WORLDLINE

Time to get practical

A PSD2 with a step-by-step preparation

White Paper

Digital Payments
for a Trusted World

Table of contents

#1

Foreward

Paris, Europe

It is close to a year since the European Commission's revised Payment Service Directive – or PSD2 – came into force on January 13 2018. The impact of the innovative regulatory framework is being felt not only within Europe but across the globe, where a wave of open banking initiatives inspired by PSD2 is currently transforming the payments landscape as we know it.

One of the objectives of the mandatory directive was to enhance innovation and competition in the European payments industry, by introducing two new roles as Third-Party Providers (TPPs) in the banking ecosystem: Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs).

Both roles are open to current and new players in the ecosystem, and the banks are required to support these new service providers if their customers want to grant access to their (payment) accounts as described in the directive's Article 66 and Article 67. This new practice is commonly referred to as "Access to Account" or XS2A.

At this point, the European payment industry is busy implementing the regulations – most recently the Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and secure communication – and figuring out how to make PSD2 work in practice.

Until now, 5 of the 28 European members states have failed to communicate full transposition measures to the European Commission, while infringement procedures by the Commission are pending against 16 member states "due to the lack or delay of the notification of national transposition measures or their incompleteness [...]"[1].

In turn, this is creating a degree of uncertainty within the industry, both regarding the implementation timeline going forward but also regarding the legal status and operational capabilities of TPPs in the countries that have yet to implement PSD2 completely.

Arguably, the reactions to PSD2 amongst the European banks fall into two categories; some banks choose to adopt a minimum compliance approach, where they direct customers to a multipage web browser to authenticate; others recognise the regulations as a unique opportunity to augment services and redefine their value proposition towards their customers by engaging in mutually beneficial relationships with the TPPs through open APIs.

No matter the approach, the deadline for PSD2 RTS compliance is fast approaching. By March 2019, banks must have their open APIs ready for testing by approved AISPs and PISPs, so that the TPPs can successfully integrate by September 19 2019[2], where the RTS become mandatory.

Practical step-by-step PSD2 guide

Looking towards this final deadline, banks need to adjust their solutions fast in order to meet compliance requirements and prepare for an Open Banking reality.

Addressing the urgency amongst banks for qualified and immediate assistance, this whitepaper will shed some light on possible opportunities and includes a practical step-by-step preparation guide to PSD2 for banks.

The guide encompasses preliminary questions that banks need to consider as soon as possible to understand suficiently their own potential positions and roles going forward.

Being a European leader in the e-payments and transactional services sector, Worldline possess the necessary competences and technological and industrial capacity to help banks unfold their PSD2 potential in the manner that suits the banks' specific needs. They include managing several business workflows in line with European standards, providing simple and secure developmental and administrative portals, and ofering additional services to help banks retain customer relationships as part of an integral Open Banking strategy.

However, whether a bank chooses – at some stage – to turn to Worldline as PSD2 provider or decides to try to go all the way alone, the same questions apply as part of the preparation process.

Prior to the step-by-step guide, we will give a very brief introduction to the key elements of PSD2. If you are already familiar with PSD2, you can move directly to chapter 4.

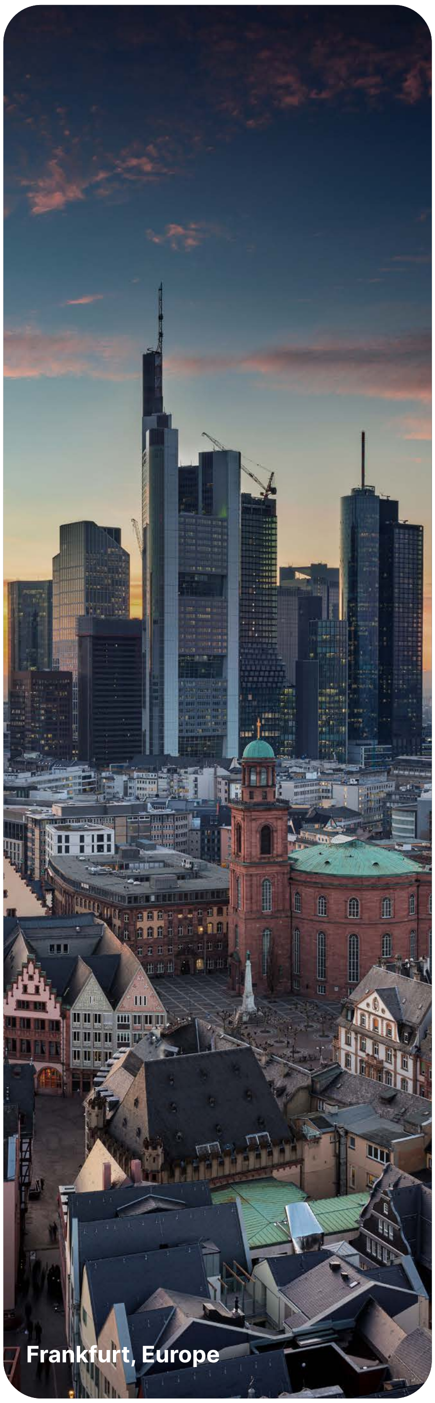
[1] https://ec.europa.eu/info/publications/payment-services-directive-transposition-status_en

[2] It should be noted that it is up to the relevant national regulator – or FSA – to decide how "ready" the APIs of the test environment need to be.

#2

From PSD to PSD2

To the surprise of a great many Europeans, who used to believe that the EU system was far too bureaucratic to ever take the lead on innovation, PSD2 has turned out to be more disruptive than anything any bank would expect from any fintech start-up.



Frankfurt, Europe

Clearly, the new directive, conceived by the European Commission and adopted by the European Parliament and the Council of The European Union, did not come out of thin air. PSD2 is an enhancement and further development of PSD, which was adopted by the EU in 2007. In a press release on 8 October 2015, the Commissioner of Competition, Margrethe Vestager, said :

"We have already used EU competition rules to ensure that new and innovative players can compete for digital payment services alongside banks and other traditional providers. Today's vote by the Parliament builds on this by providing a legislative framework to facilitate the entry of such new players and ensure they provide secure and eficient payment services. The new Directive will greatly bene it European consumers by making it easier to shop online and enabling new services to enter the market to manage their bank accounts, for example to keep track of their spending on diferent accounts".[1]

Legal platform for SEPA

For many years, a successful realisation of The Single Market Strategy has been one of the most important overall goals of the European Commission and the European Union. The strategy has been divided into separate sub-strategies: the Single Market for Goods, the Single Market for Services, and the Digital Single Market.

As part of the latter, the Single Market strategy for Payments materialised for the first time in 2007 in the form of the first Payment Services Directive or PSD (Directive 2007/64/EF) which became law in November 2009 and – among other things – provided "the necessary legal platform for the Single Euro Payments Area[2]" or SEPA.

The idea behind SEPA was not at all new in 2007. In fact, it was already part of the Lisbon Agenda launched in 2000, and, later that year the Commissioner for Internal Market, Frits Bolkestein, stated that: "There is a clear need for a change. [...] The Commission's political objective is exactly that: a modern Single Payment Area for the entire EU where there is no frontier effect for cross-border payments."[3]

Cost reduction of up to 28 billion Euros

In a later speech, Bolkenstein said that "a Single Payments Area will mean lower costs for payments, an end to unnecessary delays and much greater certainty over security and legal responsibility."[4] Furthermore, he emphasised that a Single Payment Area would also be "crucial for the competitiveness of the EU economy."[5] Stronger competitiveness was one of the very reasons for the launch of the irst Payment Service Directive.

In December 2007, the EU Commission stated its ambition of generating a reduction in costs of up to 28 billion Euros a year thanks to the new directive..

«Currently each Member State has its own rules on payments, and the annual cost of making payments through these fragmented systems is as much as 2-3% of GDP. Payment service providers are effectively blocked from competing and offering their services throughout the EU. Removal of these barriers could save the EU economy €28 billion per year overall."[6]

These significant economic bene its and the synergies of this type of European consolidation paved the way for new pan-European legislation.

[1] http://europa.eu/rapid/ press-release_IP 15 5792_ en.htm?locale=en

[2] http://ec.europa.eu/fnance/ payments/framework/index_ en.htm

[3] http://www. europeanpaymentscouncil. eu/index.cfm/newsletter/ article

[4] http://europa.eu/rapid/ press-release_IP 03 1641_ en.htm?locale=en

[5] http://europa.eu/rapid/ press-release_IP 03 1641_ en.htm?locale=en

[6] http://europa.eu/rapid/ press-release_IP 07 1914_ en.htm?locale=en

#3

PSD2 - The most important news

The PSD2 (Directive 2015/2366/EU) starts out with 113 introductory recitals setting the scene and explaining the reasoning behind the new directive.

Brussels, Europe

The main reason for updating PSD1 was the immense development and growth within the retail payment market and the related digital technologies – such as mobile payments - since the first directive in 2007. The development has "given rise to significant challenges from a regulatory perspective. Significant areas of the payments market, in particular card, internet and mobile payments, remain fragmented along national borders."[1]

This fragmentation, in combination with rapid technological advancement (resulting in many new products and solutions which fall outside the scope of the old directive) had, according to the EU Commission, led to "legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas."[2]

The Commission's conclusion was that the PSD1 framework was no longer adequate and an update was necessary to take the next steps towards full integration across the EU:

The continued development of an integrated internal market for safe electronic payments is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market."[3]

Access to Account (XS2A)

The most talked about, and most important, innovation in the new directive is that banks are required to provide access to payment accounts for Third Party Providers

(TPPs) – on the condition that the TPP has received a permission from the bank customer to whom the accounts belong. This new requirement is stated in the directives' Article 66 for Payment Initiation Services (PIS) and Article 67 for Account Information Services (AIS):

Article 66. Rules on access to payment account in the case of payment initiation services. 1. Member States shall ensure that a payer has the right to make use of a payment initiation service provider to obtain payment services as referred to in point (7) of Annex I"

And : *Article 67: Rules on access to and use of payment account information in the case of account information services. 1. Member States shall ensure that a payment service user has the right to make use of services enabling access to account information as referred to in point (8) of Annex I."[4]*

The two XS2A articles, written and proposed by the European Commission and The two XS2A articles, written and proposed by the European Commission and adopted by the European Parliament and the Council of The European Union, are nothing less than historical in terms of their perspective and potential impact on the entire European financial sector. >>

[1] http://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=DA, recital 4, p.36

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=DA, recital 4, p.36

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=DA, recital 5, p.36

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=DA, p.92 and p.93

Definitions

AISP

Account Information Service Provider

An AISP is a Third-Party Provider (TPP) which, with access via a standardised interface (e.g. an API), can draw information from a customer's (payment) account in a bank. For example, this could be PFM tools which aggregate data and create an overview, or lending companies using the access to create a precise credit score for a customer.

ASPSP

Account Servicing Payment Service Provider

An ASPSP is "a payment service provider providing and maintaining a payment account for a payer." For the time being the role of ASPSP is covered by banks.

PII

Payment Instrument Issuer

Not only ASPSPs issue payment instruments. There is an increasing number of merchant or airline issued payment instruments. PII can utilise AISP or PISP (see below) to conduct fund checks and/or transactions.

PI

Payment Instrument

The directive defines the PI as "a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order."

PISP

Payment Initiation Service Provider

A PISP is a Third-Party Provider (TPP) with an access via a standardized interface (e.g. an API) and which can carry out payments directly from a customer's account through the banks' own A2A infrastructure. Examples of this kind of services are Sofort (owned by Klarna) and Trustly.

PSP

Payment Service Provider

This category covers all providers that ofer services for accepting electronic payments. This includes card-based payments (credit/debit) as well as account-based (real-time) transfers.

PSU

Payment Service User

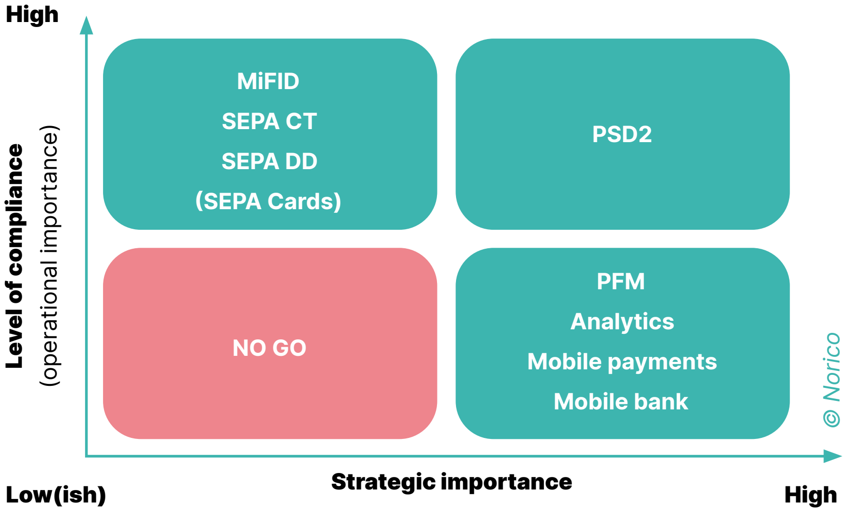
A PSU is a legal entity – e.g. an individual or a corporation – with an ASPSP account "making use of a payment service in the capacity of payer, payee, or both."

TPP

Third Party Provider

A TPP is a third party, which is granted access to a bank account either as an AISP or a PISP. Not to be confused with the concept of a TTP – Trusted Third Party – as used in cryptography.

Strategy vs compliance



As this diagram shows, PSD2 is unique in that it has both a strategic and an operational importance. This is also challenging for many organizations as the compliance teams and the marketing teams are often not used to working together.

Concern among bankers

The “Access to Account” requirement is disruptive in several ways:

It imposes operational risks and costs on the banks since they are responsible for finding secure and efficient ways of communication to provide access for the potentially huge number of diverse TPPs.

Furthermore, the banks continue to be liable for all transactions and are expected to react promptly to all customer complaints. If a TPP finds itself involved in a compromising transaction, it will need to prove its innocence. At the same time, the banks must give the TPPs – which can include innovative fintechs, global tech giants, and competing banks – access to their customers’ accounts.

This means that banks face the risk of losing the direct relationships with their customers and therefore of being reduced to the role of basic infrastructure providers – and this will mean a drastic cut in their revenues.

Seen from this perspective, it came as no surprise that 88 % of all bank senior executives in a survey conducted by PWC in 2016 expressed concerns about the possible direct consequences of these new requirements for the European banking industry.[1]

New opportunities

Despite these reasons for concern, PSD2 has proven a unique strategic opportunity for the banks who have the courage and the innovative power to seize and unfold it. By the very nature of their business, banks are endowed with a wealth of valuable customer data like transactional data, spending habits, and credit records.
In an increasingly digitized world, such data has assumed a central role as a means of delivering value-added services to customers. Consequently, it is highly sought after, particularly by TPPs.

The fact that PSD2 only expect banks to grant TPPs access to the customers’ payment accounts – and not additional accounts and information needed for TPPs to create a complete aggregated experience for their customers – leaves the banks in a favorable position to negotiate profitable deals with the TPPs that provide them with access to such accounts and information in return for a piece of the payment value chain.

Following this line of reasoning, banks should try to look beyond the competitive relationship that was initially articulated between the two parties to a point where TPPs are considered an entirely new customer segment. Many TPPs are new and inexperienced players in the payment industry, providing the banks with an ideal opportunity to offer their assistance, expertise and push premium services within areas of e.g. marketing and back-office management.

By creating additional products and services – like onboarding of third parties, real-time account information access for AISPs, certification of applications, test infrastructures, and fraud checks – around its APIs, banks are able to define new commercial business model for themselves and develop additional revenue streams.
At the same time, TPPs can help banks redefine their customer-relationships by placing the customer experience at the heart of the new banking business model. That being said, banks also have the opportunity to become TPPs themselves and tap into competing banks’ accounts if they want to launch payments solutions themselves (as a PISP) or launch information/data aggregating services in the role of an AISP.
As such, competition and collaboration do not need to be mutually exclusive.

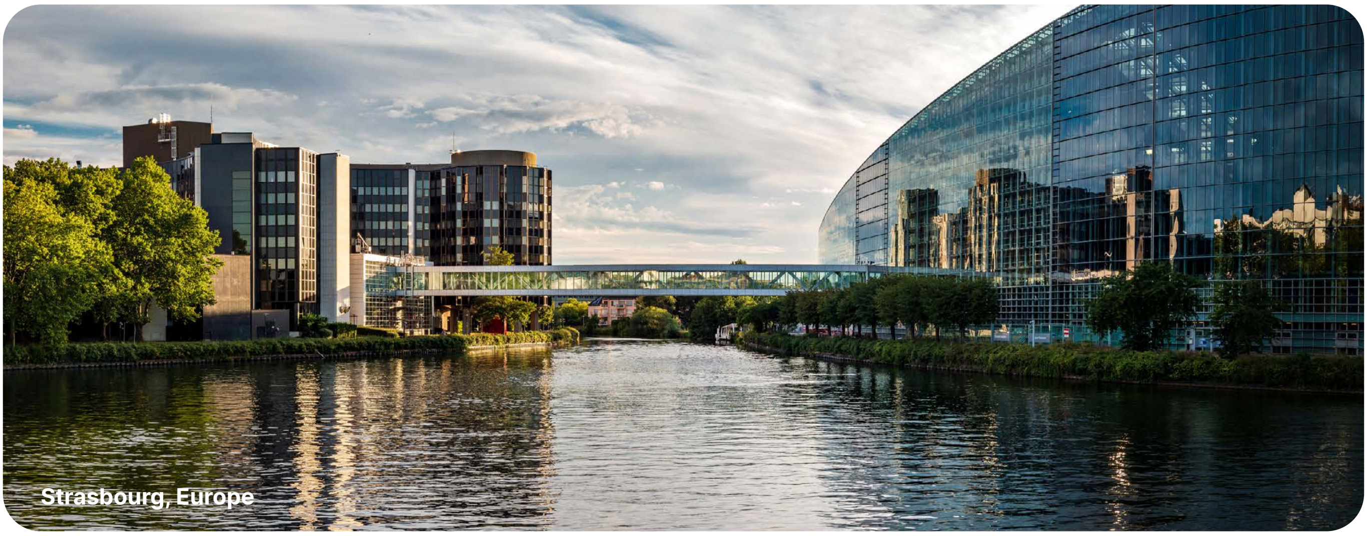
In conclusion, PSD2 points in the direction of Open Banking and should inspire banks to go above and beyond PSD2 compliance and to keep the bank account central to this innovation.

[1] In Q1 of 2016 PWC made a survey amongst senior executives in 30 European banks revealing “a mixed, but mostly negative, perception of PSD2.” 88% of those interviewed believed that PSD2 would impact their business, but only a minority had a PSD2 strategy. https://www.strategyand. pwc.com/media/file/Catalyst-or-threat.pdf, p. 12 and p. 22.

#4

Step-by-step guide for banks

Based on our own market research, we know that many banks still have an immediate need for practical PSD2 guidance. In the following section, we will present a short step-by-step preparation guide based on a number of questions that banks need to consider as part of their PSD2 preparation exercise.



Strasbourg, Europe

On 13 March 2018, the Regulatory Technical Standards (RTS) concerning Access to Account and Strong Customer Authentication was approved and publicized by the European Commission, entering into force the following day. This means that the RTS will apply from September 2019, leaving less than a year for all European banks to be PSD2 compliant.

Following the latest timeline provided by the European Banking Authority (EBA), these are the dates that should be top of mind for banks in 2019:

14 March 2019: Deadline for banks to have their open APIs ready.

14 June 2019: Application deadline for banks who seek fall-back exemption.[1]

14 September 2019: Deadline for banks to be fully in line with the RTS.

In addition, the EBA has also recently (July 2018) published its inal guidelines on fraud reporting under PSD2. The guidelines require payment service providers to "[...] collect and report data on payment transactions and fraudulent payment transactions using a consistent methodology, de initions and data breakpoints."[2] This means that all PSPs should already prepare to collect data from the 1st of January 2019.

Looking ahead, banks have a number of important deadlines to meet, and for those banks who have not yet started the compliance process, there is absolutely no time to waste.

As regards the compliance part of PSD2, the banks need to address the following basic questions:

- What do we need to do to be PSD2 compliant?
- Do we have the internal resources needed to become compliant in time?
- Do we need external help to complete the compliance process?

But before the banks can even start answering those questions, they need an overview of all elements included in a full PSD2 compliance. So, the questions here are:

- Which elements do a PSD2 compliance include?
- How many of those elements do we have covered already?

[1] For a bank to receive a fallback exemption, an API must have been available for testing for six months as well as been working in production for at least three months.

[2] https://www.eba.europa.eu/-/ eba-publishes-fnal-guidelines-on-fraud-reporting-under-psd2

Full PSD2 compliance for banks includes at least the following seven elements. And each element opens up new questions:

1. Compliance with a dedicated interface handling communication with TPPs Banks must be able to offer a dedicated interface managing account access for TPPs based on common and secure communication standards: it seems that open APIs will cover this need, but industry standardisation is in progress.

Basic questions

- Do we have a plan ready for the XS2A compliance process?
- Are the IT department and the compliance department in our organisation aligned? Have they met and started planning the project together?
- Do we know what it takes to develop the APIs needed?
- Does our IT department have the time and the skills for the design and coding of the APIs?
- Do we have a suitable test environment in place enabling us to run the necessary tests before releasing our APIs and opening up the accounts? (security is crucial in this case)
- What will it take to set up an external test environment for TPPs?
- Who will produce the documentation required?
- Do we know the costs (in time and money) of the compliance project?

Vienna, Europe

2. SCA approach How are we, as a bank, going to do this?

According to Article 97 of PSD2: “Member States shall ensure that a payment service provider applies strong customer authentication where the payer: (a) Accesses its payment online; (b) initiates an electronic payment transaction; (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.”

Furthermore, the article states that the same shall apply for data (and not only for payments) when it is “requested through an account information service provider.” By default, liability for Strong Customer Authentication (SCA) lies with the banks, and the banks need to decide as soon as possible how they are going to comply with the SCA requirement. Even banks who already have a functioning SCA setup need to consider whether their solution can handle a significant increase in transactions generated through potentially thousands of new TPPs, and whether they might want to improve the user experience by offering several types of SCA.

Furthermore, the banks need to be aware that decisions around SCA cannot wait for the PSD2 RTS deadline because weak authentication opens up a GDPR (General Data Protection Regulation) hole.

GDPR came into force in May 2018, and as far as SCA is concerned, this date was the actual deadline for the banks even though the PSD2 requirements come into force at a later date. No SCA means stored and weak credentials, which can be breached and may be used to hack third parties, who can then subsequently sue the bank for any fines.

Implementing an open API with no SCA in place is asking for trouble and is simply not an option for the banks. The banks need to ask themselves several questions as soon as possible regarding this topic. Fines are clearly estimated £in the GDPR, so the financial risk is highly significant.

Basic questions

- What is the status of our SCA setup?
- What kind of SCA solution do we want to use going forward?
- Do we want to offer more than one solution?
- Do we want to invest in the best possible user experience and turn our SCA solution into a competitive resource?
- Are we able to scale our SCA solution so that we can handle a significant increase of SCA-based transactions?
- Do we have a plan ready for design and implementation of our future SCA solution?

3. Authentication reset processes

With the more frequent and versatile use of the banks' SCA solution across different TPP-driven solutions, the banks issuing SCA should anticipate a higher load on their customer care processes as well as more attempts on social engineering.

In theory, banks should apply SCA to deliver or reissue SCA credentials, meaning that whenever a customer requests new SCA credentials they should use SCA. This is practically a Catch 22 as most banks will only have one SCA solution and not a fail-over of equal strength.

Banks, therefore, need to make a careful assessment of their current systems and procedures related to issuance and resetting of credentials.

Basic questions

- What is the current capacity of my service center?
- Can my service center scale if needed?
- Are the current manual authentication procedures sufficiently strong?
- Do we have systems in place to detect social engineering attacks?
- Should we implement a secondary SCA solution to act as a fail-over?

4. Sizing the problem of handling the API calls into their core systems

Any good business needs to be prepared for success. But with PSD2 and TPPs accessing the banks' systems via APIs, banks also need to prepare for successful TPPs – and even for TPPs that by mistake (or by design) generates high load on the APIs.

The creativity of TPPs will lead to a load on core systems in a way that might be difficult for banks to anticipate. This means that load balancing and scalability are of the essence. Banks also must ensure satisfactory response times – not only towards the TPPs but also in their own core systems. It is vital for banks not to jeopardise the running of their own businesses because of heavy load on the systems from TPPs.

In addition, this capacity planning must be done with attention to the fact that instant payment serves as a key milestone to answer the API calls because banks must have the same level of service for TPPs as for their customers' calls through the online banking website.

Basic questions

- How many calls to our APIs do we expect?
- What types of calls do we expect?
- Do we have proper load balancing in place?
- Are our core processes safe during heavy loads?
- How much can we scale our core systems?
- How do we communicate error messages to TPPs?

5. Stress testing their systems – to make sure the bank is not inadvertently opening up security holes with the new digital payment channel.

It cannot be emphasised enough how important it is for the banks to prepare carefully for any possible security incidents that might occur as a consequence of the new PSD2 requirements of XS2A for TPPs. The banks' IT departments should team up with the internal PSD2 experts as well as with external PSD2 service providers – like Worldline – to think through all possible risk scenarios that PSD2 services might inflict on the bank.

Opening up payment accounts for third parties is certainly something that could introduce a number of security risks, but, at the same time, it might introduce new patterns of activity which could mistakenly be interpreted as security breaches. For example, a large number of requests related to an ultra-popular TPP might be interpreted by the bank as a Denial of Service (DoS) attack.

Basic questions

- Do our IT people understand the basics of PSD2? (or should they be offered a crash course)?
- Do we have a complete overview of possible new risk scenarios that might be inflicted on our bank as a direct consequence of the PSD2 requirements? Which systems will be the most likely to break?
- What happens if different components break down under the load?
- What are the fail-over mechanisms?
- What kind of error messages do we transmit (and what kind of information do we share)?
- How do we tell the difference between a DoS attack and an ultra-popular TPP?

6. Figuring out how to identify the TPPs

The large number of expected new encounters between banks and TPPs going forward raises some complex questions. How will the banks be able to authenticate in a suficiently secure way that the TPPs are who they claim to be, and that they have the rights to gain access to a certain bank customer's account? Clearly, the banks cannot jeopardise security by opening up to TTPs unless they are absolutely certainty of their identity.

For this purpose, EBA Clearing subsidiary PRETA is currently testing a central repository – known as Open Banking Europe (OBE) directory – which lists the TPPs with their characteristics. The directory is expected to be fully operational in January of 2019. By screenscraping the 28 websites of each national regulator, PRETA ensures that all information is standardized and registered in one place. However, the repository will only reflect the information provided by the national regulators on their own websites, which leaves the question of liability if a national regulator fails to update accordingly.

Set aside the liability concerns, a register with TPP names does not assure the banks that the TPPs are the ones listed in the register, even though they claim to be so. In accordance with Article 15 of PSD2, the "EBA shall make the register publicly available on its website", and since this means that anybody can find the names of the TPPs registered, a secure authentication method and procedure – besides checking the register – is needed for the banks to ensure that the TPPs are actually the ones mentioned.

Something more is needed. Which is why the European Telecom's and Standards Institution (ETSI), in accordance with these concerns, has defined a PSD2 standard (TS 119 495) for implementing the requirements of the RTS for use of qualified certificates as defined in eIDAS regulation since September 2017[1]. Now, EU regulations guarantee the validity of any digital certificate throughout its territory, regardless of the country of origin.

A Qualified Trust Service Provider (QTSP) – which must be given qualified status and permission from a supervisory government body to provide Digital Certificates – will be in charge of issuing the certificates and managing their overall lifecycles.

Basic questions

- Do we have proper authentication in place to verify that the TPPs knocking on our door are the ones they claim to be?
- How do we avoid spending too much time on assurance and still ensure a suficiently high security level?
- Once identified, how do we ensure that the TPPs have the permissions from the account owners that they claim to have?
- Are we able to check the validity of a qualified certificate from a TPP?
- How do we know that the certificate has not been revoked by an issuing authority in another EU country?
- Will we be able to scale our solutions and procedures for TPP handling?

7. Figuring out how transactions are made.

As there is no governing scheme in place for PISP-initiated payments – except the SEPA scheme managing the credit transfer – banks must decide for themselves how to handle the request for settlement of the transactions. This includes adding and storing suficient transaction data (and metadata) to handle monitoring, as well as disputes and claims, eficiently.

A bank can choose to enter into diferent consortia or other types of collaboration to prepare for PSD2-based payments. Alternatively, everything can be prepared in-house.

While account-based payments are very close to the core from a bank perspective, gearing up to handle the potential volumes and, more importantly the new role of the bank infrastructure, is a big step for most banks. This makes the strategic decisions even more important. The good news is that the innovations around the bank account will allow the banks themselves to deliver improved services to their clients.

Basic questions

- What kind of role do we want to play in transaction settlement?
- Will we handle settlements bilaterally with other banks?
- Should we join a consortium or hook up to a specialised integrator?
- Which transaction data and metadata is needed to operate efficiently?
- Can we leverage this new type of transaction handling to open up for new (data driven) services?
- Is our dispute management setup geared for non-card-based disputes?

Berlin, Europe

[1] https://www.openbankingeurope. eu/standard-etsi-ts-119

#5

Worldline’s PSD2 services for banks

The number one challenge for all banks brought about by PSD2 is how to implement the requirement of providing access to accounts in a cost-efficient manner without jeopardising the bank’s security, losing customer relationships and reducing themselves to the proverbial “dumb pipes” (still with the potential cost of liability!), while the TPPs take over the end-consumer relationship.

Milan, Europe

This challenge does not only mean exposing a dedicated interface to the TPPs. It covers a range of areas in which banks are required to:

- handle new business workflows in order to process the queries (AIS, PIS, PIIS) coming from the TPPs
- assist the TPPs on the usage of this interface
- export the expected data into regulatory reports

Today, Worldline deploys its solution WL Access 2 Account Compliancy to help

European banks cope with this challenge. For banks that lack the resources and competencies to handle PSD2 compliance themselves, Worldline’s solution is key for them to comply cost-effectively.

The solution includes:

- **The management of several business workflows** in line with the main European Standards to perform Payment Initiation (PIS), Account Consultation Services (AIS) and availability of funds (PIIS). More than collecting the requested data onto the Core Banking System, these workflows are in charge of checking the TPP, triggering Strong Customer Authentication, and analyzing/capturing the PSU’s consent.
- **A developer portal** where API documentation is published and which can also be used by the bank to support its TPP community (forum, FAQ etc). This portal also allows access to the sandbox environment, enabling TPPs to perform tests on APIs.
- **An administration portal** offering all the features for a bank to monitor activities and the performance of the solution, allowing it to export the expected data into regulatory reports.

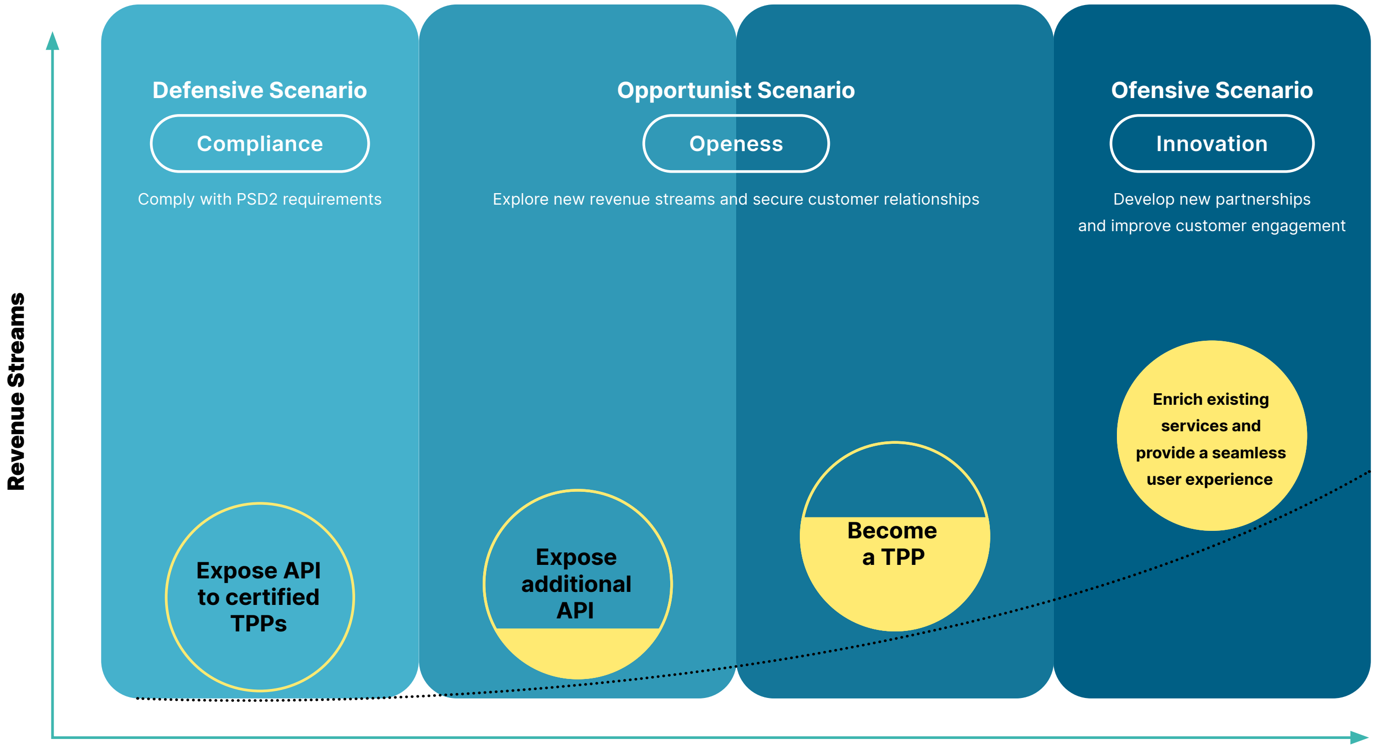
In addition to its XS2A Compliancy solution, Worldline also ofers optional services to help banks further their Open Banking strategy and retain customer relationships. These are:

- Additional APIs to support for instance customer onboarding and customer care as well as a monetization engine to de ine and follow the new business models associated with these additional data and services.
- Strong Customer Authentication solutions (WL Access Control Server, WL Authentication Process Management, WL Trusted Authentication, Exemption Rule engine, Risk Based Authentication) to cope with the expectations of the PSD2 RTS regulation but also to provide the end-user with a consistent and seamless experience whatever the channels used and the transaction asked for (card-based remote commerce, remote banking transfer, Access to Account, e-banking, e-identity).
- Fraud solutions covering the analysis of card & non-card transactions in line with the security policy of the bank to help minimize risks.

Towards Open Banking

Some of the most progressive banks are already sizing up the new area of Open Banking, and others have set out to become TPPs themselves. Those aiming for the TPP role are mainly banks which are very active in the acquiring business. However, retail banks with many account holders might also have strong interests in developing PISP and/or AISP services available to their end customers.

Whether a bank aims for just for basic compliance or wants to go much further, Worldline has the ability and the competences to act as a trusted strategic advisor as well as a technical service provider all the way.



Revenue Streams
Defensive Scenario
Compliance
Comply with PSD2 requirements
Opportunist Scenario
Openess
Explore new revenue streams and secure customer relationships
Ofensive Scenario
Innovation
Develop new partnerships and improve customer engagement
Expose API to certified TPPs
Expose additional API
Become a TPP
Enrich existing services and provide a seamless user experience

#6

Closing Remarks

Long before any European bank started thinking about Open Banking, companies like Amazon (2002), Twitter (2006), LinkedIn (2009), and IBM (2013)[1] realised the value of opening (some of) their APIs to the outside world.

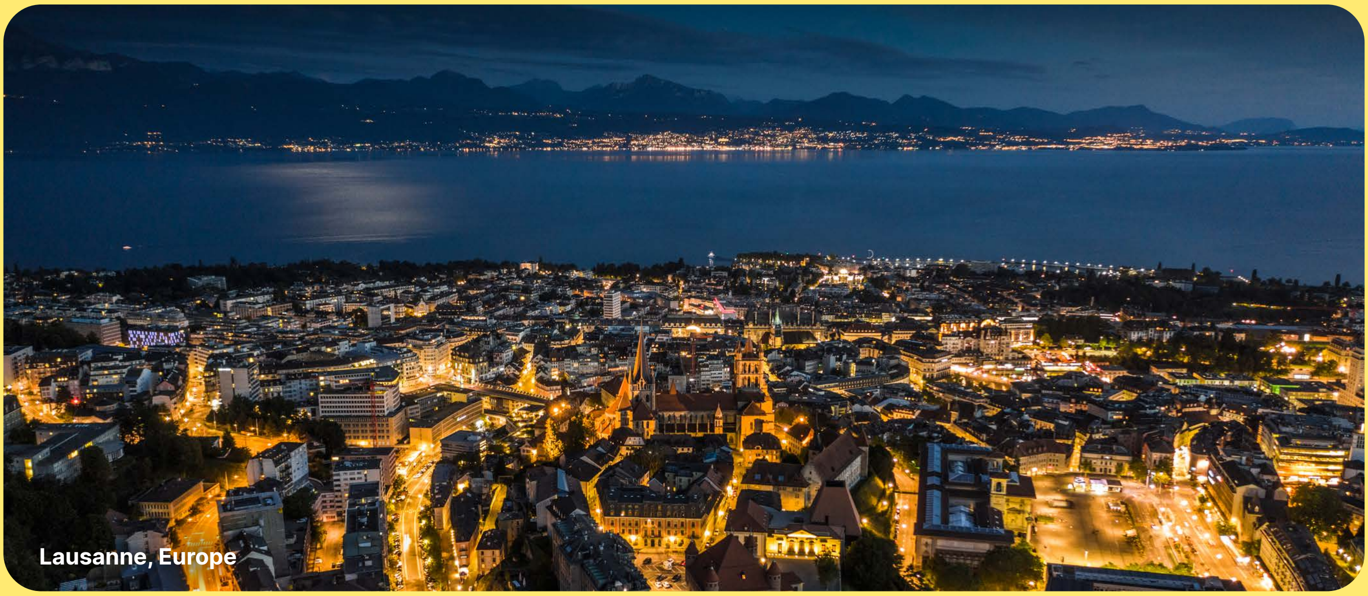
Within the payments industry, PayPal took the lead by introducing open APIs as early as 2004, when it first launched its developer portal and started inviting external developers to build new services to enrich the PayPal community. Since then, both MasterCard (2010) and Visa (2016) have opened their own developer portals.

Among the banks, the use of open APIs is still relatively new and only a few banks would claim to have an implemented Open Banking strategy. Some of the current frontrunners are BBVA[2], Crédit Agricole, and Denmark's Saxo Bank. However, in an increasingly competitive and technology-driven payments market more and more banks recognize the possibilities brought on by Open Banking, both in terms of improved customer experiences and new revenue streams.

Although PSD2 has applied since January 13 of 2018, some countries are still struggling to communicate full transposition measures to the European Commission. This is circulating a general sense of uncertainty in the European payments ecosystem regarding the implementation timeline while generating an ambiguous legal and operational status for TPPs in the relevant countries.

The finalization of regulatory technical standards, rulebooks, and certificates are to some extent counterbalancing the uncertainty by delivering an approved framework for all industry players to navigate within. But for banks, these additions are also gradually increasing the compliance burden and raising new complex questions about how best to cope with new business requirements.

Worldline believes that banks – small or large – can benefit greatly from the effects of PSD2 – if they position themselves in a timely and proactive manner. By managing business workflows, providing simple and secure developmental and administrative portals, and offering additional services that help retain customer relationships, Worldline possesses the necessary solutions for banks of all sizes and prospects – no matter if a bank wants to remain strictly compliant or assume a more competitive position in an increasingly Open Banking environment.



Lausanne, Europe

[1] In the case of IBM, developers outside IBM are invited to join Watson Developer Cloud and start exploiting the fascinating world of cognitive computing - https://www.ibm.com/watson/ developercloud/

[2] https://bbvaopen4u.com/en/ actualidad/psd2-and-open-apis-banking-start-exponential-era-fntech-and-online-payments

Amsterdam, Europe

About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry and #4 player worldwide. With its global reach and its commitment to innovation, Worldline is the technology partner of choice for merchants, banks and third-party acquirers as well as public transport operators, government agencies and industrial companies in all sectors. Powered by over 20,000 employees in more than 50 countries, Worldline provides its clients with sustainable, trusted and secure solutions across the payment value chain, fostering their business growth wherever they are. Services offered by Worldline in the areas of Merchant Services; Terminals, Solutions & Services; Financial Services and Mobility & e-Transactional Services include domestic and cross-border commercial acquiring, both in-store and online, highly-secure payment transaction processing, a broad portfolio of payment terminals as well as e-ticketing and digital services in the industrial environment. In 2020 Worldline generated a proforma revenue of 4.8 billion euros.

worldline.com

For further information
sales-fs@worldline.com