WHITE PAPER | JANUARY 2016

PSD2: Igniting Digital Payment Innovation

PSD2 (EU Payment Services Directive revised) is just the beginning of a journey towards a more open and collaborative financial system. To navigate safely, organisations need to embrace the API-based, composite app world that is pushing traditional financial systems towards digital transformation.

Jordi Gascon
CA Security EMEA Presales

Andrés Gómez
CA API Management Presales

Juan Lopez-Rubio
CA Services

ca technologies

Table of Contents

Executive Summary

Challenge

In 2013, The European Commission proposed to review the existing EU Payment Services Directive 2007/64 (PSD) both to modernise it and to take account of new types of payment services, such as payment initiation services. Suppliers of new types of payment services have brought innovation and competition, providing more and often cheaper alternatives for Internet payments; but these services have until now been unregulated. Bringing them within the scope of the PSD has boosted transparency, while supporting innovation and improving security in the single market. The move has also created a level playing field between different payment service providers.[1]

At the same time, certain rules set out in the PSD have been transposed or applied by member states in different ways, leading to regulatory arbitrage and legal uncertainty. These rules include those exempting a number of payment-related activities from the scope of the Directive, such as payment services provided within a "limited network" or through mobile phones or other IT devices

In a number of areas, the lack of regulation around limited networks has resulted in impaired consumer protection and created competitive distortions. Updated definitions ensure a level playing field between different providers and address in a more efficient way the consumer protection needed in the context of payments.[1]

The revised EU Payments Services Directive 2015/2366 (PSD2) will force financial institutions and other corporations who receive electronic payments to open their customer information to so-called **Third-Party Providers (TPPs).** Some of these TPPs will be acting on behalf of a user to collect and consolidate information about bank accounts **("Account Information Services – AIS")**. Others will be facilitating the use of online banking to make Internet payments **("Payment Initiation Services – PIS")**.

Opportunity

The opportunity is two-fold: Firstly, financial institutions could become TPPs themselves, leveraging their installed customer base and expanding their services catalogue to their clients and prospects before they lose footprint and relevance in the market to new entrants. Secondly, for each organisation, the need to be compliant can ignite digital transformation towards a secure, open, API-based and customer-centric organisation.

Benefits

There are many benefits of implementing the changes required for PSD2 compliance, particularly when taking a strategic approach.

- Market Expansion
  - Becoming a TPP or a "trusted identity" will not only help your organisation to keep loyalty in your customer base but expand your business to capture new prospects.

- IT Modernisation
  - PSD2 might force you to redesign parts of your infrastructure to become customer-centric, API-based and open. This will bring the need to implement a renewed architecture that can secure the processes to protect your customers and your organisation. Risk analysis, identity management, strong authentication and API management are just some of the technological support that will be needed.
- Future Proof
  - Today's challenge is PSD2, whereas previously it was SEPA or PCI/DSS, and tomorrow there will be other regulations. There is a need to build a new architecture able to scale and support new regulations and future market needs easily. A modular and pluggable engine-based approach that is sustained by APIs will be critical.
- Time to Market
  - Decoupling processes to make them API-based, modular and pluggable will create a side effect of being able to create new services in your offering catalogue more quickly.
- Customer Satisfaction and Protection
  - Providing new and extended services while being compliant and protecting your customer data and privacy will strengthen your commercial relationship with your customers.

Section 1: Challenge

The Need to Be Compliant

Being compliant with regulations is not optional. Furthermore, while the former directive (2007/64/EC) only applies to intra-EU payments, PSD2 extends a number of obligations to payments to and from third-party countries where one of the payment service providers is located in the EU.

Transposition to Member States level legislation is still to be finalised, but the EU has been clear that "they must not adopt new measures contradicting the provisions of PSD2".[1]

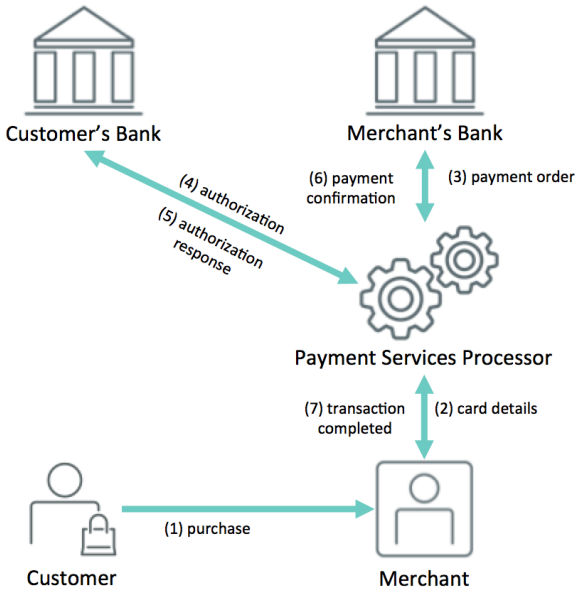


Figure 1.

Current payment schema

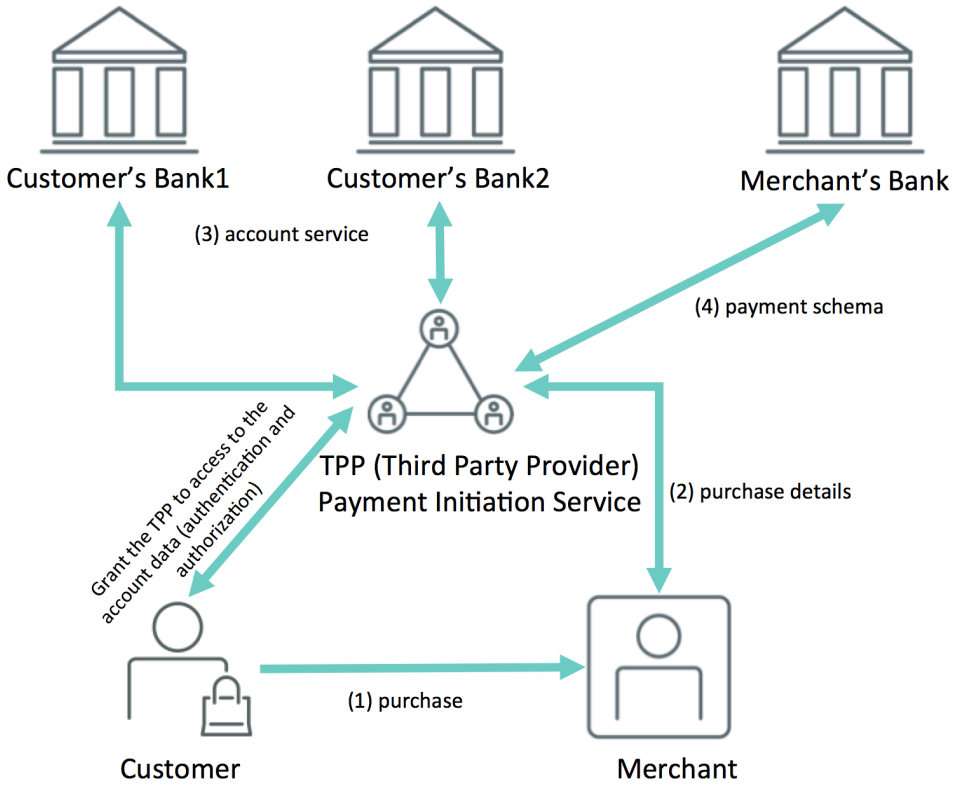
So how does this new directive change the current payment schema?

Today the flow of most payment transactions is as shown in Figure 1, where the customer has a credit or debit card. The customer wants to buy something from the merchant and provides his or her card details to different actors in the chain, normally the merchant and one or more payment services providers (PSP). The PSP will initiate the payment order with the customer's bank and will receive the transaction status (completed or rejected) from the bank.

The PSD2 regulation proposes to open the account data of the customer's bank to third-party providers (TPPs) in order that anyone can initiate a payment transaction and not only the current PSPs. The TPP can be any actor; it could even be the merchant itself, the current payment service providers or the banks. Figure 2 shows, at a high level, where the TPP appears in the flow of the payment transaction and how the bank expose the account services to be consumed directly from the TPPs. Of course, in this new paradigm a trusted relationship must be established between the customer's banks and the TPP, and the customer must grant access to his account data to the TPP's apps.

Figure 2.

PSD2 enabled payment schema.



You may be thinking that both models are very similar. The difference is that the TPP role in Figure 2 can be played by anyone, for example a merchant or a bank. The 'middle man' does not need to be a PSP. However, to be able to act as a TPP, and also to be compliant, at least two trusted relationships must be established: with the customer's bank and with the customer.

Why Is PSD2 Different From Other Regulations?

While in the past banks had control of practically the whole transaction process from beginning to end, the part of PSD2 concerned with access to accounts (XS2A) demands that banks in particular allow access to customer accounts to other parties (Account Information Service Providers – AISP) acting on behalf of their customers. In practical terms, this means banks will need to provide a method (likely using an API) for third parties able to access their customer data so it can be consumed by a mash-up or composite application created by the corresponding TPP. However, this is not just as easy as opening the account to another party; banks will still need to establish customer-managed trusted relationships with their partners, and to provide strong customer authentication as well as customer protection (unconditional refund right will be guaranteed through PSD2).

Another important aspect of this directive is its aim to open up the market for innovative electronic payments, not just those based on credit cards. This will certainly help develop new payment services and facilitate new market contenders other than traditional financial institutions.

Section 2: Opportunity

Leveraging the opportunity to accelerate your digital transformation

Whether traditional banking organisations decide to become a TPP or not, they will still need to open up their data to third parties that will act on behalf of their customers. This requirement will force banks to establish a secure and documented method to be used by those external actors while at the same time they will still need to provide the appropriate security controls and guarantees to protect their customer data.

Nowadays, the optimal way to expose data and processes to third parties (internal or external) is definitely through an API-based approach. However, once the API is exposed to the outside world, you need to secure and manage all aspects of the use of the API itself (service level agreements, metering, security, enrolment, subscription, auditing, monitoring, etc.). In this case, because of the requirements of XS2A, you will need to provide control of how the data is accessed to its owner so a mechanism for customer self-service is also necessary.

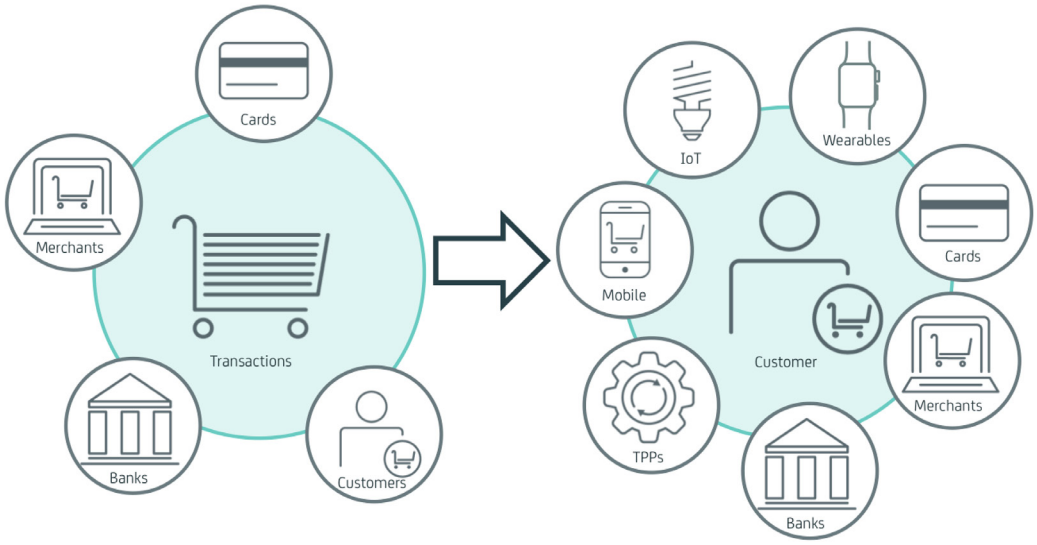
Given the aforementioned requirements, this need becomes an innovation driver that will help supporting the overall digital transformation of processes and services. If organisations are forced to deploy these features in order to be compliant they may take advantage of the model and plan an 'API-fication' model for all existing and future banking services. By taking this approach banks will be able to deliver new digital services to the market in a faster, standardised and secure way that will improve their market competitive scope.

Traditional banks and other organisations can take advantage of this to increase customer satisfaction, loyalty and revenue average by developing innovative new apps and financial products oriented to the new disruptive trends such as wearables (watches, authentication wristbands, etc.), mobile devices or the Internet of the Things (IoT).

If applied strategically, this customer-centric approach can help achieve compliance and take advantage of new market opportunities more effectively than a traditional transaction-based approach.

Figure 3.

The evolution of transaction processes



Section 3: Benefits

Key Benefits

Market Expansion

Becoming a TPP will not only help your organisation to maintain a loyal customer base, but also expand your business to capture new prospects.

New market contenders will fight to become the front-end for customer payment services and own the relationship with end users to strengthen their position for proposing new products and services directly.

Established organisations that hold a position of "trusted identity provider" will be able to create a new collaborative ecosystem where customer identity and the confidence placed in this identity will help them develop a new set of innovative digital services and marketplaces.

IT Modernisation

The move from a transaction-based approach into a customer-centric approach needs to be sustained by a deep technology transformation. While a "big-bang" approach is likely to be difficult to embrace (except for new entrants), a phased adoption of the new digital paradigms allowing the incorporation of the new regulatory requirements and digital market trends is recommended.

Data, protocol mediation and transformation will be needed in order to incorporate legacy systems and adapt them to the overall new architecture.

Future Proof

The IT architecture needs to be revisited so it is able to keep the pace with regulations as well as business drivers. A layered approach supported by generic engines or "brokers" tasked with specific topics is recommended as processes are no longer isolated end-to-end or proprietary. On the contrary, there is a new world of mash-ups, composite and collaborative applications to take advantage of and your architecture needs to be ready to support it. Beyond the regulatory needs of implementing PSD2, new requirements can be easily plugged into the existing engine or "broker".

Time to Market

There is a compelling need to reduce time to market and deliver new services faster while keeping or increasing the quality of service that customers expect. By decoupling common functions from core processes such as authentication, authorisation, risk management and analysis, access control, identity management and federation, organisations can create a foundation for effectively standardising, controlling and measuring those transversal features which can remove complexity and reduce time to market.

Customer Satisfaction and Protection

Providing new and extended services while being compliant and protecting your customer data and privacy will strengthen your relationship with your customers.

Furthermore, opening up customer data on behalf of your own customers to third parties will increase the need to secure that process with the appropriate due diligence. Only by providing clear and user-controlled visibility of how its data is accessed and managed ("the five Ws"—who, where, when, why and what) will an organisation create the appropriate level of trust with its customers. The new directive focuses on strong authentication, going a step further than the previous PSD directive and EBA guidelines, which already stated the need to protect sensitive payment data when stored, processed or transmitted.

Section 4: Conclusions

Conclusions

PSD2, while being a mandatory regulation for EU member states, also provides an opportunity to modernise your architecture, open up back-end data, accelerate your digital transformation effort and take advantage of the new business opportunities.

When considering how best to respond to the new regulations, we cannot forget that this is not just a directive but also confirmation reflection of the trend for putting IT at the service of people, in particular consumers. In fact, the directive looks set to improve citizens' options for adopting innovative payments that will make their lives easier and enrich the way the payments market works today.

There will be more directives in this spirit and adopting user-centric digital services in your organisation will allow you to align with future market requirements, as well as meeting today's PSD2 demands.

Those organisations that seize the opportunity to create a strategic advantage out of their compliance efforts will set themselves on a journey to competitive advantage moving forwards. Now is the time to consider your own PSD2 response and explore how an API-based approach can empower your organisation to boost customer satisfaction and accelerate your digital transformation.

Section 4: About the Authors

About the Authors

Jordi Gascon, CISM is Senior Presales Director for Security at CA Technologies EMEA. With more than 25 years of experience in the IT industry, his current responsibility includes the support for the entire CA Security portfolio across the EMEA region by analyzing and designing the technology solution that best meets customers' or partners' needs.

Andrés Gomez, CISA is Principal Presales Consultant in charge of the CA API Management solutions for Spain and Portugal. His focus is to bring to the Iberian market the awareness and adoption of a sound and proper management approach for API-based digital transformation projects.

Juan Lopez-Rubio, CISA, CISSP, is a Services Architect for the Security Practice in South EMEA. He works with CA Technologies customers and partners for delivering the proper solution architecture to maximise the value of the security technology and meet market requirements.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

References

1. European Commission – Fact Sheet. "Payment Services Directive: frequently asked questions" MEMO/15/5793

Sources

1. DIRECTIVE 2007/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC
2. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC
3. EBA/GL/2014/12_Rev1 FINAL GUIDELINES ON THE SECURITY OF INTERNET PAYMENTS. European Banking Authority
4. SUPPLEMENTARY REPORT on the proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC (COM(2013)0547 – C7-0230/2013 – 2013/0264(COD))

CS200_174616_0216