galitt

PSD2 & OPEN APIs: Threats and opportunities for the banking sector

…Are we moving towards Open Banking?

www.galitt.com

Contents

About this white paper & acknowledgements

Galitt, a company specialised in payments, and the law firm DS Avocats have come together to bring you this white paper concerning Open Banking and all the issues arising from France's implementation of the second Payment Services Directive (Directive 2015/2366), known as PSD2, which, on 13th January 2018, replaced and revoked in French monetary and financial law the original PSD1 from 2009 (Directive 2007/64/CE).

We would particularly like to thank the following people for their participation and expertise:

Clément Coeurdeuil: *CEO and co-founder of Budget Insight*

Clément Coeurdeuil is an engineer who graduated from the Paris Ecole Centrale in 2012, specialised in IT systems. A passionate entrepreneur, he co-founded Budget Insight with Romain Bignon in 2012. It is now the leader in the French field of aggregating financial data and initiating payment

Budget Insight provides account aggregation services (via its Budgea app) and also supplies APIs which allow banks and other financial institutions to improve their service provision. Authorised equally as a payment initiation PSP, this Fintech is based in France and Luxembourg and connected to over 300 financial institutions. Several hundred thousand businesses and individuals use its services daily.

Sébastien Taveau : *Chief Developer with Early Warning*

Sébastien Taveau is the Chief Technologist at Early Warning, where he supervises technological and innovative operations for P2P payment solutions. With over twenty years of experience in the field of mobile payment technology, he sees himself as a puzzle-solver and a look-out, scanning the horizon. Sébastien Taveau is an acknowledged expert in Open API, with numerous articles and appearances on CNN, The Wall Street Journal, The Huffington Post, Mashables, Reuters, Forbes, Dark Reading, Digital Transactions, Newsweek and more.

Early Warning is specialised in mobile payment technology. Founded 25 years ago by Wachovia, JPMorgan Chase, Bank of America, BB&T Corporation and Wells Fargo, Early Warning is still at the centre of events with the launch of Zelle.

Hervé Robache : *Standards Manager with STET*

Hervé Robache is in charge of Standards and Norms at STET, which he joined soon after it was set up in 2005. With more than 20 years of experience in the field of interbank settlement, Hervé has taken part in the conception and development of STET's CORE clearing platform. He now works at the heart of the Open Banking sector, leading STET's initiative on the subject of PSD2 APIs and coordinating work with other European projects (such as the Berlin Group and Open Banking UK), as well as taking part in work led by ISO to standardise ISO 20022 for APIs.

STET, founded by 6 French banking groups is a major player in multi- instrument payment processing (card payment, transfers, withdrawals, instant payment, payment by cheque, etc.) in the European market. Its main work covers national clearing for domestic retail payment operations, in both France and Belgium, as well as instant routing for card authorisation requests, via its dedicated e-rsb network.

About DS Avocats

Set up in Paris in 1972, DS Avocats has developed its know-how and put it at the disposal of both businesses and public bodies. This double-faceted public and private culture is both an asset and an emblem of the firm.

DS Avocats currently has more than 400 law professionals spread across 26 offices around the world, who can step in either in an advisory capacity or in litigation.

Amongst its specialities, DS Avocats has become renowned in the field of banking and finance, with its specialist teams for financings as well as on the subject of Fintechs, digital banking and crypto-finance.

The Fintech, Digital Banking and Crypto-Finance unit covers all transactional aspects, including acquisition operations, mergers, cooperation agreements, outsourcing and taxation.

Contacts :

Thibault Verbiest : Partner
+33 6 25 44 12 71
verbiest@dsavocats.com

Frédéric Bellanca : Partner
+33 1 53 64 50 00
bellanca@dsavocats.com

About Galitt

As a reference in the domain of payment systems and electronic transactions, Galitt is the market leader in France in every one of its business sectors, and throughout the world for its testing tools and its expertise in innovative technology.

Galitt is recognised for offering a wide range of skills and complementary knowledge to assist its clients throughout the lifecycle of their projects and in every link of the payment value chain. The company's size allows it to take on large projects while retaining its ability to be reactive, its personal touch and the ambition of an organisation that is run on a human scale.

Galitt is the reference in the execution of the most advanced payment technologies and the definition of tomorrow's technological architecture

Galitt's services are based around 5 Business Units:

- **Payment Consulting** experts and their innovative approaches inform and enlighten our clients' strategic decision-making;
- **Payment Services** consultants help our clients with the execution of their payment projects;
- **Testing Solutions** teams develop testing software and take part in both the industrialisation phase of testing and the certification of solutions;
- **Payment Solutions** associates develop and operate high value-added card and transactional applications;
- **Payment Education** trainers pass on Galitt's expertise and experience during our training seminars.

In 2017, Galitt achieved a turnover of E 31.1 million and employed 260 people

Galitt is a Sopra Steria Group company. To find out more about Galitt, please visit our website, at: www.galitt.com

Contact Galitt Payment Consulting :
Rémi Gitzinger
Executive Director
+33 6 20 66 77 40
r.gitzinger@galitt.com

Background

Entered into force Europe-wide on 13th January 2018, the second Payment Services Directive (PSD2) paves the way for a new notion: open banking. From now on, the right of customers to entirely dispose of their banking data requires banks to make them available to third parties, via application programming interfaces (APIs). Main goal is to stimulate competition and innovation in the banking sector.

This opening up of banking data and the fact of making it available to regulated third parties have raised several questions and controversies in France and across Europe, which this white paper focuses on.

Issues

With PSD2, how can the access rights be organized, and what impacts will there be on the banking ecosystem ?

The first part of this white paper describes the effects of the legal revolution which PSD2 has sparked in terms of the control of banking data on payment and includes three interviews that reflect the implications and strategies for different firms involved. The second part presents the new ecosystem which is arriving across Europe, by describing the operational and technical consequences. Finally, the third part sets out the stakes for the banking sector as a whole, illustrated by market initiatives that already have some significant success.

The white paper summarises the major dates in the future implementation of PSD2. Indeed, in mid-March 2018 the long-awaited Regulatory Technical Standards (RTS) was unveiled. The decree implementing PSD2 which deals with strong authentication and secure exchanges with third parties sets the countdown for on the opening up of payment information systems. As it also dictates new rules for authenticating customers, this text completes the directive - with no transposition required - and leads us into the era of a more collaborative payments economy.

API Economy Glossary

- API (Application Programming Interface): the general, normalised group of classes, methods and functions used in order to organise access to services, resources and data for third-party apps. These interfaces have to be scalable, reusable and secure, all whilst offering simplified use and ease of integration to IT developers;

- **EBA** (European Banking Authority): the independent EU body, in charge of harmonising prudential supervision and technical regulations for the banking sector, while also drawing up RTS and guidelines;

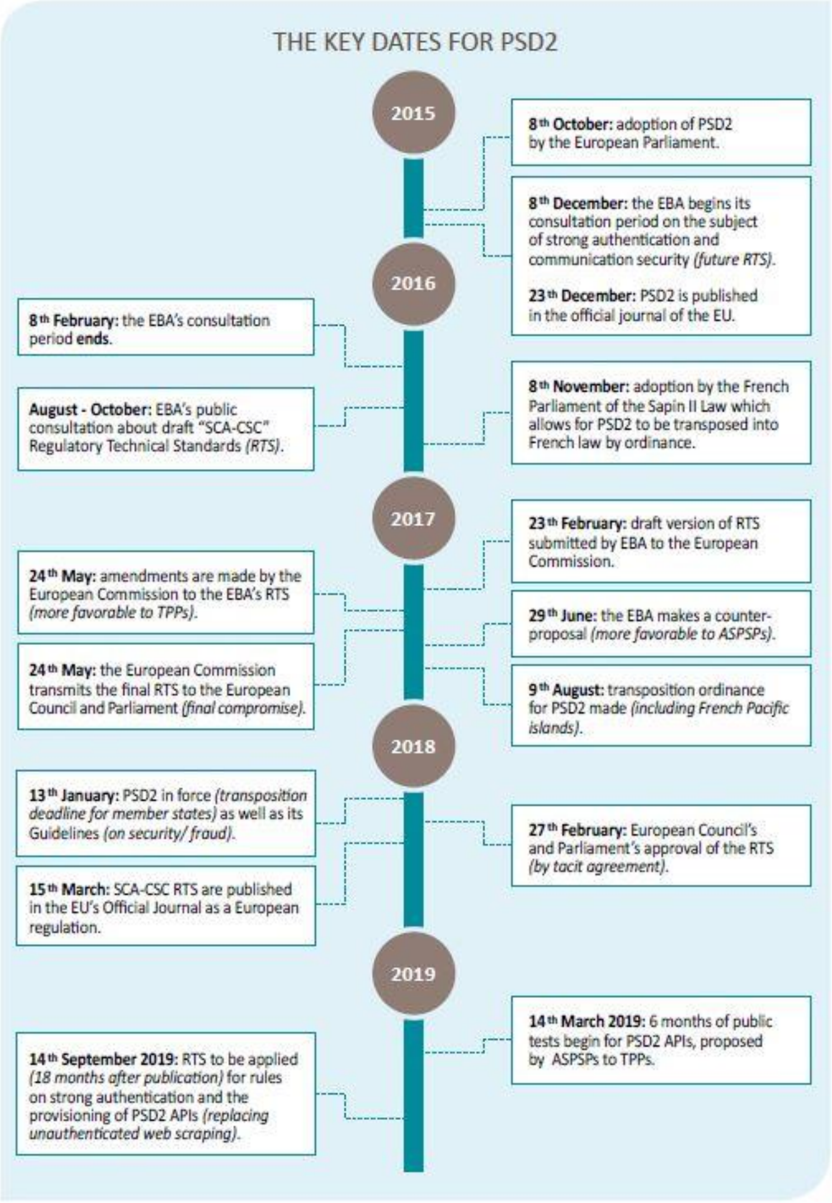
- **Open API**: an API which is made available to third parties outside the firm. This interface organizes access to their data and/or to identified and documented services;

- **Open Banking**: a banking strategy which relies on banking data transparency to provide Open APIs which allow third-party financial firms to enrich both their own offers and those of the bank;

- **Open data**: opening up the data within an internal IT system so that it is freely accessible, useable and reproducible by all with no restriction on ownership, copyright or any other control mechanisms. This allows app developers to offer innovative services, which can even by updated in real time;

- **PSP** (Payment Service Provider): a legal term covering a variety of statuses for financial institutions which are authorised to offer payment services. It brings together credit institutions (banks, consumer credit firms), payment institutions (PIs), electronic money institutions and, now, account information service providers;

- **RTS** (Regulatory Technical Standards): the overall body of technical standards prepared by the European Banking Authority, in collaboration with the ECB (European Central Bank) and the national central banks. Various RTS are included in the directive to harmonise operational implementation. Those which beef up strong authentication and security for exchanges between PSPs were amended by the European Commission on 27th November 2017 (as a delegated act) and published on 13th March 2018.



THE KEY DATES FOR PSD2

2015

8th October: adoption of PSD2 by the European Parliament.

8th December: the EBA begins its consultation period on the subject of strong authentication and communication security *(future RTS)*.

23th December: PSD2 is published in the official journal of the EU.

2016

8th February: the EBA's consultation period **ends**.

August - October: EBA's public consultation about draft "SCA-CSC" Regulatory Technical Standards *(RTS)*.

8th November: adoption by the French Parliament of the Sapin II Law which allows for PSD2 to be transposed into French law by ordinance.

2017

23th February: draft version of RTS submitted by EBA to the European Commission.

24th May: amendments are made by the European Commission to the EBA's RTS *(more favorable to TPPs)*.

24th May: the European Commission transmits the final RTS to the European Council and Parliament *(final compromise)*.

29th June: the EBA makes a counter-proposal *(more favorable to ASPSPs)*.

9th August: transposition ordinance for PSD2 made *(including French Pacific islands)*.

2018

13th January: PSD2 in force *(transposition deadline for member states)* as well as its Guidelines *(on security/ fraud)*.

27th February: European Council's and Parliament's approval of the RTS *(by tacit agreement)*.

15th March: SCA-CSC RTS are published in the EU's Official Journal as a European regulation.

2019

14th March 2019: 6 months of public tests begin for PSD2 APIs, proposed by ASPSPs to TPPs.

14th September 2019: RTS to be applied *(18 months after publication)* for rules on strong authentication and the provisioning of PSD2 APIs *(replacing unauthenticated web scraping)*.

1

A new legal framework to reflect an emerging ecosystem

1.1 The legal framework

1.1.1 Some defintiions set out by PSD2

- **PSU** (Payment Service User) : a private or professional user possessing one or more payment accounts (current accounts) and/or the user of a payment service;

- **ASPSP** (Account Servicing Payment Service Provider): a financial institution within which a customer (PSU) holds one or more accounts and/or within which the PSU initiates payments. Each ASPSP must hold the status of Payment Institution (PI)[1], with potentially the passport that would allow them to operate in different EU countries. Credit institutions, electronic money institutions and payment institutions which already hold status are considered as being ASPSPs;

Clarification - Payment Institution (PI): : these were created following the first Payment Services Directive (PSD) in 2009. Previously, only banks and credit institutions were authorised to provide payment services. With the growth of online payment, new, smaller firms have been able to gain this status so as to bring greater competition to the sector. The status is accorded by the financial authorities of the country in which the request is made; in France, this means the ACPR (Autorité de Contrôle Prudentiel et de Résolution), connected to the French central bank. Gaining and keeping the licence is subject to rigorous procedures in order to provide payment service users with strong guarantees.

- **TPP** (Third Party Provider): a service provider who is able to initiate payments at the request of the payer, without holding the funds and from accounts which the provider does not manage. A TPP can also provide consolidated information concerning these accounts;

This comprises the following three categories of service providers:

- **PISP** (Payment Initiation Service Provider) : a financial institution which offers a service that can initiate a payment order, at the PSU's request, from a bank account which is held by an ASPSP;

[1] *The **ACPR's** definition of a payment institution.*

- **AISP** (Account Information Service Provider): a financial institution which brings an information consolidation service concerning one or more accounts held by a PSU with one or more ASPSPs; ;

- **CBPII** (Card-based Payment Instrument Issuer[2]): a financial institution which issues a card or similar online solution (e.g.: a Wallet or prepaid card), linked to a third-party account which it debits using an ASPSP. The third-party issuer may also request the ASPSP to confirm the availability of the requested amount for each transaction - without reservation or guarantee from the ASPSP, which answers yes or no.

Without doubt, the main innovation that PSD2 brings, and which has raised the longest debate, is the recognition of these three new payment services, enabling a third party to be positioned between a user and his/her ASPSP.

In comparison with ASPSPs, new entrants (TPPs) enjoy lighter operating and prudential requirements. They must however get the mandatory authorization (license) by their regulator, like any payment service provider (NB: account information service providers only need to be declared). They also need similar professional liability insurance in each country where they provide services. Its minimum amount is defined in the EBA's Guidelines published on 7th July 2017.

1.1.2 Right of Access

Articles 65, 66 and 67 of PSD2 set up, firstly a right of access to payment accounts for Payment Initiation Service Providers (PISPs), and secondly, a right of access to the payment account information for both Account Information Service Providers (AISPs) and for Card-Based Payment Instruction Issuers (CBPIIs).

These access rights come with a certain number of guarantees:

1. Access is limited to payment accounts which are accessible online;
2. The explicit consent of the Payment Service User (PSU) is required for any transfer of his/her data;
3. PISPs must not hold the payer's funds;

[2] *Sometimes abbreviated to CISP = Card-Issuing service provider.*

4. Personalised security data (credentials) is not accessible to third parties, and its transmission to both the user and the issuer must be via effective and secure channels;

5. Secure communication is required between the Account Servicing Payment Service Provider (ASPSP), the TPP, the payer and the payee, and must comply with the Regulatory Technical Standards (RTS);

6. PISPs shall preserve data integrity, operations cannot be modified (total amount, beneficiary, etc.);

7. AISPs must only have access to information originating from the designated payment account, and its associated payment operations;

8. PISPs must not store PSU sensitive payment data, which means “data, including personalised security credentials which could potentially be used to commit fraud”. As part of PISP and AISP activities, this excludes the account servicing PSP’s name and the account number;

9. AISPs must not request for transmission of these sensitive payment data related to payment accounts;

10. Only information which is essential to provision payment initiation services or account information services can be requested to the PSU;

11. Use, consultation or storage of data must only be done with the intention of providing either payment initiation services or account information services;

12. ASPSPs must have the ability to refuse to give PISPs and AISPs access to a payment account, for any objective and documented reasons to be addressed to the regulator, in relation with unauthorised or fraudulent access attempt.

These new actors, their service offer and their integration into the payment value chain are described and analysed in the second part of this paper, which focuses as well on the subject of technical repercussions of the sharing of banking data.

PSD2'S TRANSPOSITION: SAVINGS AND CREDIT ACCOUNTS HOTLY DEBATED

On 8th February 2018, the French Parliament ratified the government's transposition ordinance of 9th August 2017 (N° 2017-1252).

During debates in the French Senate, on 22nd March 2018, amendments were made concerning PSD2's initial scope of application, which is restricted to payment accounts, including deposit accounts. Senators proposed to extend authorised access procedures to all payment, savings and credit accounts. They underlined that "Today, 80 % of linked accounts are not payment accounts, but savings accounts, credit accounts or life insurance accounts".

This extension shares the view expressed by German banks, which have been active in pushing for an extensive application of PSD2. As an example, the German bank HypoVereinsbank opened up its customer data to the Fintech MoneyMap. Rather than opposing PSD2's access to data, German banks have preferred to sign agreements with Fintechs aiming to provide new services to the banks' customers.

After negotiations failed between the Parliament's two chambers, the final Act no longer includes the amendment bringing savings and credit accounts in PSD2 scope. The French transposition therefore remains consistent with the European legislation's scope.

1.2 The new ecosystem creted by PSD2

PSD2 aims to regulate the new payment actors, in addition to the ecosystem of payment service providers and banks.

Clarification - Fintech: a portmanteau word combining “finance” and “technology”, these are innovative start-ups which use technology to rethink and offer financial and banking services at lower cost to the end customer. There are several categories of Fintech: crowdfunding, virtual currencies, mobile apps, electronic payments, robo-advisors, etc.

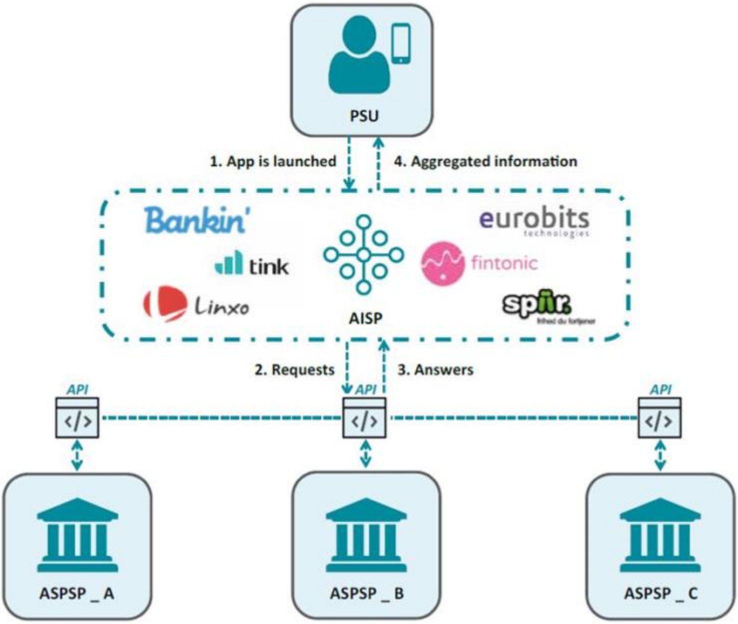
The market position of each of these types of company, and the functions they carry out in the value chain of payments is outlined below.

1.2.1 The role of AISPs (Account Information Service Providers)

AISPs can offer their customers (PSUs) the opportunity to aggregate their various accounts held by different institutions (ASPSPs), within a single app which can provide a consolidated view of their data.

The aggregation service is defined by the directive as follows: After receiving the PSU consent, the aggregator connects to the ASPSPs which hold the customer (PSU) data, via a dedicated interface.

HOW AN AISP WILL OPERATE AS SPELLED OUT IN PSD2



After collecting the account information from each ASPSP, the app analyses the data received and passes it on via a user-friendly interface that can present an aggregated overview of all the accounts.

Two aggregators currently dominate the market in France, Linxo and Bankin'. The former was set up in 2010, currently has 900,000 users and is the market challenger to the latter. Bankin', is a Parisian Fintech which can claim 1.3 million users spread across four European countries. Another start-up which has made a name for itself in France is Fiduceo, which was bought out in 2015 by Boursorama, the online banking subsidiary of Société Générale.

Around Europe, other aggregators have grown strongly in size. The most notable are Tink in Sweden, Spiir in Denmark and Fintonic and Eurobits in Spain, which have several hundred thousand users each.

In order to stand out from the crowd, these platforms have developed other added-value services such as personal financial management (analysing expenditure or financial coaching), or even document management (bills, expenses claims, etc.). Customers are at the heart of these companies' strategies, with the aim of making their user experience as smooth and simple as possible via innovative and intuitive services.

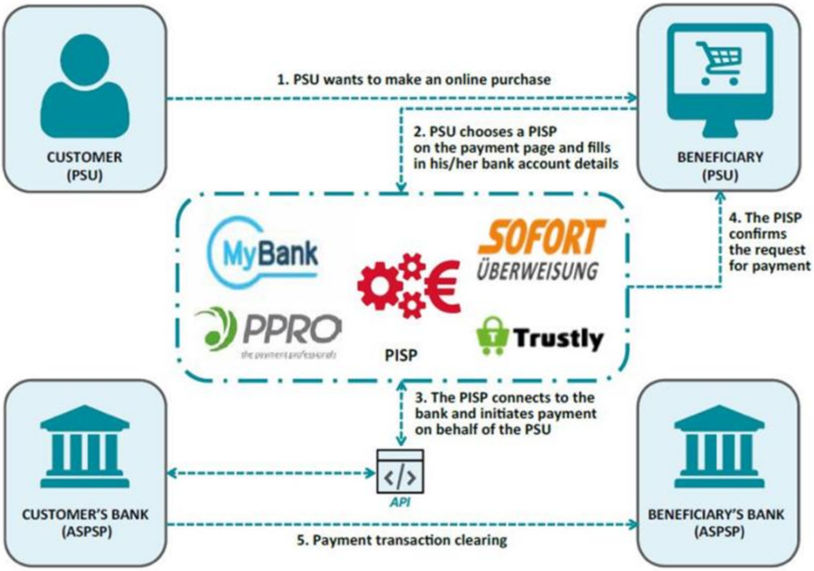
1.2.2 The role of PISPs (Payment Initiation Service Providers)

Those companies which initiate payment transactions are particularly working in the field of e-commerce. Now, an e-merchant can broaden his/her payment portfolio by integrating these third-party companies alongside the big payment networks: CB / Visa / Mastercard / American Express or PayPal. When paying, a customer (PSU) could then choose to use a PISP to pay. The service claims to be simple, with no need for pre-registration prior to the transaction. The PSU will simply need to give authorisation for the PISP to have access to his/her account, by entering his/her online banking connection ID. This procedure, laid out by PSD2, will enable payment to be completed via transfer or withdrawal to the benefit of the e-merchant.

PISP's offers are mostly targeted at countries where the use of payment cards is less widespread. PISPs therefore have a well-established position in Northern Europe, particularly in Germany with Sofort (a company from the Swedish Klarna group), and in Sweden with Trustly.
Just as with the aggregators, these apps can be paired with other functions in order to offer more elaborate services.

Trustly can thus offer its customers a view of the balance in all their different accounts (savings or current) and enable them to choose which one to use for each payment. Its service today supports all the Swedish, Danish, Finnish and Spanish banks. Trustly is currently enlarging its network amongst games platforms and marketplaces, and also with money transfer services.

HOW A PISP WILL OPERATE, AS SPELLED OUT IN PSD2
(for payments made by transfer)


CUSTOMER
(PSU)
1. PSU wants to make an online purchase
BENEFICIARY
(PSU)
2. PSU chooses a PISP on the payment page and fills in his/her bank account details
4. The PISP confirms the request for payment
MyBank
SOFORT ÜBERWEISUNG
PPRO
the payment professionals
PISP
Trustly
3. The PISP connects to the bank and initiates payment on behalf of the PSU
API
CUSTOMER'S BANK
(ASPSP)
BENEFICIARY'S BANK
(ASPSP)
5. Payment transaction clearing

Ever since Sofort was set up in Germany in 2005, and the impact which its new online transfer service had, the European payments market has been in an unprecedented state.

In Germany the banks, finding themselves unable to prevent Sofort from connecting to their interfaces, decided to go to the regulators to contest the legitimacy of this opening up of their interfaces, claiming that complete access to their customers' accounts was a risk.

At a European level, within the framework of the establishment of the Single European Payment Area (SEPA), this new firm was seen by legislators, particularly the European Commission, as an innovator which could stimulate competition in the payment services sector with its efficient and low-cost offer.

With PSD2, the European Commission has therefore decided to favour this new type of innovative, or disruptive, company. The Commission has greatly liberalised the regulatory framework, while still securing data exchanges between TPPs and account servicing PSPs via new standards and communication protocols.

Several of these TPPs already operates, alongside Sofort. Therefore, this paper explains their current modus operandi, known as “web scraping”, as well as the methods which will necessarily replace it: the Open APIs required by PSD2.

1.2.3 The role of CBPIIs (Card-based Payment Instrument Issuers)

Above and beyond officialising these two new payment services, PSD2 will now allow PISPs and issuers of payment instruments linked to payment accounts to directly connect to ASPSPs. In real time, they will obtain confirmation that the sum of the transaction is available in the account linked to (and debited by) the payment instrument. In its Report on the Setting-Up of RTS, the EBA also authorised this service from PISPs.

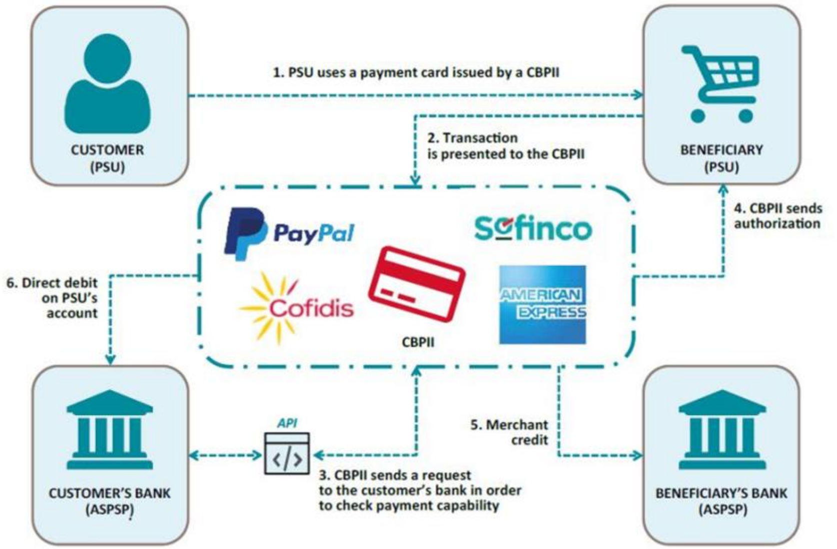
Card-Based Payment Instrument Issuers (CBPIIs) can take advantage of this new fund confirmation service, whether it issues consumer credit cards, rechargeable pre-paid accounts or deferred debit cards similar to T&E (Travel and Entertainment). In practice, it involves an account for which the outstanding amount of transactions is periodically settled by debiting a current account held by an ASPSP. For every payment made with a card from a CBPII, the latter can, after the event, withdraw funds from the PSU’s current account. The details of the account are given to the TPP upon registration (with an IBAN), on the strength of a direct debit mandate (SDD).

These firms have existed for years in the payment card market. International companies, such as American Express or PayPal, or French companies like Cofidis or Sofinco will be able to take on this role of CBPII.

The new fund confirmation service for third-party issuers, as set out in PSD2, allows CBPIIs to make sure that, at the moment of a transaction, the funds really are available in the ASPSP-held account, by contacting the latter directly. Therefore, these issuers will have more information: data which could be helpful for example in managing non-payments and fraud.
On the other hand, checking the money is there isn’t the same as reserving the funds. If the funds are available at the moment of the transaction, nothing guarantees that they will still be so when it comes to settlement. This new service

is only for information to help strengthen risk management amongst CBPIIs. They still retain the right to authorise a transaction or not.

HOW THE FUND CONFIRMATION WILL OPERATE FOR A CBPII, AS SPELLED OUT IN PSD2


CUSTOMER (PSU)
1. PSU uses a payment card issued by a CBPII
BENEFICIARY (PSU)
2. Transaction is presented to the CBPII
4. CBPII sends authorization
PayPal
Sofinco
Cofidis
AMERICAN EXPRESS
CBPII
6. Direct debit on PSU's account
CUSTOMER'S BANK (ASPSP)
API
3. CBPII sends a request to the customer's bank in order to check payment capability
5. Merchant credit
BENEFICIARY'S BANK (ASPSP)

1.2.4 Combined payment services for an improved cutosmer experience

Some TPPs already offer a combination of these new payment services, aiming to provide added-value services to PSUs.

Indeed, many institutions - whether it be high-street banks (Société Générale), online banks, (Boursorama), or TPPs (Bankin', Linxo) - have been offering, since 2017 and in addition to the aggregated consultation of the PSU's accounts, the ability to initiate transfers from other accounts from within the app or the customer area. The users can now thoroughly manage their accounts without needing to connect to them individually. After consulting, via aggregation, the PSU can, if he/she needs to balance them up, transfer an amount via the payment initiation service.

In practice, methods differ from institution to institution: some only offer the chance to carry out internal transfers between accounts whereas others also permit external transfers (as long as the account details of the beneficiary have already been validated with the online bank of the account giving the order).

Taking the frictionless customer experience a step further involves offering individual customers an automated cash management service: as aggregation gives you an overview of all the customer’s accounts, then configuring payment initia- tion allows you to optimise the funds available between those accounts. This feature could be triggered according to criteria set by the customer, for example:

- By automatically transferring to a savings account as large an amount as possible, depending on the funds available, at the end of the month;

- Or, in order to avoid going into the red, setting up a transfer from a positive account once a threshold (set by the user) is reached in the main account.

This cash management service stems from the opportunities created by PSD2. It is just as relevant for businesses, particularly smaller businesses which, up until now, haven’t benefitted from the type of cash-pooling service that most banks reserve for their larger customers.

2

Key battleground: securing and standardising exchanges within the new ecosystem

2.1 Web scraping as a data recovery technique

2.1.1 A technique currently used by TPPs…

Most AISPs and some PISPs use a technique known as “web scraping” or “web harvesting” in order to be able to function. This technique is a way of extracting content from a website, via a script or a program which reads the html code, with the aim of transforming it, and being able to use it in a different context. It is a technique much used by, for example, price comparison websites (trivago.fr, liligo.com, etc.).

In our example, a TPP, will ask its customer (PSU) for his/her connection ID to his/her ASPSP. It will then put this data into a program which acts like a robot, simulating the action of connecting in the customer’s place. It can then harvest from the relevant page all the information it needs to operate, whether it be a one-off situation (payment initiation) or regularly (account information).

2.1.2 …But which poses a few problems

- **For ASPSP**: having a robot continually passing over your Internet page can slow the page down. If there are many simultaneous connections, this method can lead to what is called a “denial of service attack” (“DoS” - there are so many requests made at the same time that the server can’t handle them all, leading to it crashing);

- **For TPP**: this method requires them to have as many robots as there are ASPSPs, seeing as the different sites are not standardised, which leads to a very long programming time. The robots can also become obsolete overnight if an ASPSP decides to update or modify its page;

- **For the PSU**: when giving consent to a TPP, the PSU is giving access to all the information contained in his/her online bank account. Although the new services which are offered are legitimate, and the PSPs guarantee data confidentiality, they are nevertheless now capable of harvesting all the information in the customer account; balance, transfers, withdrawals and the metadata associated with it (place, date, time, business, amount, rentpayments, refunds, loans, telephoneoperators, insurance, salary, medical insurance, consumer habits, etc.);
- **For all three parties**: the major problem with web scraping lies in the shared liability and the principle of proof. Let’s take the example of a case of fraud, in which a transfer has been initiated from the account of a PSU without his/her knowledge. As much as the PSU gave his/her online banking credentials to a TPP, it can be difficult to work out the chain of liability: does it reside with the PSU, the TPP or the ASPSP?

LE REGIME DE LA RESPONSABILITE DE LA DSP2

One of the stumbling blocks for PSD2 concerned the designation of liability between the various firms involved in each step of the payment chain.
Articles 73 and 90 have established rules of responsibility for Account Servicing Payment Service Providers (ASPSPs) to their users, in case of unauthorised, uncompleted or badly-completed payment operations, even though the payment operation is initiated by the Payment Initiation Service Provider (PISP). Furthermore, article 74 protects the giver of the order from all financial responsibility, placing it upon the financial institution if the latter hasn't carried out Strong Customer Authentication.

PSD2 includes, however, a number of guarantees:

1. an assumption of liability on the part of the PISP (who must prove to the ASPSP that the fault or the problem doesn't stem from itself);
2. a first demand guarantee of reimbursement for ASPSPs against PISPs;
3. the right of ASPSPs to verify, in advance, that a PISP is satisfying the conditions laid down by PSD2;
4. and the transfer of the obligation to refund the user onto any PISP which is found to not be satisfying the conditions laid down by PSD2.

Nevertheless, the directive doesn't require a contract to be signed between the two parties: a PISP may access an account simply thanks to the existence of PSD2.

Under pressure from the major high-street banks, the French Central Bank restated in Spring 2018 that liability for strong authentication lies with the ASPSP, as the payer's institution. It is therefore the ASPSP which may set the methods and frequency. This check should still guarantee a smooth user experience for the customer (PSU) without creating obstacles for the TPP's own user experience[3].

2.2 Final RTS : defining competition and security

The initial draft RTS, submitted in February 2017 by the EBA under article 97 of PSD2, was amended by the European Commission on 24th May that year, to be more favourable to TPPs. Following the EBA's counter-proposals, at the end of June 2017, and a long search for a compromise, the Commission proposed the final version of RTS to the European Council and Parliament. There being no

[3] *Defined, by the French Central Bank, as not imposing more than 5 steps upon the PSU outside of the TPP's own environment.*

objections, the RTS were published in the EU's Official Journal on 13th March 2018 as a European Regulation (see also PSD2's key dates).
Although they are directly applicable, the RTS will be subject to further clarification in France, as an applicative decree is envisaged to ratify PSD2's transposition. It will concern the methods of exchanges between ASPSPs and TPPs.

2.2.1 Authorising TPPs to be payment service providers

The first condition of accessing accounts is the requirement for all AISPs and PISPs to obtain the status of payment institutions (at least) with the relevant national authorities, which will study the reliability of the services offered. The authorisation procedure is standard for PISPs but lightened for AISPs (a declaration with tacit agreement). In France, the regulator remains the ACPR (Prudential Supervision and Resolution Authority) overseen by the French Central Bank.

2.2.2 The use of certificates that comply withe IDAS regulation[4]

European eIDAS (electronic IDentification And trust Services) regulation from 1st July 2016 aim "to create a climate of trust in the online environment" by providing a full, cross-sector, European framework for secure, simple and reliable electronic transactions between citizens and businesses.

To access accounts, the use of eIDAS certificates can authenticate ASPSPs, AISPs and PISPs. They will come from the recognised certifying authorities, which will guarantee the authenticity of each institution's legitimacy, and its role (AISP, PISP, ASPSP, issuer of a payment instrument linked to a card/ CBPII).

2.2.3 Strong Customer Authentification

PSD2 requires adherence to the principle of strong customer authentication in every payment situation where the risk of fraud exists, and particularly for access to online payment accounts and electronic payment transactions.

This strong authentication necessitates at least two factors, from the following list of categories:

[4] *The ANSSI's presentation of eIDAS regulation.*

- **What the customer knows** (e.g. a PIN code or private information);

- **Who the PSU is** (e.g. a biometric factor such as fingerprints);

- **What the PSU owns** (e.g. a secure payment card, telephone number or email address to receive the order, or an address to receive mail).

In addition, each strong authentication generates data unique to the transaction, which is carried through to the end of the process: the "authentication code"[5].

With these two demands, authentication is carried out by the ASPSP, which is liable. Before any operation, it must verify the authenticity and the role of the TPP. Never- theless, it mustn't systematically check for customer consent. Therefore, it needs to set up, via its APIs, a customer security policy (following SCA criteria) which doesn't discriminate - that is, which doesn't create obstacles for any TPP's activities.

In addition, the TPP must have the right to use the ASPSP's authentication procedures via its API, should the TPP wish to.

The final RTS establish 9 (voluntary) cases which are exempt from strong authentication. Amongst the possible situations for a TPP using an API[6], let's look at two examples.

- L'exemption en cas de consultation des informations sur les comptes s'applique Exemption for consulting account information applies:
  - if it is not the first connection to the ASPSP's services via this TPP, and if the connection is carried out less than 90 days after the previous authenticated connection;

  - if the information service is limited to data defined as non-sensitive (name, account number and statement of account transactions within the last 90 days[7]);

[5] *This "authentication code" stemming from the authentication will differ from any code used to authenticate, as one of the required factors. It is a code carried through the*

[6] *Other exemptions are summarised in the appendix. In all cases, only the payer's institution can decide to use one or other of the applicable exemptions.*

[7] *The ASPSP must set up a 90-day clock for each district access made by the same customer (direct, via 1 AISP, via a different AISP, etc.) without accounting for different access channels (mobile, Web or other).*

- Exemption for distance payments of small amounts applies to transactions of under E 30, as long as the cumulative total since the last strong authentication doesn't exceed:
    - either E 100;
    - or a total of 5 transactions (the choice between these two options can be made by the payer's institution);
- Exemption on behalf of trusted beneficiaries applies to all payments for which the receiver has previously registered by the customer with the ASPSP, using SCA. The French Central Bank has decided that PISPs will have write access to this list.

2.2.4 New standards and open protocols for secure communication

ASPSP's must make a dedicated interface available to TPPs in order to securely communicate data and resources needed to supply the CBPII, PISP and AISP payment services[8]. The EBA has left the technical implementation of this up to the firms involved, but has imposed the following conditions:

- There must be the same functions as with direct access by the customer (that is, via their online banking) with the same availability and level of performance;
- There must be a guarantee of secure data exchange, via open and universal communication standards, such as for completely automated financial messages under ISO 20022[9];
- There must not be the unaccompanied use of generic Internet standards such as HTTP, HTTPS, TLS and SSL which don't provide the necessary security guarantees for the exchange of financial data.

[8] *See articles 97(5), 65(2)c, 66(3)b and 67(2)b of PSD2.*

[9] *ISO 20022: Universal financial industry message scheme, an ISO standard for electronic data interchange between financial institutions.*

2.3 APIs as an answer to the challenge of secure and standardised data exchanges

2.3.1 The principle of APIs

The idea of APIs had largely emerged even before PSD2. Even though neither the text of the directive nor the RTS mention the notion of APIs as such, and the EBA merely gives a list of technical requirements, APIs appear to be the most suitable solution, when taking all of those requirements, listed above, into account.

INTERVIEW

Sébastien Taveau - Chief Developer with Early Warning

In order to shine a light onto the ideas of APIs and Open APIs, we spoke to Sébastien Taveau, Technologist with Early Warning.

Galitt : could you define what the term “API” means for you?

Sébastien Taveau: an API is a structured means to open a service or some data to third parties via an easily-controllable and secure gateway. In essence, it is no more or less than a logic of questions and answers.

Thus, in the example of a data aggregator (AISP), he will send a request from his application, asking to recover defined data. This request will be handled via the gateway - the API - which will ask the relevant part of the ASPSP in order to get hold of the information. The data will pass via the gateway to the AISPs application, which will compile it (see graphic p.15).

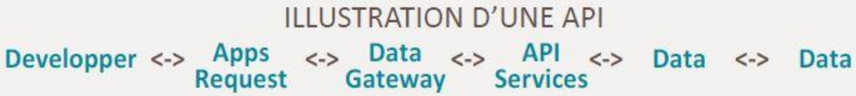


ILLUSTRATION D’UNE API

Developper <-> Apps Request <-> Data Gateway <-> API Services <-> Data <-> Data

Sébastien Taveau : there are several types of API, of which the main ones are:

- **Private APIs:** this is a 1:1 integration. In this case, the API has been conceived with a specific partner in mind and is usable only by them. Private APIs are very generally used for sharing sensitive data, which can pose dangers for those involved (black lists, personal data, etc.);

- **Public APIs**: these are the most widespread APIs, and don’t pose any particular concerns. We could give the example of Google Maps’ API or that of Twitter’s news feeds. Registration is encouraged but not necessary ;

- **Open APIs** : these are conceived for a wider public than Private APIs. They require a TPP to accept the terms and conditions of use and necessitate a guarantee and security procedure via the authentication enrolment called "OAuth". Registration is required for this service. Within the framework set out by PSD2, Open APIs are the ones which best correspond to the need to use dedicated interfaces, as Open APIs allow an ASPSP to verify the users which connect to their service wanting to recover data.

Another important element to take note of is that some APIs can generate revenue, whereas others don't bring high added value (used for broadcasting free media content or as an eye-catching service, but without any particular economic outlook).
For example, Public APIs are not aimed at turning a profit, but it is important to mention the maintenance costs and the data input, as all types of API have a significant financial impact. The business model lies in the large-scale use of APIs, or the cross-pollination with other APIs, or via the underlying paid services that come with the use of an API. It's possible to bring together several different functions, depending on the mapping capacity of the APIs.

Galitt : what advantages can Open APIs bring?

Sébastien Taveau : APIs, and particularly Open APIs, offer a lot of flexibility as they allow you to keep a layer of security, while forcing the administrator to think about what uses might be required by third parties. I often compare an Open API to an object inside a box made of toughened glass: you can see it, you can shake the box, but you can't touch it.
As we have seen, an API is a group of predefined calls which access a service via a gateway. The gateway is the critical point, in terms of security, as the third-party PSP will, via the API, directly connect to the ASPSP's information system. Technically, it is easy to build into the system a way of locking down the communication if a problem is detected.

Moreover, with an Open API, the OAuth authentication is mandatory, which further reduces the risk. OAuth is not an authentication protocol, but a protocol to delegate authorisation, so it can authorise an application

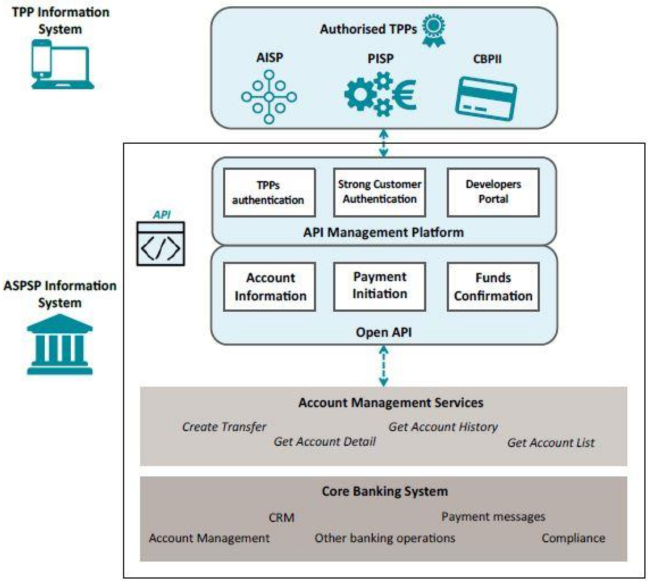
to use a secure API on behalf of a user. This represents an added layer of security, on top of that brought by the strong authentication.

Once again, the analogy of the object behind toughened glass is very striking. In addition, the reply provided by the API is the only information that the TPP can receive, which is essential.

To summarise this section, we can see that the directive will completely revolutionise relationships between companies, both legally and technically.

The biggest impact of these innovations today will be felt by the banks themselves. In the next section we will analyse the different possibilities on offer at the moment, and the noticeable initiatives.

OPEN BANKING APIs ARE AIMED AT HELPING TO FACILITATE INTERFACES BETWEEN ASPSPs AND TPPs
(Interface architecture for Open Banking APIs)

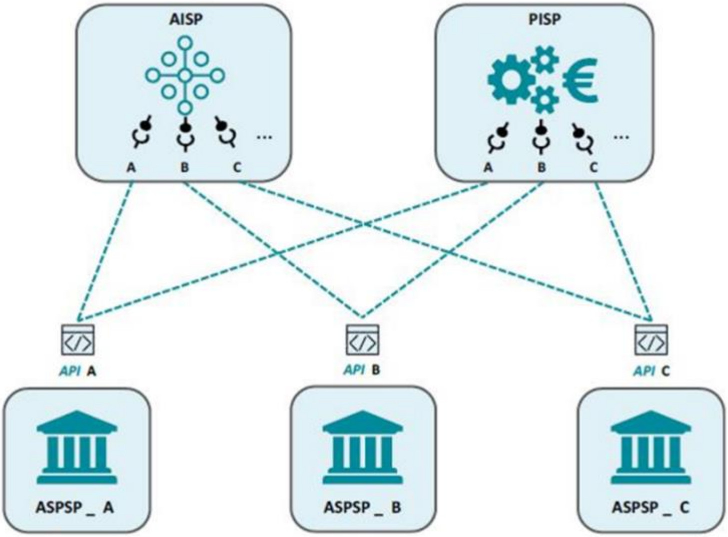


2.3.2 Standardising APIs, essential for a disruptive model

Standardisation is a fundamental part of the deployment of a disruptive model. For it to work, the TPP must be able to connect via a secure interface, essentially an API provided by the ASPSP, and recover the information it needs.

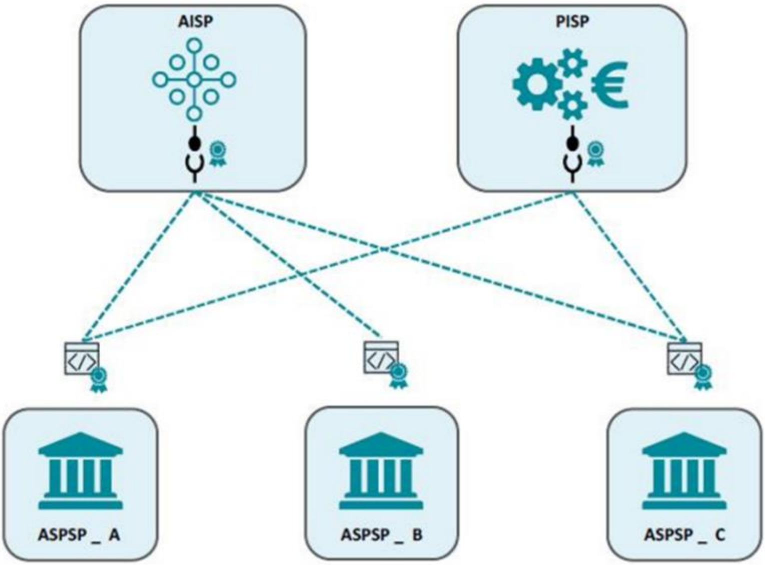
The diagram below shows how APIs are set up by ASPSPs on behalf of TPPs.

DIFFERENT APIS FOR EACH ASPSP



The diagram shows that in order to connect to bank A, the TPPs (AISPs or PISPs) have to identify the technical means to allow their apps to connect to the particular bank's API and to interpret the data received. This development operation has to be repeated for each different ASPSP. The TPPs therefore need to be able to handle the technical complexities stemming from a great variety of API programming and tiered data.

ILLUSTRATION OF A UNIVERSAL API



In this diagram the TPPs and the ASPSPs use the same communication standards. Thus, each API is identical and only one type of program is needed. Standardisation makes inter-company relations easier. Looking further ahead, the project aims to clear the way for Open Banking. Banks will become a modular platform upon which firms can interact via the API.

This principle of bank-as-platform is outlined in the case study of SolarisBank on the following page.

SOLARISBANK, THE BANK OF TOMORROW ?

SolarisBank was founded in 2015 by the German financial group FinLeap. It claims to be the first 100 % digital bank and received its banking licence from the German financial regulator, BAfin, in just nine months.

Targeting its strategy at young businesses, SolarisBank operates a B2B2C business model which is typical of Open Banking. It offers a white-label platform by which banking services can be provided “à la carte” by whichever Fintechs want to work with it. Customers can then interact directly to create the banking environment they prefer by choosing the apps they want.

Thus, the bank acts as a modular toolkit via its API. Available services include account holding, retail payment, credit cards, credit issuance in real-time and trusted third-party. With its latest round of fund-raising in March 2018, Solaris brought Visa, BBVA and ABN Amro into its capital. Having gained 60 business customers, it is now targeting 100 by the end of 2018.

“Our services are like Lego bricks: our partners can choose the bricks that they want and assemble personalised solutions with them to meet their own needs. Partners can get access to the Solaris Platform services through our API. Integration is simple and allows users to concentrate on their own roles. In addition, our services are secure and guarantee the confidentiality of our user data.”

Andreas Bittner: Founder and Board member, SolarisBank[10]

[10] *SolarisBank: Presentation of the company.*

In short, a firm can use this white-label platform in order to create its own bank. SolarisBank retains the key banking functions, such as customer database, card issuing, bank account management, compliance, risk management etc. Nevertheless, it brings in different companies for the implementation of each step.

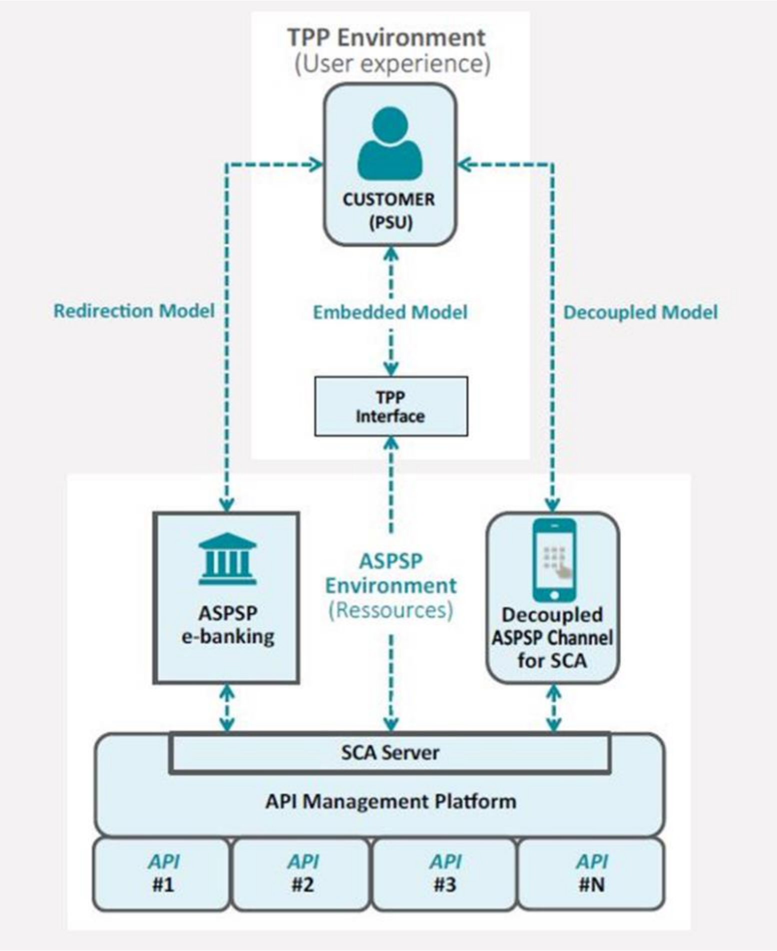
In this bank-as-platform model, the banks position themselves at the centre of a new economy in which APIs are a source of income and allow the banks to meet the various needs of their customers more efficiently.

SolarisBank is not the first company to offer this type of model. The pioneer in this field is Fidor Bank, recently acquired by the BPCE group.

The obvious interest of standardising has equally led to several initiatives throughout Europe which aim to pool and harmonise a foundation of PSD2 APIs. A crucial point for each specification of API defined in these initiatives concerns how to set up strong customer (PSU) authentication.

MODELES DE MISE EN ŒUVRE DE L'AUTHENTIFICATION FORTE

Customer authentication is a specific constraint imposed by PSD2's RTS for strong authentication and standards for open, common and secure communication. Three approaches or customers paths are envisaged.



STET

STET is the operator for the Clearing and Settlement Mechanism (CSM) in France, and therefore a major player in handling retail payments in Europe.

Mandated by its shareholders (La Banque Postale, BNP Paribas, BPCE, Crédit Agricole group, Crédit Mutuel-CIC, Société Générale, CB Investments), in July 2017, STET published a first draft of API specifications for PSD2-compliance of its members.

Nevertheless, the final version of RTS, adopted by the European Commission at the end of November 2017, called the specifications into question as article 32.3 of the RTS forbids ASPSPs from imposing its own authentication interface on TPPs for identifying their customers.

This redirection model, which was systematic in STET's initial version, has since evolved into a multiple approach using 3 models which allows TPPs to control the process of authenticating a PSU. This update (version 1.3) was published on 10th April 2018[11].

[11] *Depuis, à la demande du régulateur, la spécification STET devra s'enrichir, dans une version prévue en septembre. Principales évolutions : accès à tous les types de virements disponibles en banque à distance (récurrents, multiples, différés), avec leur option d'annulation ; accès des AISP à l'encours d'opérations carte à débit différé ; accès des AISP en lecture seule aux listes de bénéficiaires de confiance, et en écriture seule pour les PISP, avec vérification de la présence d'un bénéficiaire (cette évolution a été transmise pour avis à l'EBA).*

INTERVIEW

Hervé Robache - Standards Manager with STET

In April 2018 STET published version 1.3 of the French "PSD2 API" specifications, which was an opportunity to talk to Hervé Robache, Standards Manager with STET, in charge of the project.

Galitt: who are the stakeholders in this project for standardising PSD2 APIs?

Hervé Robache: beyond STET's own shareholders[12], the French Central Bank, the French Deposits and Consignments Fund (CDC) Crédit Mutuel Arkéa and HSBC France. Working groups have also been conducted with the OCBF (Financial and Banking Coordination Office) and with Luxembourg banks such as BNL or Raiffeisen Luxembourg.

We are also in close contact with other PSD2 API-standardising initiatives across Europe.

Galitt: how are your relations with these other initiatives?

Hervé Robache: convergence work with the Berlin Group was initiated after our shareholders requested it: the first results of this work were included in STET's April update for PSD2 APIs and will also be in the Berlin Group's forthcoming update.

Contacts have also been made with British and Polish standards. In the case of UK Open Banking, there have been several meetings, even though the British project is a different beast, due to Brexit, but also to the fact it has a wider and more prescriptive scope than PSD2's. As for the Polish initiative, a first contact was made in the Spring. However, so far there has been nothing with Slovakia or the Czech Republic.

[12] *See more § "Standardisation of APIs" (as a reminder: La Banque Postale, BNP Paribas, BPCE, Crédit Agricole group, Crédit Mutuel-CIC, Société Générale, CB Investments).*

This convergence work has been welcomed by the European authorities, as well as by business representatives and consumer groups.

Galitt: briefly, what are the principle modifications in the new version of STET's PSD2 APIs?

Hervé Robache: the final version of RTS adopted by the European Commission led us to propose two new strong customer authentication approaches per ASPSP, which match those proposed by the Berlin Group. In particular, the "Embedded approach" allows a TPP to enter a PSU's ID and the necessary strong authentication factor within its own user environment, in order to transmit them to the ASPSP. On this point, STET's specifications warn against using a static password so as to avoid any risk of replay attacks using the authentication elements.

Another structural change is in managing PSU consent to give access to his or her various accounts, which can now be proposed by the ASPSP as well as by the TPP.

Many other suggestions, particularly from the banks, from TPPs, from processors and from the work carried out with the SWIFT working group - in charge of ISO 20022 standards - have been taken into account.

Naturally, the results of our convergence work alongside the Berlin Group are also included (see below).

Galitt: what are the first results of the convergence work with the Berlin Group? And, in contrast, are there any sticking points?

Hervé Robache: we are working together on two areas of convergence: security and technical convergence.

In terms of security, a breakthrough was the adoption, as we have seen, of the three approaches to strong authentication (redirection, decoupling and embedding). These three approaches differ particularly in how they manage rights of access - our specifications are based on the standard OAuth 2.0 protocol, whereas the Berlin Group only use this protocol on an optional basis, alongside another specifically designed protocol.

As far as technical aspects are concerned, the gap between STET and the Berlin Group varies depending on the type of service that the TPP operates. For AISPs, structures and formats are almost 100% identical. For PISPs however, there is significant divergence: there is more input data with STET; by contrast, the Berlin Group distinguishes between 5 "payment products" (due to the specifics of the various domestic markets represented within the Group). Inbetween lies the "fund confirmation" API, for which the defined methods are similar, but the data structure still differs.

We're talking about signposting name tags for structures of data blocks exchanged (requests, results). Indeed, our JSON formatting was used to following the ISO 20022 methodology used for SEPA messages as much as possible. A few divergences remain there with the Berlin Group. For example, in STET's specifications, the PSU is identified as a debtor in the body of the payment request (equivalent to the "debtor" which is within the ISO 20022 SEPA messages), whereas the same information is found in the HTTP header in the Berlin Group's specifications.

Galitt: what are the next steps for STET, before we see your API specifications adopted by account servicing PSPs?

Hervé Robache: we are continuing our convergence work with the Berlin Group with the aim of publishing a unified API in 2019.

Meanwhile, the STET API has also been studied by the European API Evaluation Group. Assisted by 30 industry experts, split into dedicated sub-groups for each API project, this body works for the EBA (see insert 7) proposing methods to evaluate the compliance of PSD2 APIs with the RTS. For the time being, eight initial criteria have been defined, which STET's specifications adhere to, it would appear. These recommendations, aimed at regulators, are particularly concerned with exemptions for fallback solutions, but will remain non-binding for the regulators. In France, the regulator will work with a national forum of banks and TPPs.

Berlin Group

Since 2006, the Berlin Group[13] has been proposing standards for exchanges between European payment systems, developed by the main European card industry stakeholders (primarily card systems and major processors).

In 2017 the Group entered the field of PSD2 access-to-account with its NextGenPSD2 project. With 43 payment players, it aims to establish a pan-European standard.

Published on 8 th February 2018, its API specifications detail access-to-account (XS2A) by TPPs (PISP, AISPs and CBPIIs) for all three core PSD2 services (payment initiation, account information, checking fund availability) while still supporting additional services which ASPSPs could offer via this interface.

Where the Berlin Group's approach is original is how it offers three options for identifying the customer (PSU), according to the RTS rules on SCA. Each ASPSP has to indicate to the TPP the method or methods used in the development of the APIs that it is putting at their disposal:

- A redirection model, where the TPP redirects the PSU to the ASPSP e-banking interface in order to be identified;
- A decoupled model, where strong authentication is carried out by a separate channel (for example the ASPSP's mobile app or a third-party instrument[14]) which is still controlled by the ASPSP. (This is therefore a variant of the redirection model);
- An embedded model, where the TPP's own interface initiates identification of the PSU, receives from the PSU' the banking authentication factors, transfers them - and is responsible for them - and receives confirmation of the success or failure of the process.

[13] *Within STET's PIS API specifications, the simplified payment interface offers just one payment product. A possible convergence path could be to add it alongside the 5 envisaged by the Berlin Group.*

[14] *For example, a hardware token, or a single-use password generator.*

Open Banking UK : a precursor

The UK tackled the subject of open APIs several years ago. In 2015, the British government, in order to stimulate competition and encourage new firms to enter the market, put forward the rising need to share more data between banks, Fintechs and their common corporate customers.

Thus, in September 2015, even before PSD2, the Treasury Department decided to set up the Open Banking Working Group. This working group brought together banks, other businesses in the sector, consumer associations and research institutes, and published "Open Banking Standard"[15], a standardisation guide for formatting, sharing and using data within the banking industry.

Following this work, the Open Banking Implementation Entity (OBIE) was set up in 2016 by the Competition and Markets Authority (CMA), which manages the Entity. The OBIE, financed by the country's 9 major banks[16] aims to roll out Open Banking across the UK. In July 2017, it published API specifications to provide a standard for the minimum service of British Open Banking.

3 primary API specifications were formalised by the OBIE and completed by "guidelines":

- API Open data, which enables an institution to offer data about its services and products to third parties, so that the latter can develop its own mobile and/or web apps for customers, based on the published resources;
- API Open Banking Read, which enables an institution to offer access to its PSU's accounts and the statements of the PSU's transactions (provided the PSU has agreed beforehand) to AISPs;
- API Open Banking Write, which enables an institution to allow a PISP to initiate payment from a PSU's account (provided the PSU has agreed beforehand).

Meanwhile, the OBIE oversees the use of these APIs by the 9 banks which committed to setting up their availability on 13th January 2018.

[15] *Open Banking Standard.*

[16] *Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, RBS Group, Santander.*

After a grace period[17], and 3 months of successful tests, the TPPs (authorised by the Financial Services Authority (FCA)), are offering their customers account information services based on the OBIE's specifications since September 2018.

Payment initiation services are still being tested, with delivery dates currently staggered between March and September 2019[18].

Other national common API initiatives

Following the example of the UK and France, Poland, the Czech Republic and Slovakia have also defined the specifications for APIs targeted at their members. The banking associations responsible are the ZBP, CˇBA and SBA respectively.

THE API EVALUATION GROUP

[17] *On 13th January 2018, 6 of the 9 banks couldn't fulfil their commitments: Bank of Ireland, Barclays, HSBC, RBS, Santander and Nationwide. Each negotiated an extension to the deadline, published in the Treasury's official journal.*

[18] *The roadmap for rolling out Open Banking APIs was reviewed by the OBIE in July 2018.*

The API Evaluation Group is an independent body of twenty or more market sector representatives, brought together in January 2018 following the ERPB's work on payment initiation (the PIS Working Group).

Representatives of major stakeholders are present; TPPs, ASPSPs (such as the European Banking Federation, the European Savings Banks Group and the European Association of Cooperative Banks) and PSUs (EuroCommerce, E-commerce Europe and the European Consumer Organisation (BEUC)), as well as a representative of the EMA (E-Money Association) and one from the EPIF (European Payment Institutions Federation).

Its aim is to establish a list of objective compliance criteria for PSD2 and its RTS on the subject of strong authentication and standards for open, common and secure communication, and to study each API project in the light of these criteria.

The criteria will act as a guide, as much for the bodies creating the specifications as for the institutions putting them into practice, and for the relevant national authorities acting as regulators.

INTERVIEW

Clément Cœurdeuil - CEO and co-founder of Budget Insight

To give us an idea of how TPPs are directly affected by the coming interfaces, we spoke to Clément Coeurdeuil, CEO of the aggregator Budget Insight and an expert with the API Evaluation Group, a multi-party group brought together by the EPC at the European Commission’s request.

Galitt: may we get an insight on the criteria to be used to assess APIs’ compliance against PSD2 RTS’ rules?

Clément Cœurdeuil: certainly, insomuch as I am a rapporteur about the last version of STETs API specifications. At the European level, the Commission’s API Evaluation Group hasn’t yet published the final version of its own evaluation criteria.

In France, I presented the conclusions of our analysis to the CNPS (Comité National des Paiements Scripturaux, National Committee on Cashless Payments) during a meeting with the French Central Bank, in which Budget Insight represented TPPs alongside Bankin’ and Linxo. There are 9 requests for changes within it, divided into 14 criteria, which cover the business functions that correspond to the RTS. These requests for change are currently being discussed within the group, and it will present its final decision before the end of the year.

From our point of view, the RTS are clear on the fact that account-holding banks mustn’t control customer (PSU) consent - to be verified by the TPP - nor put any obstacles in the way of the TPP’s activity. Within the STET’s specifications, however - which were established without consultation with TPPs - security concerns, although they are legitimate, appear to be used as a pretext to hinder our connections. According to the rules which apply to TPPs, these security barriers are unfair.

Galitt: what objective examples could you give us?

Clément Cœurdeuil: to begin with, according to our analysis of rules and current usage, the three options for strong customer authentication (SCA) don’t all contain the same level of fluidity or of hindrance in their customer journeys. The Redirect method is much more impactful than the Embedded method. This is particularly true for account information services, with SCA required every 90 days. This adds another obstacle onto the responsibility of securing the service for the customer which TPPs already have to handle. In addition, TPPs are now authorised and controlled by the ACPR in France. They apply PSD2's rules, and will soon apply the RTS, just like banks!

Another example: STET doesn't specify the methods of accessing the list of beneficiarys which the customer has registered in his or her online banking space. This lack of means may lead TPPs to display a poorer business offer in comparison with what customers can do directly on their e-banking service. We have launched the pilot of a P2P service. In partnership with the Lydia prepaid Wallet service, our customers can send funds to a pre-registered beneficiary with an account that we aggregate. Today, web scraping allows us to recover the account's IBAN and the customer can authorise the whole transaction. Soon, this data will not be available via the PSD2 APIs which follow STET's standards.

With these restrictions in mind, the working sub-group's report on STET APIs includes an amended version of STET's specifications, which conforms to RTS in as much as it allows iso-operation between the TPP's services and the online bank.

Galitt: in your opinion, how will the "fallback" solutions, envisaged by the RTS in cases where APIs fail[19] to access accounts, work?

Clément Cœurdeuil: I think that, in an urgent situation where you need to ensure the continuity of service from regulated institutions like ours, you have to be pragmatic. Account servicing PSPs must be able to identify us, therefore we will confirm the IP addresses of our robots, ideally before any incident occurs. In fact, most of them know the

addresses already (if they didn't they would block us)! Afterwards, they can check our authorisation and its role (AISP, PISP etc.). According to law, TPPs have to present their digital certificates only when they use the API itself.

[19] *Except if exempted by the regulator, each account servicing PSP must always be able to allow a TPP to revert to web scraping in an emergency, on condition that the TPP identifies itself to them.*

Galitt: how should APIs be evaluated before and during the initial six-month testing period (note: March to September 2019)?

Clément Cœurdeuil: TPPs are ready to connect to APIs to test them as soon as the documents on connection and use are published by the account servicing PSPs, and as soon as their testing environments are available!

3

A strategic turning point for the banking sector

In France, as in Europe, banking institutions have entered the field of Open Banking with a variety of differing strategies. From open collaboration to acquisition, via monetising services which go beyond the regulatory minimum (consultation and initiation). Relationships with TPPs are overturning the banks' traditional business models.

Amongst these different strategies, two stand out:

- The first consists of using the Fintechs' own ecosystem, via takeovers and partnerships in order to offer innovative services to their customers as quickly as possible, while still keeping control of their public image and customer relations;

- The second, on a more ambitious level, aims to embrace Open Banking by granting third parties access, via APIs, to the banking institution's own products and services.

3.1 Takesovers and equity stakes in Fintechs: the French banks' strategy

This move is in line with the group's declared strategy of "Growing Differently". The aim is clear: strengthen and accentuate the bank's digital transformation. Fidor Bank was set up in Munich in 2009 and was the first totally digital neo-bank.

As with SolarisBank, its strategy marks a clean break from competitors and Open Banking is a priority. The arrival of a major shareholder in Fidor Bank's capital gives it the means to follow and accelerate an offensive strategy, aimed firmly at innovation and customer service. Indeed, this bank is targeted at individual customers, unlike SolarisBank which focusses mainly on professionals.

Fidor Bank relies on a community of 500,000 members, of whom 200,000 are customers, who are encouraged to get involved in the bank's strategy by helping to define its supplementary services or suggesting changes to its existing ones. The community, like a social network, shares its advice, including advice about offers from rival banks. Active members are rewarded for their involvement.

BPCE is hoping that this strategic asset will help with launching new offers. While in Algeria the mutual group has announced the launch of the Banxy app - a neobank which is based on Fidor's technology - a launch is also planned for France, but in a seemingly more limited manner. Indeed, the French service will operate without a banking licence, at least to begin with.

French banks, in recent years, have been particularly interested in start-ups offering account aggregation services. So much so that this type of service is now an integral part of the French banking landscape.

Crédit Mutuel Arkéa and Crédit Agricole became shareholders in Linxo in 2012 and 2015 respectively. The online-only banks of these two groups - Fortunéo and BforBank - have thus signed partnerships with Linxo to allow their customers to benefit from the aggregator's services.

HSBC France, without investing directly in the French Fintech, also began a partnership with Linxo in October 2016, so as to offer its customers the latter firm's technology and services under a white-label[20], thereby giving them the chance to receive help in the management of their personal finances.

Another example, Crédit du Nord, launched its service aggregator, called "Synthèse multi-banque" in October 2016, based around technology developed by Fiduceo[21]. The subsidiary of Société Générale strengthened its range of services in February 2018 with its "Synthèse Multidoc" e-bill aggregation offer. In March 2017, Société Générale France itself launched an account aggregation service, which also uses Fiduceo technology.

Other major French banks don't want to be outdone: BNP Paribas has added an external account aggregation feature in collaboration with Budget Insight, while for Crédit Agricole this service is no longer the prerogative of BforBank customers. Now all Crédit Agricole customers can take advantage via the "Ma Banque" app.

3.2 Opening up banks' information system and the emergence of the API economy

The opening up of banking information systems allows banks to offer, in addition to their CBS, or Core Banking Solution, other services developed by partners, who

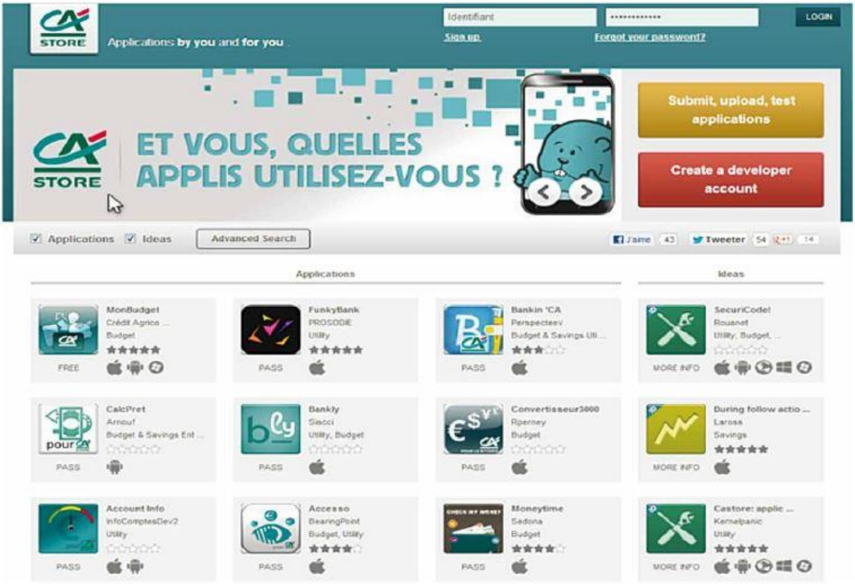
[20] *Linxo: press release about its partnership with HSBC France.*

[21] *A startup taken over, we should remember, by Boursorama, a part of Société Générale group.*

may be Fintechs or even banks, via Application Programming Interfaces, or APIs, which can bring ever-richer features. A recent example of a bank proliferating APIs: Singapore's DBS Bank, which claimed to offer 155 when it launched its API platform in November 2017, thanks to more than 50 partnerships with third-parties.
In France, several initiatives stand out which either already exist or are at the development stage.

With its singular approach, which was unprecedented at the time, Crédit Agricole stands as a major player in French Open Banking, and open innovation more generally. The bank's API, called "Simone", was born in 2012 and allows external developers to supplement the features of its banking app.

The principle is simple: the bank provides a software development kit via this API that gives developers secure access to its customers' banking data. The bank has gone further along this path and anticipated the danger of data theft, by accepting complete legal responsibility in case of fraud or theft.



The bank then created its own appstore, called the "CAstore", allowing developers, whom they called "Digiculteurs" (or "Digiculturalists") to offer their apps to the bank's customers. To use these services, customers pay according to the level of access they have signed up for: the basic "Pass Découverte" gives them the use of between 1 and 10 apps per month, or the "Pass Premium" with unlimited use. The sums earned are used for the upkeep of the platform, with the money left over going to the developers.

The platform has been very successful and Crédit Agricole organises regular hackathons in order to stimulate further innovations through themed competitions. The innovative nature of the service has been remarked upon several times, for example in the World Economic Forum's August 2017 report into disruption in financial services[22].

WILL BANKS BE LIEABLE FOR THEIR APP STORES ?

What would happen if one of these apps contravened the law? Would a bank be liable for an illegal app developed by a third party but released via its own app store? For France, the answer is contained in the law for trust in the digital economy, dated 21 st June, 2004 (LCEN - Loi pour la Confiance dans l'Economie)[23], which applies to all public communications, including app stores provided by banks.

LCEN distinguishes between two types of company: content editors, which are automatically liable; and hosts, which only become liable if they do not act promptly to remove all illicit content, once they have been informed of its illicit nature. When applying LCEN, the bank can be considered as editors of apps only if it validates the app before making it available to the public. Otherwise, the bank can only legally be considered as the host of the app.

In a more Open Banking-oriented approach, BPCE will soon launch a financial services marketplace based on supplying APIs. Beyond PSD2's regulatory service,

[22] *World Economic Forum: Beyond Fintech: A Pragmatic Assessment Of Disruptive Potential In Financial Services.*

[23] *Legifrance: Loi n°2004-575, of 21 st June 2004 for trust in the digital economy.*

the platform should make APIs available which grant easier access to products and services throughout the BPCE group.

Société Générale is preparing a comparable approach, with the launch of a similar marketplace planned for the end of 2018 or the start of 2019.

These additional APIs are particularly aimed at neobanks which are looking to widen their range of services.

STARLING BANK

This is the business model adopted by the neobank Starling. The British mobile bank, set up in 2014, built its mobile "banking marketplace" by integrating third-party apps. Its APIs mean that existing services can be assembled for an attractive user experience at both a lower cost and a shorter time-to-market than if they were developed separately.

In addition to a current account with interest and payment means, the service for individuals adds savings, cashback and collecting loyalty points via payment, as well as being able to dematerialise purchase details (to eliminate paper receipts). In February 2018, Starling Bank connected to BACS, the UK's CSM for clearance of transfers and withdrawals, having already joined Faster Payments UK (real-time mass transfers) and Transferwise, which competes with SWIFT for international transfers.
Since the end of April 2018, it has added services for businesses which are free for SMEs (with less than 10 employees and under 2 million annual turnover).

Such an approach, aimed at opening access to a veritable library of APIs, is the chance to generate new income streams. Indeed, if the use of PSD2 APIs is to be free, access to other data or types of third-party banking services, via APIs, can be monetised. This new trend, named API Economy, therefore offers enormous possibilities to increase both attractiveness and profitability.

Beyond the income generated by monetising them, well though-out APIs can bring indirect benefits, such as improving brand awareness or enriching a service thanks to the use of the API by, and fresh input from, partners.

BBVA, the Spanish bank with can claim 10 million customers (4 million of whom use digital channels), was the first major European bank to target such a strategy. On 24th May 2017 it launched its "API Market" platform.
This project was born out of a year of testing, with 1500 firms and developers, aimed at co-building a security policy with strong customer authentication at its heart. Its economic model depends on direct remuneration by API-using partners. In return, they have the chance to test their offers free in a dedicated environment.

The API Market platform[24] now offers 10 APIs for the Spanish market, with 4 of them equally available to the US market, and 2 for Mexico. BBVA claims to have won over several major Spanish groups, as well as a few Fintechs.

INTERVIEW

Clément Coeurdeuil - CEO and co-founder of Budget Insight

On the subject of TPPs and their ambitions for innovation, we spoke to Clément Coeurdeuil, CEO of the aggregator Budget Insight.

Galitt: for all types of account, apart from payment, web scraping will remain unregulated, and therefore authorised. What will you do? If banking APIs allow access to them as well, will you be willing to pay? Or, for that matter, to pay for "premium" services outside PSD2 for payment accounts?

Clément Coeurdeuil: GDPR[25] allows PSUs to have access at any time to all data collected about them by service providers. Banking data could therefore be made available to third-parties, such as TPPs. With clear consent, the latter could then web scrape the customer's other types of account, outside the scope of PSD2. If the account servicing PSP's API gives access to them, at a charge, then the price shouldn't be discriminatory. It should be within the average range of prices charged generally by all ASPSPs in the EEA, in relation with costs for interbank infrastructure and account management.

As an account aggregator, we have an economic interest in this. Web scraping costs us money; increasingly so. At Budget Insight, since we started in 2014, we

[24] *BBVA: API Market.*

[25] *European General Data Protection Regulations strengthen consumers' rights regarding their personal data and its transfer and has been in effect since 25 th May 2018 (n° UE 2016/679).*

have noticed that the time taken to incorporate a new banking institution into our web scraping tool has gone from three to five days per online banking site. It's even more for mobile banking apps, even though their information systems require less work or adaptation from us.

Galitt: what is your innovation strategy?

Clément Coeurdeuil: we want to bring payment to the heart of new styles of usage which are growing strongly, both intuitively and seamlessly. I'm particularly thinking of real-time conversation apps, or chat.

In partnership with the operator, such as WhatsApp, an artificial intelligence algorithm will be able to detect, in the chat, any need for P2P payment. An in-context offer will pop up, with the user's consent, and lead to the relevant payment initiation within a partner's dedicated interface. Any chat service could thus initiate a transfer, for instance when users have discussed about a common gift or a shared bill.

The social network or chat app operator will be in charge of their own customer experience. It's up to them to detect recurring needs, to find the appropriate context and then to find a authorised professional to integrate the payment service - or even other financial services, like investments, (micro-) loans etc.

Galitt: even just in the field of personal finance, the potential is huge and the need is for many differing APIs. How can you reconcile these regulated roles with the spontaneous nature of real-time exchanges?

Clément Coeurdeuil: the answer lies in part in what I call the chaining of APIs. Specialists in each identified field of finance bring their API or APIs, which match, or help to meet, an identified need. An API management module interconnects and orchestrates them, according to the customer's requirement, and combines them if necessary.

When the customer gives his or her consent the module can send the data to and from each API.

Instead of dedicated natural-language tools, such as those you can find in many insti- tutions' sites - where the customer has to find and visit those sites - the goal here is to connect the financial action directly to where the need is born; where it is formulated.

Galitt: for account-holding banks, is this the opportunity for a new and powerful distribution channel for their financial services?

Clément Coeurdeuil: absolutely! In fact, in Europe major account servicing PSPs have already become account aggregators (AISP). To such an extent that we can already predict the disappearance of the "Second bank". Relying on this type of partnership with TPPs allows them to take advantage of emerging markets and of the Fintechs' innovation.

3.3 Third parties, outside the banking sector, eyeing up banking data

Three profiles exist for third-party companies which are closely interested in banking data.

Firstly, we have insurance firms, which look on PSD2 as a chance to become payment institutions, and to offer their mutualist members the chance to bring all their accounts under one roof. In France, MAIF has launched just such a bank account aggregation service, called "Nestor", developed under a white label using technology from Linxo. This covers 140 account-holding institutions. A premium, subscription version, called "Nestor+", allows you to add personal expense forecast, based on your statements from recent months, as well as personalised analysis and overviews.

“Digitalisation involves a general lowering of entry barriers. Working from this analysis, we are very defensive of our core business, but there’s nothing stopping us from having an offensive approach to other branches of business.”
Pascal Demurger, Managing Director of MAIF[26].

The second group are mobile telephone operators. As an example, the launch of Orange Bank, at the end of 2017, showed the company’s desire to offer banking services to its customers. What is more, Orange has acquired a majority stake in Groupama Banque. Its objective: 2 million customers in the long term.

Finally, the last, and most disturbing, group is the GAFA (Google, Apple, Facebook and Amazon). These web giants which are at the heart of data management, and of what is more widely known as Big Data, have asserted their ambition of shaking up the traditional banking firms. Their comparative advantage over the banks lies in the, often favourable, image that their customers have of them, based on a famously strong user experience. Their entrance into the financial services market shows their desire to get hold of any and all types of data in order to have an ever-deeper knowledge of their users.

Apple’s and Google’s product catalogues both include a mobile payment Wallet, available for iPhone and Android smartphone owners respectively. Apple is continuing its roll-out, currently in twenty of so countries, while Google now appears to be prioritising Google Pay, judging from the importance accorded to the service during the most recent Google I/O annual event. The accent is put on the multichannel aspect, and of course on the customer experience, before, during and after purchasing.

At the end of 2017, Apple added a P2P payment service directly integrated within its iMessage system, thereby imitating Facebook which, as long ago as 2015, had unveiled Messenger Payments.

Amazon appears to be the GAFA member that is the most active in the financial services market, as the variety of services launched over the last few years can testify. We should especially note: Amazon Cash, a cash deposit service that allows you to top up your online account; Amazon Lending, a credit offer aimed at SMEs; Amazon Store Card, a private credit card which offers payment facilities;

[26] *L’offre d’agrégation MAIF”,an article in Les Echos.*

and Amazon Rewards Visa Signature Card, a credit card issued by Chase, launched in 2017.

The weight of the GAFA shouldn't obscure the presence of the Chinese web giants such as Alibaba in the financial services sector. Jack Ma's company offers, via its subsidiary Ant Financial, the Alipay mobile wallet and, in 2015, launched an online bank, called MYbank.

The stakes for these firms are huge: being able to control the entire value chain, and to make the customer journey smoother, but particularly to intensify their core business of collecting data and thereby getting to know their users and their users' habits more easily. For the moment, they are not drawing too much attention to themselves, but their financial power obviously leaves them capable of swallowing up any Fintechs which make the most of PSD2.

We should also note that some firms and payment services may not be impacted by PSD2. Indeed, PSD2 includes - just as PSD1 did - exhaustive lists both of categories of payment service providers and of operations which are considered to be payment services. Therefore, if a new payment method emerges, it wouldn't be regulated, as it wouldn't appear on PSD2's lists. By establishing these qualitative and technological choices, PSD2 would exclude from its scope any new payment activities, which would then find themselves in the same legal vacuum that payment initiators and account aggregators did previously.

For the banks, the short-term risk is of being disintermediated by these disruptive new firms which place themselves between the customer and his/her bank. In the longer term, a more direct form of competition could be born, with Open Banking acting as the midwife.

Opportunities or threats? It depends above all on the strategic positioning and the means which are currently being allocated. In both cases, PSD2 is opening the door to a new era in banking.

PERSONAL DATA : HOW TO RECONCILE GDPR AND PSD2?

PSD2 and the EU regulation number 2016/679, dated 27 th April 2016 relating to the protection of physical persons concerning the handling of personal data and the free circulation of this data (known as “GDPR” and in effect since 25 th May 2018) are the two major reforms of 2018. We need to consider how these two texts can be applied together and to ask if they are consistent.

On the one hand, PSD2 advocates opening up banks’ information systems to account aggregators and payment initiators, while, on the other hand, GDPR imposes strict regulations upon businesses about how to handle the personal data of European customers.

The two texts appear to have antagonistic philosophies and goals, as PSD2 views the sharing of data as an essential part of competition in the banking sector, whereas GDPR gives the citizen the control over the handling and use of this data so as to ensure maximum protection. However, a deeper analysis shows us that the two laws are, in fact, complementary.

One difficulty in reconciling the two regulations lies in the ideas of user consent.

PSD2 allows third-party service providers, distinct from account servicing PSPs, to access the user’s bank accounts, and therefore opens up the personal data harvested from them to these firms. Article 94 (2) of PSD2 provides for an explicit and contractual consent[27] between the user and the payment service provider.

In parallel, applying article 6 of GDPR, handling data is only allowed when at least one of six conditions is fulfilled:

1. Consent of the person for one or more specified goals;

[27] *Article 94 (2) of PSD2: “Payment service providers only have access to, handle and retain personal data which is central to the fulfillment of their payment service with the explicit consent of the PSU”.*

2. Processing is necessary to the completion of contract which the person concerned is a party to or to fulfil pre-contractual requirements taken at that person's request;

3. Processing is necessary to fulfil a legal requirement to which the party responsible for handling the data is subject;
4. Processing is necessary to protect the vital interests of the person concerned;
5. Processing is necessary to fulfil a public interest or in the exercise of official authority vested in the controller (the body handling the data);
6. Processing is necessary for the purposes of the legitimate interests of the controller.

In the light of GDPR, the articles dealing with consent within PSD2 mean that, by engaging in a contract with a payment service provider, the person concerned must be fully aware of the goals for which his/her personal data will be handled and must expressly accept such a clause. Therefore, such clauses must be clearly distinguishable from the other clauses inserted into the service contract.

The idea of explicit consent envisaged by Article 94 (2) of PSD2 is consequently a supplementary (and contractually-binding) condition which stands out from the explicit consent required by GDPR.

PSD2, although it is more restrictive concerning the handling of personal data, doesn't contradict GDPR.

The provisions of PSD2 which concern the gathering of explicit consent of the user as the only legal basis to authorise the gathering of personal data are therefore more restrictive than, but not incompatible with, the equivalent sections of GDPR.

Indeed, by only prescribing one situation as a legal basis for the handling of data - that is, consent - PSD2 excludes the other 5 conditions laid out in GDPR. By applying PSD2, data treatment can only be authorised by the completion of a contract.

Conclusion

Are we at the dawn of an era of Open Banking data?

PSD2 is another step along the path of open banking, begun in France by the banking mobility service and by the law dated 7th October 2016 for a digital republic. This latter bill enshrines data portability in law and entitles consumers to recover their data from their digital service providers in order to transfer them to another service provider. This right is now strengthened by the European general protection of data regulation (GDPR) which came into effect on 25th May 2018.

The boom in the banks' online services has obviously made this sector a fertile ground for these new regulations. Indeed, as of 25th May 2018, this data portability law allows consumers, particularly of online banking services, to recover all of his/her files and consumption data relating to transactions. To be able to do this, online service providers have to take all the necessary measures for a change of provider, particularly in terms of programming interfaces and data transmission.

So, we come back once again to the subject of APIs…

All through this white paper, APIs and in particular Open APIs, stand out as a real alternative to web scraping, and a pivotal point between security and innovation. Nevertheless, there is still a long road left to travel to reach standardisation of APIs and data structure, thereby allowing full interoperability between services in the European ecosystem.

We can note that French banks, after having initially been reticent, have fully understood what is at stake and the opportunities which exist to develop projects in this area. They were also inspired by European banks such as SolarisBank and Fidor Bank, which led the way in Europe for Open Banking.

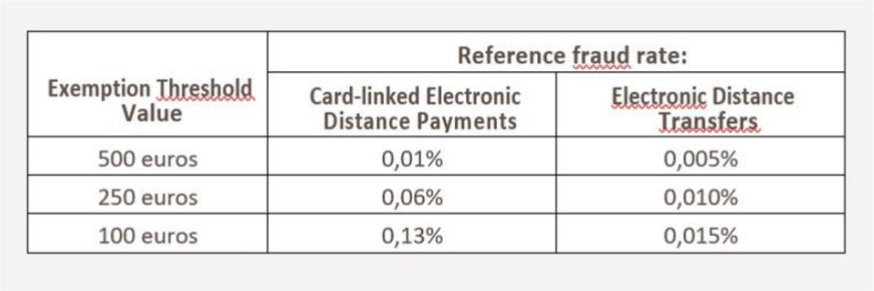
But how far can this movement go? As far as normalising banking data, which has until now been protected by traditions of secrecy and security? In any case, it is vital that the banking sector watches current developments very closely. Instead of suffering the blows landed by new firms which are often more agile, banks should position themselves at the centre of the action, with a responsible and balanced definition of conditions for access to bank accounts. And then foster the inception of a new value-creating ecosystem.

APPENDIX

The 9 cases of exemption from SCA

- When consulting account information (article 10):
    - if it is not the first connection to the ASPSP via this TPP, and less than 90 days have passed since the previous authenticated connection;
    - if the consultation is restricted to data which is “not sensitive” (name, account number, statement of operations over the last 90 days);
- For contactless payment of under E 50, and below a ceiling of E 150, limited to a maximum of 5 consecutive contactless payments since the last strong authentication (article 11);
- For electronic distance payment for amounts under E 30, and below a ceiling of E 150, limited to a maximum of 5 consecutive electronic distance payments since the last strong authentication (article 16);
- Automated payments concerning transport and parking (article 12);
- Payments to trusted beneficiarys, although the creating and amendment of the list of these beneficiarys (which the PSU can update on his/her customer space) re- quires strong authentication (article 13);
- Repeated transactions, for which the amount of successive transactions must be identical and addressed to the same beneficiary, with the first payment being sub- ject to strong authentication (article 14);
- Transfers between accounts held by the same person, as long as these accounts are held within the same ASPSP (article 15);
- Payments based on secure protocols and procedures and dedicated to transactions between legal entities, as long as the method in question is considered by the relevant national authority to offer a level of security which conforms to PSD2 (article 17);
- Electronic distance payments, if the transaction is categorised by the PSP as low-risk (Transaction Risk Analysis or TRA). This exemption is subject to fraud levels from the PSP for each type of payment (card-linked, or by transfer) which are lower than the reference levels set out in RTS. These vary according to the amount and have Exemption Threshold Values, which are set out in the table below. In addition, real-

time risk analysis by the PSP must have found no unusual element or abnor- mality linked to the payment: an unusual amount, unusual or high-risk location of the payer, similarities with known cases of fraud, unusual information concerning the channel used for payment, etc. (article 18).



Exemption Threshold Value	Reference fraud rate:	
	Card-linked Electronic Distance Payments	Electronic Distance Transfers
500 euros	0,01%	0,005%
250 euros	0,06%	0,010%
100 euros	0,13%	0,015%

About the authors

Thibault Verbiest - *DS Avocats - Partner*

A lawyer, member of the bar in Paris and Brussels and a former businessman, Thibault Verbiest boasts thorough experience parti- cularly of intellectual property, but also of the sectors of technology, the media and telecommunications. He advises our firm's clients in a variety of operations, from the dematerialisation of banking and financial services, to the digital transformation of companies, and including mergers and acquisitions in the technology sector. He also assists our clients on certain litigation files, especially in the fields of intellectual property or liability connected to cybersecurity.

Frédéric Bellanca - *DS Avocats - Partner*

A member of the bar in Paris, Frédéric Bellanca leads a specialist team in the field of banking, financial and stock market regulations at the service of financial institutions, Fintechs and industrial groups both in France and abroad. He gives advice and assists in complex financial litigation both in front of common law courts and bodies such as the AMF and ACPR.

Diane Richebourg - *DS Avocats (associate)*

Diane Richebourg is a lawyer in the Banking and Finance Department of DS Avocats, and acts in all banking and financial issues, as well as on the subject of Fintechs and crypto-finance.

Emmanuel Caron - *Galitt - Payment Consulting*

Emmanuel is Practice Manager within Galitt Payment Consulting, primarily in charge of regulatory and economic subjects. For over 15 years, Emmanuel has worked on the development of payment systems, whether that be cards or other payment means. His career has seen him lead projects on the reform of the card system, the economic balance of payment systems and the impact of the European regulatory framework. His expertise lies particularly in a deep knowledge of European payment and card markets.

Guillaume de Longeaux - *Galitt - Payment Consulting*

Trilingual, and with 20 years' experience in retail banking, Guillaume joined Galitt in 2017 as a Manager, to develop the firm's expertise in flows and cash management (instant payment, SWIFT and SCT transfers, SDD withdrawals). He also works on payment regulation compliance projects: deregulation (PSD2), anti-money laundering and sanctions/ embargoes. A graduate of the Paris Institute of Political Studies, Guillaume also leads European training courses, both on the subject of flows and of car and its variants in Europe.

Gwendal Boëdec - *Galitt - Payment Consulting*

A graduate of Rennes Institute of Political Studies and the Ecole de Guerre Economique (EGE), Gwendal is currently a Consultant within Galitt's Payment Consulting Business Unit, working primarily on subjects connected to innovation and regulation in the payment sector.

Several colleagues within Galitt have assisted with this project:

Gérard de Moura:	*Assistant General Manager*
Stéphane Dubois:	*Practice Manager*
François Flouriot:	*Practice Manager*
Vincent Mesnier:	*Executive Director - Testing Solutions*
Paul Noel:	*Consultant*
Isabelle Pujadas:	*Communications Director*
Gérard Tchakgarian:	*Chairman*
Diane Walch:	*Business Development Director*

Rendre les paiements simples, efficaces et sûrs, dans la vie de tous les jours.

galitt
a Sopra Steria company

17 route de la Reine
92100 Boulogne-Billancourt- France
Tél. : +33 1 77 70 28 00
contact@galitt.com
www.galitt.com