banking for business purposes, while from our company **József Németh** presented the IT challenges of compliance with PSD2. The lectures were followed by a panel discussion in which **John Basquill**, a journalist at Payments Compliance moderated the professional dialogue between the audience and the performers.

Prior to the event, we have compiled a detailed list of the PSD2 issues most important for the banking sector. The **Gárdos Mosonyi Tomori Law Office** was also involved in the preliminary processing of these topics.

In this document, we review what information and findings we have found to be most interesting at the event. We hope the summary will be useful and will meet you at our next events!

Budapest, 2018.06.28.

The Team of Online Business Technologies

Information, findings

API standards

The **incorporation of the PSD2 Directive** in the EU member states **is delayed**, so at the time of the workshop, the PSD2 regulations have not yet been included in all Member State's national legislation. This delay will cause problems with the so-called passporting, when a payment service provider, disposing of a service license valid in a given country, attempts to host that license in another member state (see Article 14 of the PSD2 Directive).

PDS2 API standards

The EU reviews large PSD2 APIs for compliance with the RTS SCA, but despite standardization, we expect different APIs per bank.

Accordingly, technical service providers safeguarding an interconnection between PSD2 APIs, will have a prominent role.

In early 2018, the European Commission and the European Central Bank initiated the **establishment of an API Evaluation Group**, aimed at providing – through the analysis of the five biggest API standards (Open Banking UK, Berlin Group - NextGenPSD2, STET, the Slovak National API, the Polish National API) - a general guidance concerning the compliance to the regulations of the Regulatory Technical Standard of Strong Customer Authentication and secure communication (RTS SCA) no. 2018/389, issued to PSD2. Memos of the group meetings are available on the European Payments Council website (www.europeanpaymentscouncil.eu).

If we look at the European panorama, the **NextGenPSD2** of the Berlin Group**, is growing in importance**: Germany, Italy and the Netherlands have moved towards this standard, and the French STET standard has also been harmonized with NextGenPSD2.

Concerning the listed PSD2 API standards, it is worth mentioning that these are so called **API Initiatives**, which means that the standards **do not describe a specific technical implementation**, but define technical components that can be used to create a PSD2 API. The logical consequence of this is that even two NextGenPSD2 interfaces will not be technically identical, so **all PSD2 APIs** - even those of the same standard - **will be somewhat different**!

Technical communications providers

As a consequence of the foregoing paragraphs, the importance of companies that **provide a gateway between different PSD2 APIs** is growing. The core of these companies' services is that they provide a single connecting interface to Third Party Providers (TPPs) sending PSD2 transactions/information requests, because all further interfacing to the banks' PSD2 APIs will be managed by these service providers, constructing a star communications connection between TPPs and the banks. The question arises whether these **technical service providers should qualify themselves as** payment service providers (**TPPs**)? According to our preliminary

analysis, **this is not necessary**. The technical service provider and the TPP initiating the messages must enter into a contract which, according to which the technical service provider is providing, on behalf of the sending TPP, so called outsourced activities for the TPP. Accordingly, for third parties, the sending TPP is responsible for the activities of the technical service provider, and their responsibilities must be settled in a contract concluded between them.

Strong customer authentication

Strong customer authentication

Conforming the EBA's June 13, 2018 opinion, a strong customer authentication based solely on redirect is legitimate and it is not mandatory to use other authentication methods based on the transfer of customer authentication data to TPPs.

Strong customer authentication is one of the cornerstones of PSD2 services. The publication of the final version of RTS SCA on 27 November 2017 raised the question of **whether** Article 32 (3) of RTS SCA **prohibited** the use of authentication methods **based on redirection** not requiring the release of personal credentials (such as OAuth and OpenID Connect standards)? A further question was **whether or not it would be mandatory** to use the so called embedded authentication, based on the transfer of customers' personal credentials? The opinion of the European Banking Authority (EBA) of 13 June 2018 clarified the situation: **the redirection itself does not constitute an obstacle**, if it is not created in a preventive manner, and it is **not mandatory to use other authentication procedures**, other than the redirect authentication.

Many people think that applying PSD2's **strong client authentication** rules is **only** mandatory when **accessing TPPs via the API**. That's a **mistake**. As Article 97 of the PSD2 provides for strong client authentication when accessing customer accounts online, therefore, strong customer authentication rules are **mandatory** for the **NetBank and MobilBank solutions** directly used by the customer, **too**.

Exceptions to strong customer authentication

The RTS SCA provides banks with the opportunity to improve the customer experience by making **omission of strong customer authentication**, in case of some so called **low-risk** operations. The scope of these operations is listed in chapter III of the RTS SCA.

The use of exceptions is optional for banks and the use of exceptions results in a major change in liability relationships, in the case of payment transactions, since if the payer's payment service provider **does not apply strong customer authentication**, Article 74 (2) of the PSD2 Directive states that the **payer is not liable for any loss** unless he has acted fraudulently.

The above procedure and consequences are commonly known by banks and we often encounter the view that the use of **strong customer authentication will be decided individually**

by the bank **in its own jurisdiction**, without prior notification to customers. Although this is basically true, we believe that exceptions should be reported to customers. This is due to the fact that the use of strong customer authentication entails a change of responsibilities, of which customers are to be informed in advance, so we believe that the **principles of exception management should be published in advance in bank announcements**.

With regard to the exceptions, it is worth mentioning that the exceptions include an area often overlooked. Article 17 of the RTS SCA allows the use of exceptions for **secure business processes** when the competent authorities are satisfied that the procedures used allow the same level of security as the level of security defined in the PSD2 Directive. At this time, there is no EU resolution on how and on what conditions this exemption can be obtained, so it is advisable to contact the competent local authorities concerning this issue!

What is to be considered an account with online access?

PSD2 requires **access to online accounts** via the PSD2 API (see Articles 65, 66 and 67 of the PSD2 Directive). Everyone agrees that **accounts available** through **customers via the netbank, mobile banking** channel should be included in this circle. But what about the so-called **home banking systems** used in companies, or ad absurdum the ATMs software through which the client can remotely access his accounts? **There is no uniform approach** to this, but for example. the **British legislator** applied **the following approach** to implementing PSD2: "Any invoice available to the customer through the Internet is to be considered as available online, regardless of the technical solution utilized."

Transactions available through API

In its opinion published on June 13, 2018, the EBA clarified that any payment transaction initiated by a customer (such as group transfer, value date transactions) should be accessible via APIs, not only the e-commerce related one-time payments.

The range of payment transactions available through APIs

For PSD2 projects, there is a serious question of **what payment transactions** should be made **via the PSD2 APIs**. In this regard, it was **previously** the position of European banks that paragraphs 27 and 95 of the preamble to PSD2 clearly refer to e-commerce support, so it is sufficient **for one-time payment transactions related to e-commerce** to be accessed through the PSD2 APIs. The EBA's aforementioned opinion disagreed on this because it clarified that based on the definitions of the PSD2 directive, **all payment transactions** (e.g. group transfers, regular transfers, value-dated transfers) should be made available through the PSD2 APIs.

Fallback solutions

Fallback solutions

The use of screen scraping plus is a risky procedure for

banks, even as a fallback measure. The solution is to create good APIs conforming the big standards, and to obtain exemptions from local authorities from the utilization of screen scraping plus as a backup solution.

Article 31 of the RTS SCA offers **two options** for solving TPP access. One of the options is the creation of a target specific **dedicated interface**, which is a technical channel separated from other system-access points crated for the PDS2 services. The other option is that the bank offers the same access channel for TPPs to access PSD2 services, which it uses as the **channel for authenticating and communicating with the bank's customers** (e.g. NetBank, MobilBank). If **the dedicated interfaces do not work**, then the netbank channel should be made available for the TPPs as a **fallback** solution – in case of absence of exemptions from local authorities.

If the TPPs use this latter channel to access the PSD2 services, the so-called screen scraping technology, more specifically its TPP authentication version, the **screen scraping plus** is used for netbanking screen functions and for data extraction.

The **vast majority of banks** are thinking of developing the technically more safer **dedicated interfaces**, and generally believe that the they have **nothing to do with the fallback procedure** referred to in the previous paragraph, since in these cases the TPPs automatically „scrape" the netbank, and – as per point 5 of paragraph 33 of the RTS SCA - **all responsibility is borne by the TPP**. Unfortunately, **both points are wrong**.

When using screen scraping plus, TPPs need to be authenticated, so **banks need to modify their netbank** when opening this channel as a fallback procedure. And although Article 33 of RTS SCA actually imposes obligations on TPPs, but the core responsibility toward customers remains unchanged, so it is in the **bank's** primary **interest** that **TPP access is strictly controlled in these cases, too.**

The solution is simple. **Good PSD2 APIs should be made** and local authorities should be convinced to **grant exemption** to the bank from utilizing screen scraping plus (see Point 6, Article 33 of the RTS SCA). If a bank **uses one of the above-mentioned big standards**, this exemption is expected to be easily obtainable.

Business Opportunity - Banks in TPP Role

Banks as TPPs

One of the business opportunities for PSD2 is when banks themselves launch TPP services.

Banks do not need to obtain any additional license for this.

Banks are serious about the business utilization of PSD2 APIs. One logical way is that **banks themselves provide TPP services**. These may be "classic" FinTech services (e.g. personal budgeting), but they can also use information recovery through the PSD2 API in **traditional banking processes**, like for example customer's account statements are queried - with the client's consent - through an API during credit sales. Regardless of the nature of the TPP service the banks are willing to launch, they may provide online credit transfer or bill information services **at their own discretion**, so they **do not need any extra license**.

Business Opportunity - can data collected for other purposes be used for PSD2 services?

A common business question about the data gathered with the PSD2 is whether **the information thus obtained can be used by the bank for other purposes**? Do you need the customer's consent for such use? If so, how much concrete support will be required from customers? Anyhow, is it possible any data transfer/data utilization without the customer's consent after the entry into force of the GDPR?

The PSD2 Directive and the RTS SCA are clear on this issue: **in the absence of a customer's consent**, data **should not be used to provide other services**. If the **client agrees** to use his data, **it is already possible** to use the data, but according to the GDPR, the request **for consent** must be sufficiently **specific**, ie the bank should specify the service to be provided to the client and how data will be used. Consequently, a general consent request is not possible, like for example, We would like to use your personal information to develop new products. It should be noted, however, that data sets can be utilized for research-development purposes, following the **anonymization** of the datasets (the blanketing of personal data).

With the help of a customer-authorization, it is also possible for **several banks to build a common database**, but when this activity is continued, attention should be paid to the requirement of **Article 26 of the GDPR** and the participating banks must conclude a data management contract in which they detail their duties and responsibilities.

In connection with this, it is worth pointing out that the entry into force of the **GDPR does not mean** that, from now on, the **client's consent** is required for **all data transmission**, data processing. This is not the case. If, for example**, the disclosure of data is made mandatory by law**, then the communication may also be made **without the consent of the customer**.

Business Opportunity - Open Banking

Open Banking means that a particular bank, in addition to the requirements of PSD2, also offers a wide range of services through APIs, or the bank itself also accesses a wide range of services from other providers through APIs.

Open Banking enables the creation of **service ecosystems**. In these service ecosystems, individual providers (e.g. insurers, traders) **are connected** on the level of IT systems, **through the APIs**, and are able to reach each other's services (e.g. initiating the sale of a given product). Through API connectivity, it is possible **to cover entire service value chains**, as in today's large companies, the combination of individual systems can cover entire corporate processes. However, these **ecosystems** are **not rigid structures**, since a given provider can **use** the **API** of an other provider in a way that **has not been seen before**, to provide a previously unseen service.

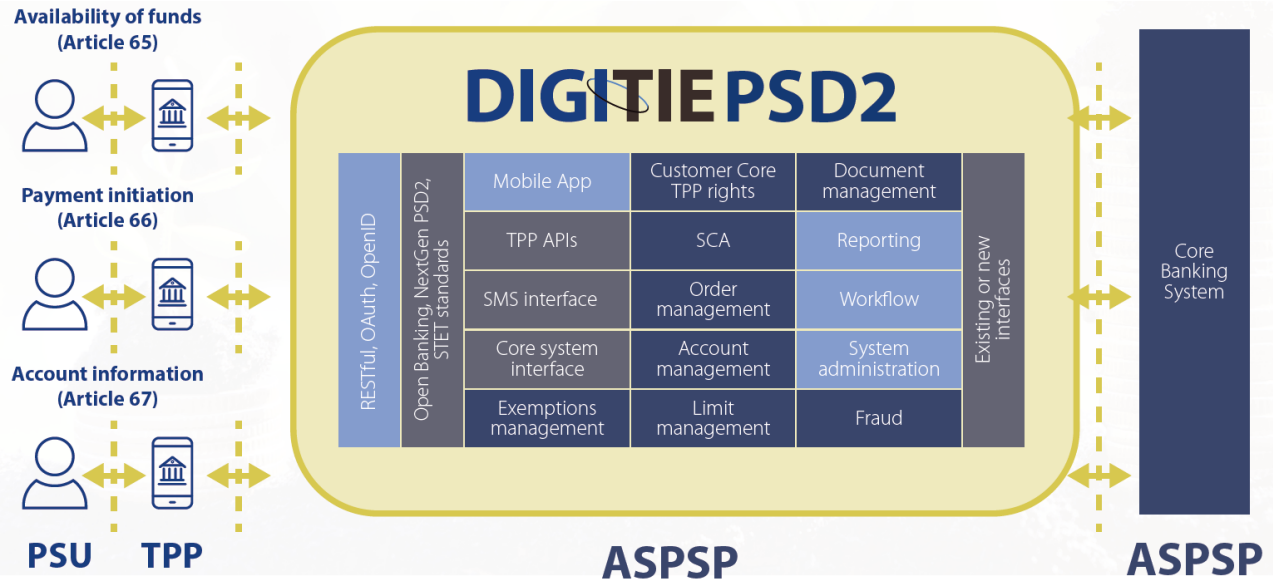
Open Banking

Open banking enables the creation of service ecosystems. The members of the ecosystem are connected on the IT system level, through APIs, so they can cover entire service value chains and are able to sell each other's services.

The **business rationality** of the ecosystem is that the services of an organization that opens up **APIs** can be **accessed by a wide range of companies**, and the related companies **can use** the services they have achieved **to provide other services**, so the bank **can "sell" its services much more widely** than it would be **possible based solely on its own resources**.

Our solution for PSD2 and Open Banking - DigiTie

We have an IT solution, which helps to meet the challenges of PSD2 and Open Banking, that is ***DigiTie***. ***DigiTie PSD2*** enables banks to be compliant with PSD2.



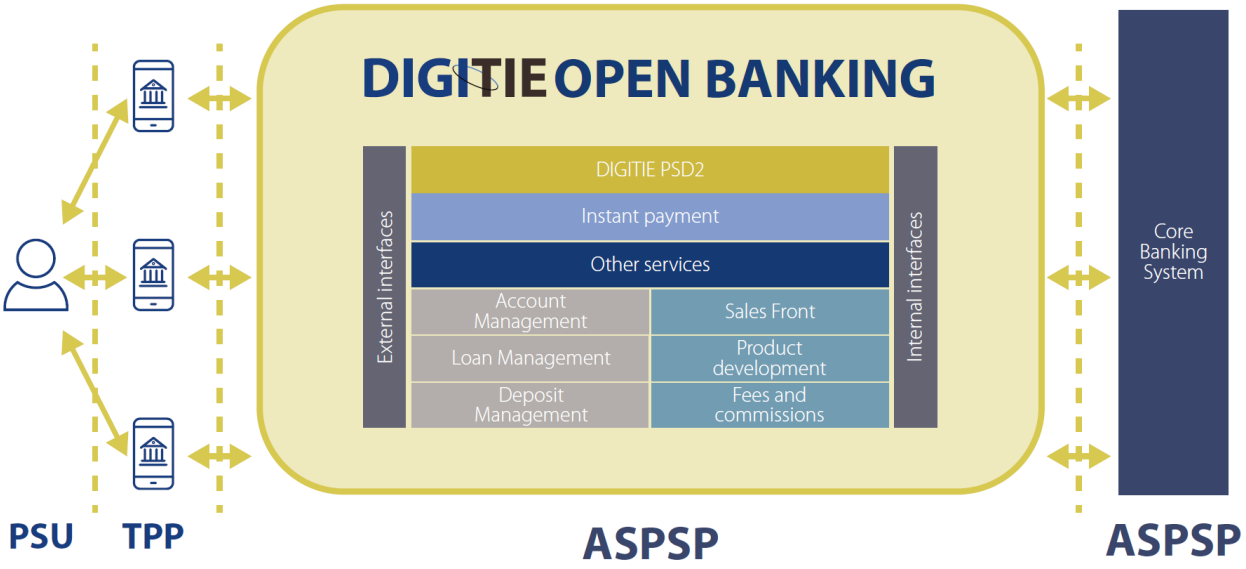
DigiTie for PSD2 serves as a front-layer for banks to manage the requests of TPPs (Third Party Providers) from PSUs (Payment Service Users) 24/7/365 and to transfer the requests to core banking systems of ASPSPs (Account Servicing Payment Service Providers). It is developed to be compliant with any PSD2 standard (OpenBankingUK, NextGenPSD2, STET). The solution uses state-of-the-art technologies like RESTful interfaces, TLS 1.2 for secure connections, OAuth 2.0 and OpenID Connect 1.0 for authentication and authorization, X.509 for certificates. The PSD2 solution provides different options for SCA, such as the classical combination of static passwords and dynamic passwords sent in SMS, or highly advanced methods like the combination of using fingerprints and mobile app-based certification. The mobile app for SCA is available on iOS and Android platforms. It is also possible to rely on the existing SCA methods of banks.

Upon request we can connect DigiTie for PSD2 to core banking systems using either existing bank e-channel (e.g. Internet Banking) interfaces or a new, customized interface. In the case of existing interfaces only minor development is required from the bank.

The solution is able to handle exemptions from SCA, like low-value transactions, contactless payments etc. In order to ensure secure operation, it also includes limit handling, and as part of the Fraud component offline confirmation etc.

DigiTie for PSD2 helps you to be compliant with PSD2 regulations and gives you the opportunity to extend the solution with further services later (see on the next page).

While DigiTie for PSD2 opens services necessary to be compliant with PSD2, ***DigiTie for Open Banking*** can open up additional services to join FinTech ecosystems. The options are endless in this area, which might include 24/7 loan disbursement based on applications submitted by FinTechs, or creating deposit accounts based on the request of PFM (Personal Finance Management) solutions. DigiTie for Open Banking includes all the functions of DigiTie for PSD2 and provides additional features to help the cooperation with FinTechs (see the picture below).



These features include custom tailored Open APIs for FinTechs under RESTFUL or other technologies (e.g. SOA web service). While DigiTie for PSD2 opens only a few payment services free of charge, DigiTie for Open Banking makes other banking services (e.g. loans, deposits) available under agreed business terms.

In order to support these services 24/7, DigiTie for Open Banking provides core banking functionality for time periods when main systems are down, serving as a shadow core system. These new services will be available for agreed fees that can be managed by the Fees and commissions module. New channels might require the selling of new products. This is the point where the Sales front and the Product Development modules can help.

Online Business Technologies

H-1032 Budapest, Vályog street 3. | +36-1-437-0700 | https://www.online.hu/contact