fabrick

# PSD2 Fallback Solution

Simplified complexity for the Banking Industry

fabrick
SHAPING FINANCE, TOGETHER

## Index

fabrick
SHAPING FINANCE, TOGETHER

# Foreword

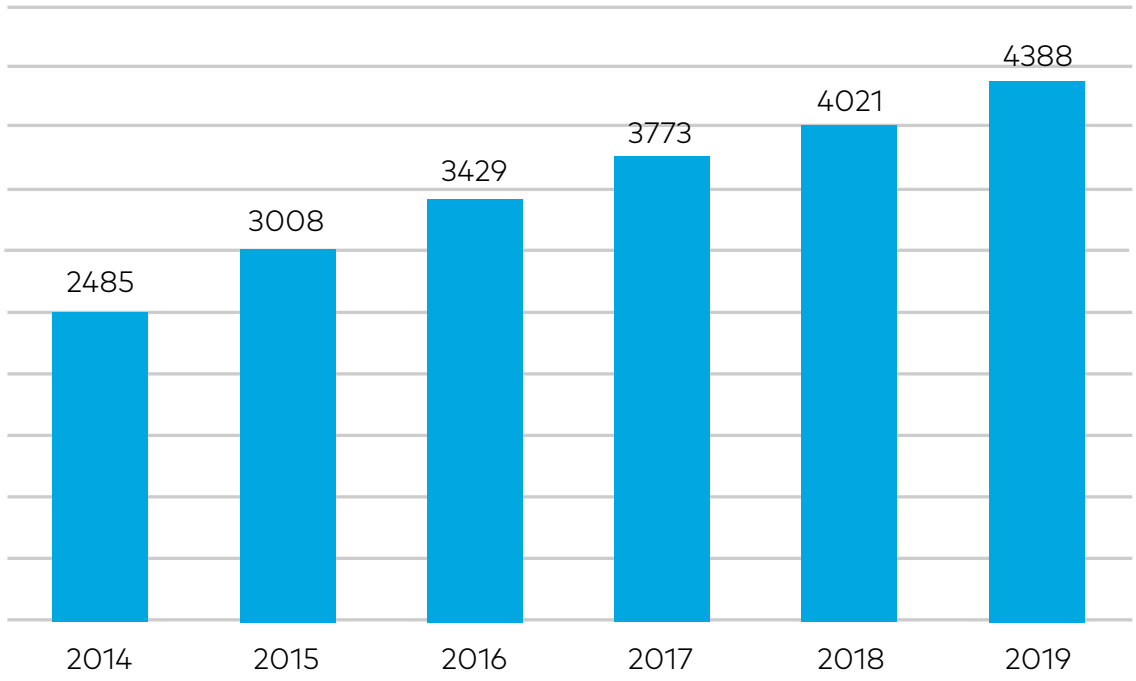
The world we live in is one of rapid change, brought on by the onslaught of the digital realm. Not least the banking industry, and that of the financial services at large, is being invested by paradigm shifts the reaches of which are still hard to grasp.

Even for those who are deep into it, like us at Fabrick, greasing their hands into the hogs and cogs of the new architecture that is arising on the back of the PSD2.

The Revised Payment Systems Directive has been handed down from the European Commission, and entices all banking institutions across the EU and EEA to update their standards of access for a new, digital-first world.

Indeed, it is not news to see charts, such as the one below, which explain how digital interactions have been creeping into an ever-growing array of daily activities, from cab hailing to food-delivery, all the way to full e-citizenship in some more advanced realities (most notably Estonia).

**INTERNET USERS OVER TIME (IN MILLIONS)**




From: wearesocial

What the PSD2 seeks to accomplish, therefore, is to support a digital upgrade of the banking and financial services sector, for which the disruption seen in other industries was long due.

Incidentally, this white paper seeks to outline, a solution we developed at Fabrick, yes!, but more than that one of the most delicate aspects that the new European Directive has expressed with a very light touch (and sensibly so!), for it deals with the levels of service required by the new infrastructure.

And when it comes to digital communications + financial services, performance and security are all the more paramount.

As such, the Fallback Solution, which has been mainly seen as a safety net hopefully best avoided, has turned out to be a valid and ready-to-use solution for implementing a safe space on which, well, to fall back on, just in case.

The paper is a good hearted attempt at trying to explain the simplified complexity of such a solution, as much as hoping to create some food for thought for those who are deep into it.

fabrick
SHAPING FINANCE, TOGETHER

# PSD2 and APIs: the once and future paradigm

Since the financial crisis, there has been a growing trend in trying to reshape financial services for the modern consumer, updating not only ethical standards of transparency and ease-of-use, but also security and conformity of communications.

This has implied a boom in new companies, specialized in leveraging the technological landscape (e.g. Artificial Intelligence, Cloud Computing, etc.) to produce solutions that are reshaping expectations and behaviors; especially when it comes to three main activities:

1. Saving
2. Investing
3. Paying

**INBOX 1: SEPA AREA**
The SEPA area includes all Euro payments made within the 28 European Union (EU) Member States with the addition of Iceland, Norway, Liechtenstein, Switzerland, the Principality of Monaco and San Marino. From March 2019, the area has come to include the Principality of Andorra and the Vatican City

- 19 Countries in the EU and with the EURO
  ( Austria, Belgium, Cyprus, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Portugal, Slovakia, Slovenia, Spain)

- 9 Countries in the EU but not in the EURO
  (United Kingdom, Sweden, Denmark, Poland, Czech Republic, Hungary, Bulgaria, Romania, Croatia)

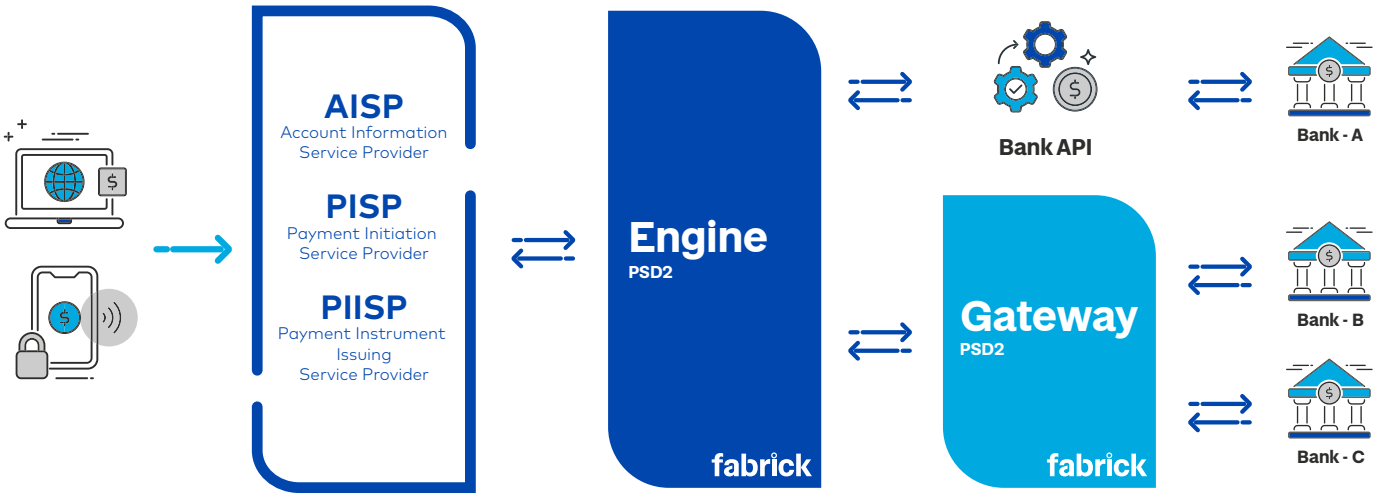
- 6 Countries not in the EU and not in the EURO
  (San Marino, British Crown Dependencies, Iceland, Liechtenstein, Norway, Switzerland, Monaco)

From:sepaitalia

**What does the PSD2 really mean, technically?**
The new European regulation has two major implications for how the banking industry and the financial landscape at large are to change.

The first implication is to have new financial intermediaries. If there were banks, eMoney and payment institutions, the PSD2 calls into being a novel type of company, which can intermediate communications at a technological level between the final user and the account holding institution.

As such, where financial institutions are redefined as Account Service Payment Servicing Providers (or ASPSPs for short), and the new intermediaries, generally defined, as Third Party Providers (or TPPs) will be of three categories:




**AISPs (Account Information Service Providers):** intermediaries that will be able to access on behalf of final users (or Payment Service Users in technical jargon), the PSU's bank accounts so as to allow the PSU to "read" the balance and the transaction list.

**PISPs (Payment Initiation Service Providers):** intermediaries that will be able to allow a PSU to initiate an online payment through a SEPA Credit Transfer (i.e. an ordinary money transfer within the SEPA area) without the need to go to bank (website or teller) to do so.

**PIISPs (Payment Instrument Issuing Service Providers):**
also known as CISPs (Card Information Service Providers), intermediaries like the AISPs above, with the marked difference that the accounts that these TPPs can access are not cash accounts, but credit card accounts.

**How does the PSD2 really work?**
In order for the PSD2 to come into being, the industry has seized upon a technology that has been around since before the World Wide Web: Application Programming Interfaces, or APIs for short.

APIs are none other than a means of communication between two machines that occurs through the Internet Protocol (or IP, to which we are usually more accustomed to when we input a website address into the search bar of our browser). When you type into the browser a website address, say www.fabrick.com, what you are doing is asking the machine to go there and show what there is.

APIs are exactly that: where the browser allows for a human-to-machine interaction, APIs allow for a machine-to-machine interaction.

Only they allow to not just retrieve information (the so called GET endpoints), but also allow to input information, edit information, and delete information.

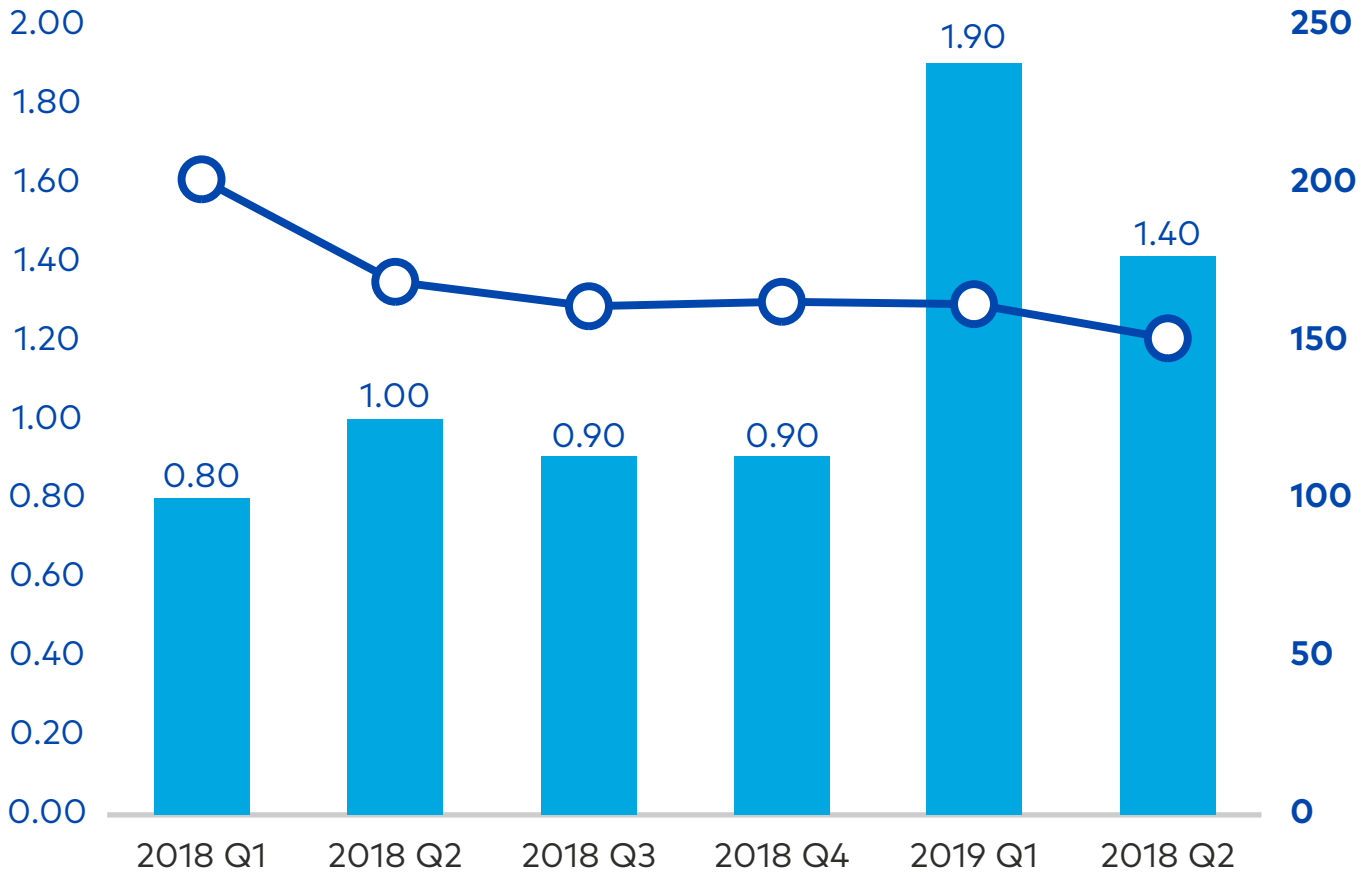
In the PSD2 context, this implies that when an app on a smartphone produced by one company (a FinTech to be sure) is opened, a final user should be able to retrieve the information usually available only by accessing the bank's app or website.

These novel methods of interaction between final users (PSUs), tech companies (TPPs) and financial institutions (ASPSPs) are actually already here, and have been around for some time. However, the way these interact have followed different custom approaches (e.g. screen scraping, see inbox) as opposed to an industry standard, thus limiting the effectiveness and reach of innovation in the financial space.

**New relationships, new issues**

Therefore, the need to build new relationships with new competitive players, which furthermore aim at market segments previously left untouched by incumbent institutions, leaves the "old" banks to respond to the paradigm shift with adequate responses. And the search for adequate responses usually alerts to new issues. Europe, albeit with marked differences, is witnessing an intense period in terms of new entrants and growing investments, bringing to market a greater array of solutions that are usually realized when working along with willing institutions.

**Total investment activity (VC, PE and M&A) in fintech in Europe**




Source: Pulse of Fintech H2'2019, Global Analysis of Investment in Fintech, KPMG International (data provided by PitchBook) June 30, 2019.

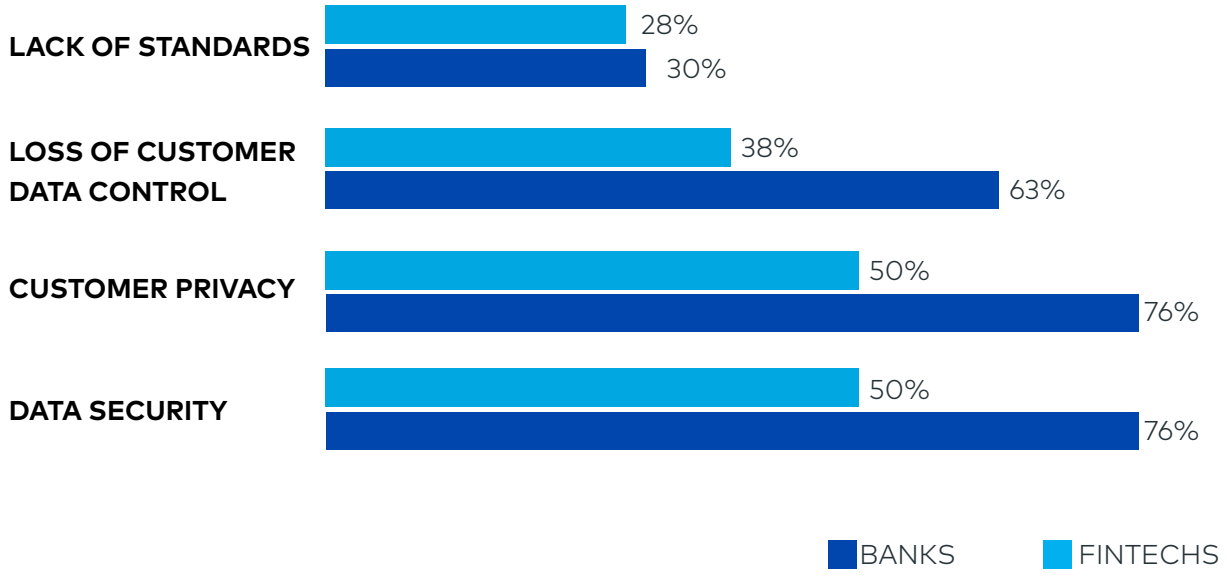
From: KPMG

The hectic pace of change, combined with a need to establish strong flows of sensitive data, is reflected by a widespread concern to the security of communications on the one side, and the performance of data flows on the other.

In other words, the hard balancing act that banks need to play out in this new digital-first, API-based context, is between guaranteeing that customer data are protected as they ever were, safe inside deep (digital) vaults, and the need to share the same data. However, the sharing of data in a digital space involves many actors, exposing it to hacking threats on the one side, and mere technical failures on the other.

It is no surprise, therefore, to see contingency frameworks also set out by the PSD2. And it being the so called fallback solution, aimed at guaranteeing connection in case of failure, while still upholding the security features implied by the Strong Customer Authentication.

**What level of concern do your firms have in the following areas when adopting open banking?**




Source: the percentage represents the fintech and banking executives who gave a rating of 6 or 7 on a scale of 1-7 for each category.

Fonte: pulselive

**INBOX 2: SCREEN SCRAPING**

Screen scraping is the process of collecting screen display data from one application and translating it so that another application can use it. This is normally done to capture data from a legacy application in order to display it using a more modern user interface. Screen scraping usually refers to a legitimate technique used to translate screen data from one application to another.

Under normal circumstances, a legacy application is either replaced by a new program or brought up to date by rewriting the source code. In some cases, it is desirable to continue using a legacy application but the lack of availability of source code, programmers or documentation makes it impossible to rewrite or update the application in an economically viable way. In such a case, the only way is to continue using the legacy application and to write screen scraping software to translate it into a more up-to-date user interface. Screen scraping is usually done only when all other options are impractical.

The screen scraping application must usually do both of the following:

- Capture screen input and pass it on to the legacy application for processing
- Return data from the application to the user and display it properly on the user's screen

Screen scraping as such is widely used by FinTechs the world over, however it presents security issues, which overcome by the Fallback contingency envisaged by the PSD2. From September 14, 2019, indeed, screen scraping beyond certified and validated processes will be deemed illegal (at least in Italy, but it will ultimately depend on National Competent Authorities)

From: Technopedia.com

fabrick
SHAPING FINANCE, TOGETHER

# Fallback solution: when efficiency and security are paramount

In order to mitigate the potential risks deriving from technical unavailability of the dedicated interface, the PSD2 authorizes the TPPs to use the interface commonly available to service users (i.e., the bank's website). This is the so-called Fallback Solution, that is activated until the appropriate level of availability and performance of the dedicated interface is restored.

Said differently, the Fallback Solution is a contingency mechanism in case the dedicated API service becomes unavailable, or is not working properly. In this instance, the Fallback Solution would essentially mean banks have to make their customer interface (such as internet banking) available for screen scraping with the ability to identify TPPs, until the API service is restored.

PSD2, however, has provided for the National Competent Authorities to establish exemptions for the ASPSPs' obligations: specifically, Banks can provide a dedicated interface that meets security requirements and conditions set out in the "Guidelines on the conditions to benefit from the exemption from the emergency mechanism of Article 33 § 6 of Reg. 389/2017" (EBA; 04.12.2018).

In this regard, the EBA stated that ASPSPs must:

1. measure on a daily basis the level of functioning / malfunctioning of the interfaces through specific key performance indicators;
2. publish quarterly statistics on the performance of the interfaces (both the dedicated and the user interface) in order to allow TPPs and the user to compare the service levels of each of the two types of interface;
3. subject the dedicated interfaces and the aforementioned KPIs to stress testing activities;
4. implement interfaces that do not create obstacles to TPPs (in particular with reference to authentication systems);
5. verify that any problems relating to the dedicated interface have been resolved without undue delay;

As such, Banks can benefit from an exemption if their dedicated interface fulfils said conditions, centered on how robust, available and well supported the solution is. However, in order to gain the exemption, the dedicated interface will also have to meet design and testing standards, and have been widely used for at least three months.

There are a number of challenges associated with the exemption process, especially given that these assessments include a technical analysis of each interface. Many regulators are very open about the fact they do not have the technical expertise required to perform all these assessments, so they are encouraging banks to use 'standardized' conformance tools available in the industry. Many have also mandated self-assessment and audit steps as part of the exemption application process. Nonetheless, there is still some way to go before obtaining a standardized landscape.

Indeed, banks who operate in more than one country need to apply for a fallback exemption more than once, depending on the corporate structure, on different local criteria and taking into consideration different deadlines. For banks with legal entities established in multiple European countries, the process can become quite a challenging piece of work.

"For example, in the UK, the exemption process is fairly straightforward and well assisted, so there isn't too much research to be done. In France, however, there are a number of additional hoops for banks to jump through, including the requirement to facilitate a full cyber audit carried out by an ANSSI-certified provider prior application for the exemption as well as several additional requirements."

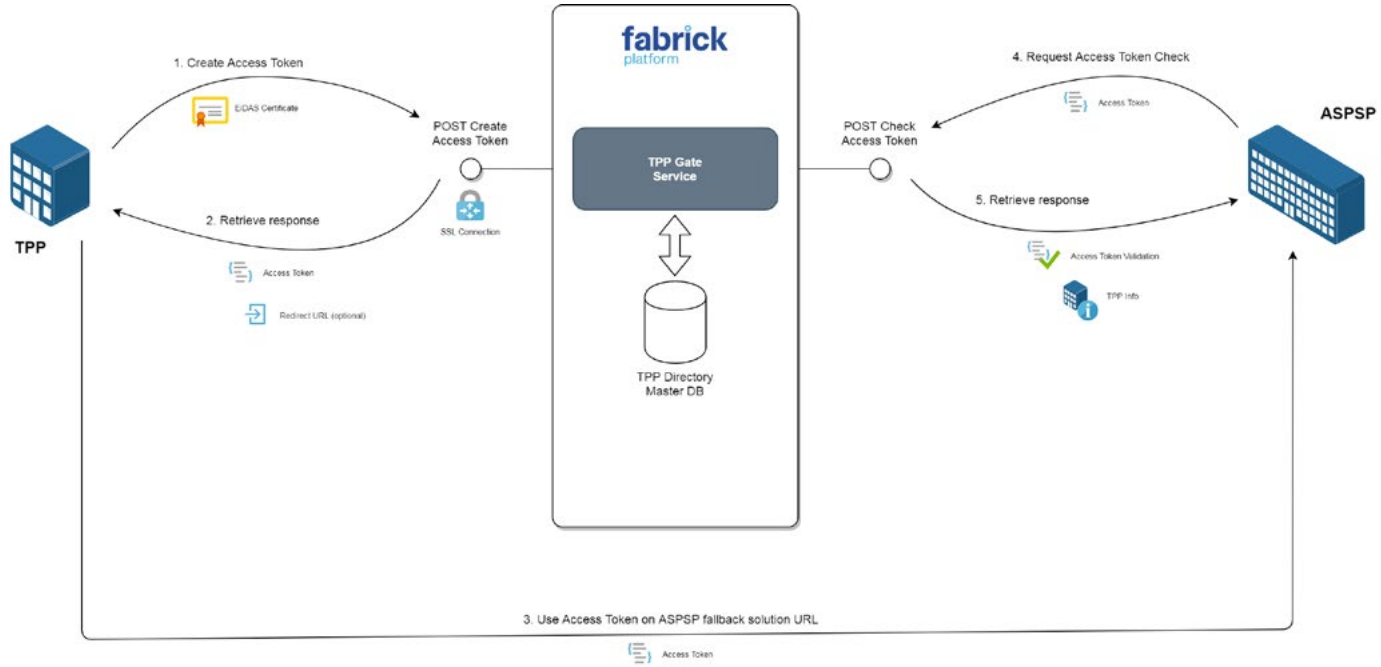
As such, for all those Banks and ASPSPs generally who feel that a fallback solution could be a technical advantage, as opposed to seeking out the exemption, there are possibilities that differ on the degree of trust and, inversely, control.

Fabrick has devised a solution, which can be adapted to three different tiers of control retention and data management. An ASPSP can differ markedly from its peers

when it comes to making decisions on the level of control, as much as on the liberty to manage data. As such, the three-tiered solution ranges from a first-tier solution, whereby Fabrick merely checks the validity of TPP information, to a third-tier solution, where Fabrick verifies and checks the eIDAS certificates along with providing updated TPP information.

**TIER 3 Fallback Solution**

In this scenario the ASPSP outsources the entire process of dealing with TPP identification. In this scenario, the TPP will request an access token that will be referred to the ASPSP, which will then check it through the gateway.




In other words, on one hand the TPP:

- creates an access token
- provides the same token to the ASPSP on the fallback solution interface

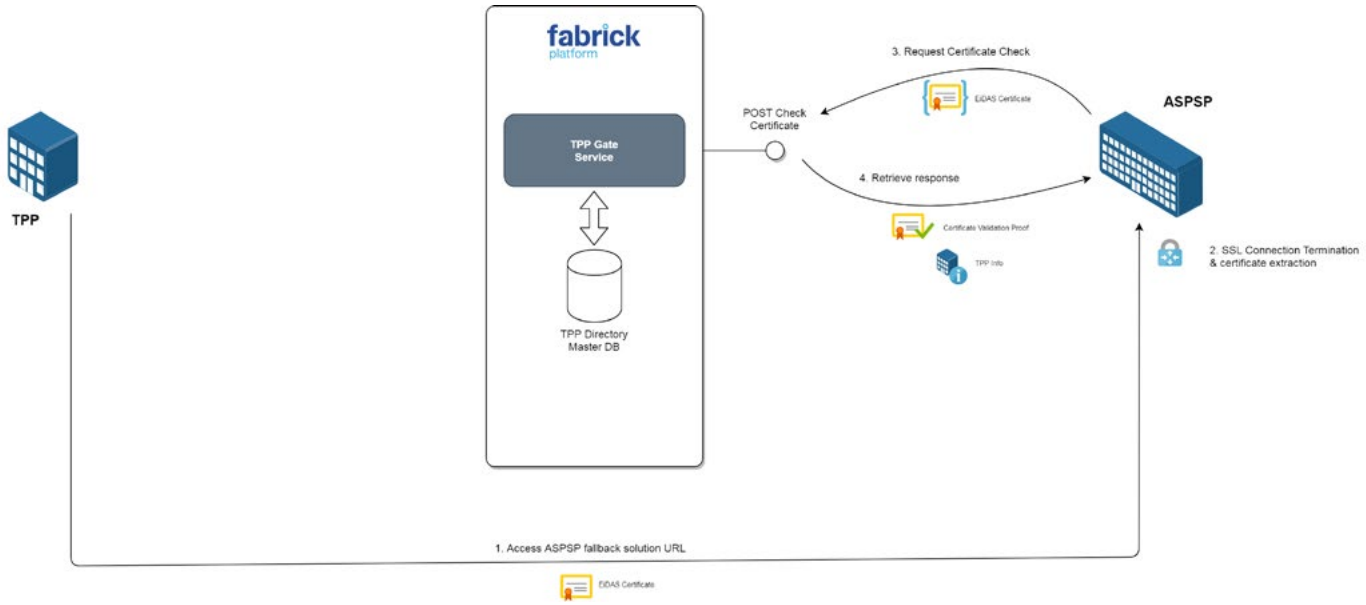
On the other hand the ASPSP will provide the access token for (implicit) validity check to the gateway, receiving in response complete TPP identification information.

**TIER 2 Fallback Solution**

In this scenario the ASPSP retains control, whereby the TPP uses the eIDAS certificate directly on the ASPSP's secondary interface, and the ASPSP has merely check its validity.

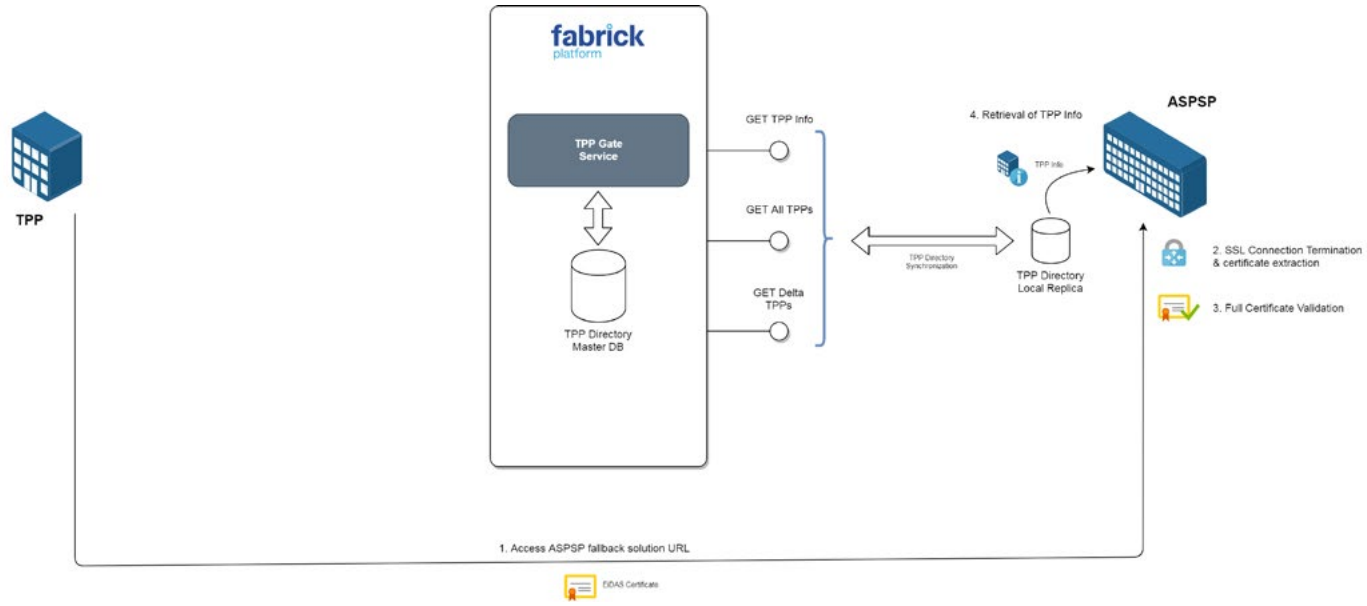
In other words the ASPSP:

- terminates the SSL connection
- provides eIDAS certificate for validity check
- receives the certificate validation proof along with complete TPP information



**TIER 1 Fallback Solution**

In this scenario the ASPSP retains the most control, whereby the TPP uses the eIDAS certificate directly on ASPSP's secondary interface, and the ASPSP has to access the TPP Directory to retrieve the information of the TPP which is presenting the PSU on the fallback solution interface.




In other words the ASPSP:

- terminates the SSL connection
- performs complete eIDAS certificate validation
- extracts TPP identification information
- retrieves TPP complete information from the TPP Directory

**INBOX 3: eIDAS certificates**

There are two types of PSD2 eIDAS certificates and each of them plays an important role:

QWAC (qualified certificate for website authentication) - is used for website authentication, so that ASPSPs and TPPs can be certain of each other's identity, securing the transport layer. Using this certificate guarantees confidentiality (nobody else could have read the data) and authenticity (that the data was not changed between the end points) of all data transferred through the channel. The ASPSP can choose between using an ASPSP QWAC server certificate or an existing SSL/TLS certificate to receive the TPP's identification request.

QSeal (qualified certificate for electronic seals) - is used for signing requests. The entity receiving digitally signed data can be sure who signed the data, that the data have not been changed since being signed. QSeals do not provide confidentiality of the data (i.e. there is no encryption of data). Yet, unlike QWAC, QSeal can trace and log the communication sessions.

From: FINEXTRA

fabrick
SHAPING FINANCE, TOGETHER

## Conclusions

The PSD2 is an outright revolution for the financial industry: it is a game changer because it alters requirements, behaviors and expectations of every stakeholder in the market significantly.

Users, lenders, savers, payers, banks, companies, institutions, startups and regulators are all in it, together.

Although there are provisions at every level for contingencies, back-ups, fallbacks, and service levels, it shouldn't surprise to expect radical changes happening to interactions and relations between interested parties.

As such, the need to rely on solid alternatives, likely to see it through the stormy winds of change, becomes an imperative. Thus hoping to have shed some light on what is, ultimately, a commercial choice, Fabrick's fallback solution is a versatile buoy, tightly anchored to the highest standards technology today has to offer.

If you'd care to know more, don't hesitate to contact us at sales.platform@fabrick.com.

fabrick
SHAPING FINANCE, TOGETHER

## Authors

**Francesco Merlo**
Platorm Architect

**Giulio Tartaglia**
Business & API Specialist

fabrick

SHAPING FINANCE, TOGETHER

**Fabrick S.p.A.**
P.zza G. Sella 1 - 13900 Biella
info@fabrick.com
fabrick.com

@fabrickfinance
Fabrick Platform
@FabrickPlatform