**Aivars Belis**
*Board member |Principal consultant*
*SIA Vedicard* | 8 December, 2017

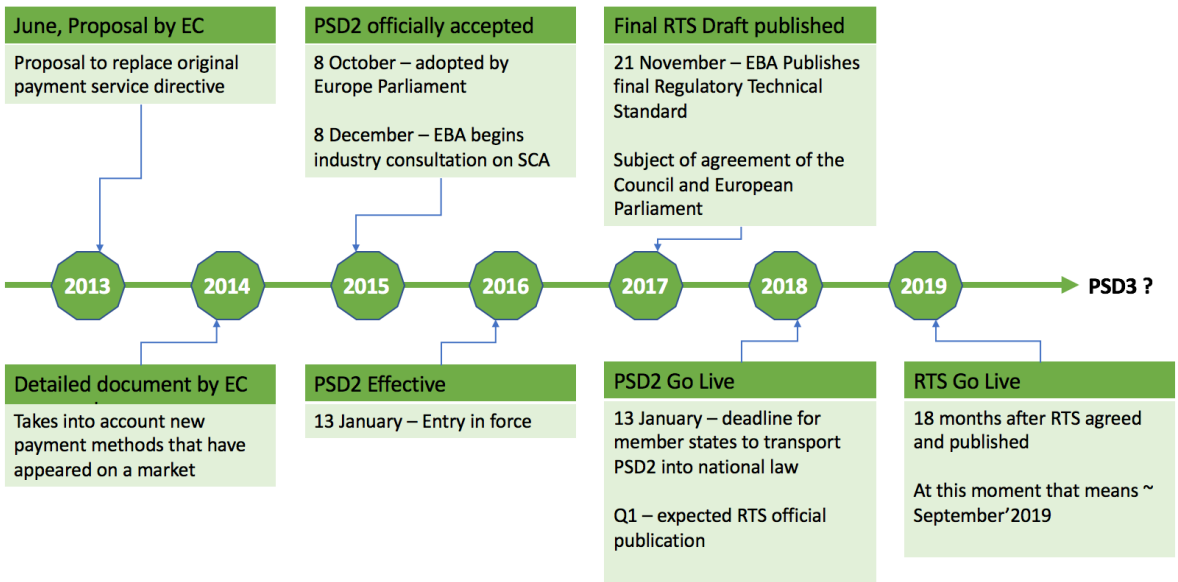
# 117 shades of black within PSD2

Thoughts on PSD2 implementation from strategic and technical perspective.

## Preface

Last 2+ years has brought a lot of changes within payment industry. It all started on October 8, 2015 when European Parliament adopted the revised Directive on Payment Services (aka PSD2) to make it easier, faster and more secure for consumers to pay for goods and services by promoting innovation (especially by third parties), enhancing payment security and standardizing payment systems across Europe.

In January 2016, the PSD2 directive came into force – and the fuse that leads to explosive market changes started to burn. With less than 3 months left, existing industry players are under heavy pressure to fulfil PSD2 requirements. 13.01.2018 is the deadline for Member States to transport PSD2 into national law and is considered the go-live date for PSD2 transparency and one leg transactions. Just recently on 27.11.2017 the European Banking Authority published final Regulatory Technical Standards (RTS) draft that defines regulatory requirement for Open API, Access to Accounts (XS2A), Strong Customer Authentication (SCA) as well as Customer protection liability and complaints. These will become applicable 18 months after date of entry into force of the RTS which is subject to the agreement of the Council and the European Parliament. At this moment that we can guess that it will be around September 2019.

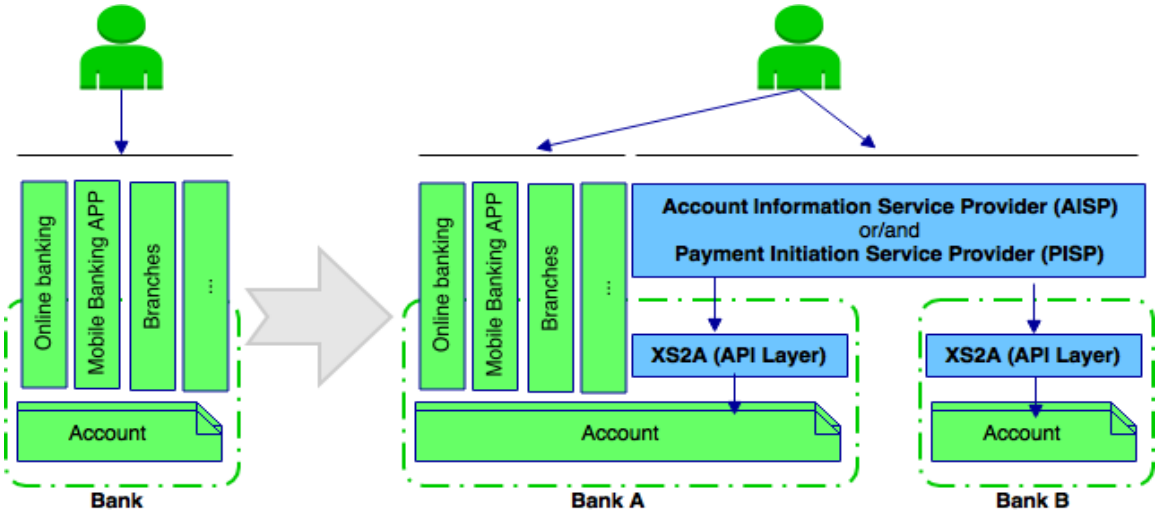


**Aivars Belis**
*Board member |Principal consultant*
*SIA Vedicard* | 8 December, 2017

## Key aspects of PSD2

- Third Party Provider(TPP) definition to enhance new services regulation, more precisely definition of Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).
- European banks (well, actually any payment Service Provider serving cardholder account with online access options) to open their IT payment infrastructure to those new TPPs.
- Widened scope of regulated transactions with inclusion of "one-leg-out" (OLO) payments, in any currency thus that applies to payments initiated and ending in all the 28 EEA countries + Iceland, Liechtenstein, Norway.
- Stricter customer authentication obligation for Payment Service Providers(PSP) every time payer accesses his account online or initiates remote payment transaction.

Besides that, PSD2 has interdependencies with other regulations like General Data Protection Regulation (should be applied from 25 May 2018) and eIDAS regulation (deadline - September 2018) thus involving multiple stakeholders and increasing complexity for implementation.




## Industry response to PSD2

Even PSD2 Regulatory Technical Standards (RTS) do not explicitly state usage of APIs, majority of industry professionals assume that APIs will be the technological road to be compliant with the regulation. Some markets are quite ahead of EU in this field – for example UK Competition and Markets Authority report in 2016 explicitly recommended usage of REST APIs to ensure open banking.

At this moment, it is perceived that existing players like banks face the risk to lose relationship with customers. However, till this day banks have safeguarded customer accounts and in majority cases have earned customer trust. According to Accenture's PSD2 UK Banking Customer Survey, 76% of respondents preffered banks to be their PISP provider and 65% to be their AISP provider. And 70% would not trust a third party as much as they are currently trusting their bank.

PSD2 RTS does not define exact specifications for mandatory APIs to be exposed thus raising several concerns that industry may end up with situation that each third bank will expose mandatory APIs based on their own specification. If so, new TPP would be required to develop various integrations and quite obviously that top size banks would be choice 1 to do this integration. Majority of industry players agree on this and have been involved in one or more than one payment interoperability standards harmonization initiative that are now actively working on topic and developing standard technical specification proposal. Most know groups/companies working in this area are 'Berlin Group', 'CAPS', 'STET' and 'Open Banking' in UK. Speaking about 'STET' – company already has created STET PSD2 API specification collaborating with BNP Paribas, BPCE, Le Groupe Credit Agricole, Credit Mutuel – CIC, La banque Postale and Societe Generale. STET also is represented in 'Berlin Group' but nobody has promised that 'Berlin Group' specifications will be equal to STET specifications. As already mentioned above, UK market has gone quite far and established 'Open Banking' implementation entity that as a first step developed The Open Data Specification allowing providers to supply up to date, standardised information about latest available products and services, so that, for example, a comparison website could gather information and possible choices options for end customers. As the second step Read/Write Data API specification was developed specifying APIs to access account information, balances and transaction history as well as initiation of payments from personal and business current accounts.

## Strategic positioning

According to several studies more than half of the banks are saying that as an outcome from PSD2 they want (or have been pushed) to change their strategic positioning. Some of those options mean stepping into the world of FinTech's. If we compare key strengths of those 2 worlds than for banking majority of respondents would state Security, Existing customer base, long term professional experience and established trust, data availability and knowledge about customer. Although regarding last two we could have a lot of debates regarding effectiveness of available data usage to obtain maximum possible knowledge about customer. If we look to the FinTech's key strengths then usually respondents would mention new technologies, orientation to improved customer experience, agility to adopt/change.

Let us take a look at possible strategic options for banks:

Be compliant

Ensure basic required access to accounts and payment initiation to 3rd parties.

Monetise Access

Besides compliance develop more advanced API platform; implementing granular access and monetise access to raw data and banking services.

Become AISP and/or PISP

Provide new value added services to the customers leveraging own insights and 3rd party products and services by establishing AISP and / or PISP.

Establish banking platform

Build banking-as-a-service platform. Play aggregator role to establish ecosystem between various players remaining in central position towards customer.

According to several surveys available just limited number of banks are going to choose 1st option e.g., "Be compliant". At least half of the banks initially have stated that they are going to position themselves as platform, ensuring open-platform for partners to deliver their products/services along with bank's offering. Those banks that will achieve that will gain powerful position. However - if we look at potential partner motives and potential required integration development to various banks (since formally there is no common API standard in Europe and several initiatives are ongoing) then we are coming to the fact that only large banks could be interesting for new partners. Which means that smaller ones potentially will be accessed via consolidators/aggregators available on a market thus strategic option of banking platform establishment for smaller players could be questioned.

It seems that at this moment a lot of existing banks has postponed making "final" strategic decision. Analysis are still undergoing regarding their strategic choice; dedicated teams are already working or will start to work on compliance. For some of the banks strategic target has been defined as compliance project by IT and Operations. Is it successful strategy? – time will show … Strong product offering e.g., producer role without stepping into distributors role also is an option to move, but products will have to be competitive to be the first choice for end customers and distributors as well.

Even if time is quite limited, a lot of banks were waiting for final RTS and are still evaluating the impact of PSD2 while some has finalized gap analysis and are ready to move on with design phase to fill gaps and develop business case(-s).

## Technical implementation requirements

Technical implementation of solution to cover PSD2 requirements must note several import requirements areas that should be fulfilled e.g., Security, Open APIs, Scalability and Real-time 24x7 operations. Historically APIs already have been used, but usually those were considered as "trusted" B2B communication setups with limited number of security controls and limited number of actions. Existing EU banks that still have legacy-based IT architecture will find PSD2 requirements implementation very costly and complex to ensure scalability to meet potential load volume and still to respond to incoming requests in acceptable timeframes; even worse – in some cases multiple systems with multiple interfaces in back-end and batch processing will make it even harder to achieve. On other hand – that will give them an opportunity finally to evolve and do things right.

Security must be an integral part of API implementation – ensuring Strong Customer Authentication as well as TPP verification. Besides that – EU's new General Data Protection Regulation (GDPR) will be mandated from May'2018. That extends security requirements with customer consent management regarding their data and what data is allowed to be passed to other TPP. Failing to meet GDPR requirements could end up with high fines for non-compliance.

Risk monitoring/prevention solutions also must be an integral part for those new solutions deployments taking into account that data load for processing will increase, APIs will be executed by 3rd parties developed applications thus not all usual data could be available for analysis as well as TPP requests verification have to be done to combat with potential Malware or Social Engineering techniques. Exposed APIs will become potential target for distributed denial of service (DDos) attacks – thus platform must ensure capabilities to fight with them. Summing up – there will be a need for Holistic Risk monitoring / prevention platforms that are well integrated into PSD2 APIs technical layer ensuring new channel and operation/activity monitoring.

## Solution choices/ options

Depending on existing bank's IT architecture there are several options how to proceed with technical solution implementation and which approach and technologies to use. For those entities having just one backend solution (for example Core Banking solution) serving accounts that needs to be exposed there is an option to extend existing solution capabilities to ensure required APIs + all required security and risk monitoring capabilities. In case of ensuring just minimum compliance that could be an option to use. But looking from risk and complexity perspective this approach will come along with big impact on existing solution,

thorough testing requirements, significant associated costs and limited possibility to extend services by re-using or implementing some additional solution/partner in a future. So, except cases when definite decision to maintain just compliance is made, I would not go with this option.

Contrary to previous approach – I believe that the best option would be to deploy APIs on separate Enterprise Service Bus (ESB) for APIs or nowadays often called API Management Platform that could be deployed considering required scalability as well that would allow much more easily to connect multiple different back-end solutions. Nowadays there are multiple solutions positioned as API Management solutions that allows publishing APIs and govern API usage rights. Various technology company's solutions could fit the purpose e.g., Red Hat JBoss Fuse, WSO2 API Management, MuleSoft Anypoint platform, Apache ServiceMix, Red Hat 3scale API Management, Oracle Service Bus, IBM Websphere, Microsoft BizTalk Server and much more. Some of those are open source projects with available payable support, some are big enterprise solutions. Thus also costs for those solutions can vary from 80'000 EUR annual support for open source solution ending up with much more higher amounts. In general, all those solutions are ESB solutions – some are modern, some not so much and some are recently packaged particularly for API management. Comparison of those solutions can take some time and I will leave it outside of this document.

Looking for the right solution the following key factors have to be considered: high availability, scalability and performance, integration capabilities that supports integrations to bank's existing solutions, security and access policy enforcement capabilities, APIs usage monitoring capabilities for statistical purpose as well as to meet SLA requirements. Besides that, chosen technology must be validated from perspective of lifetime/roadmap as well as required knowledge within your organization.

## End customer perspective

We are approaching times when customers will have access to account data via set of applications built by Bank(-s) , TPPs from all EU region, where customers will be able to see consolidated account data, initiate payments, compare offers from different TPPs and buy/subscribe to various products/services from those multiple TPPs benefitting lower prices due to much higher competition. And of course - customers will encounter Strong Customer Authentication on daily basis and hopefully that will not spoil customer experience while using payment services.

## Interested in help/advice regarding PSD2 roadmap development or validation, consultation regarding technology selection or any other information?

### Please contact:

**Aivars Belis**
*Board member / Principal consultant*
+371 2944 6951
aivars.belis@vedicard.eu

**Ludmila Bērziņa**
*Managing director / Principal consultant*
+371 2910 5855
ludmila.berzina@vedicard.eu

**Indra Kešāne**
*Board member / Principal consultant*
+371 2922 1332
indra.kesane@vedicard.eu

VediCard is a payment and banking industry consulting company established in January 2012 by a team of experienced card business professionals. VediCard offers quality experts advice, guidance and help starting from strategy development, market research, business modelling, regulatory advices and required document development, supplier selection, solution requirements definition ending with being main integrator, project management, solution design, UAT development, solution implementation, migration and certification as well as training.

© 2017 SIA Vedicard

*This material has been prepared for general information purposes only and is not intended to be relied upon as any professional advice.*