Demystifying PSD2

www.fiorano.com

Contents

Overview

PSD2, the revised Payment Services Directive, is a regulation of the European Union that simplifies the process of making online electronic payments across the banking value-chain. While strictly applicable within the 28-member European Union, starting in January 2018, the benefits of the regulation to end-customers coupled with increased competition and innovation across the industry driven by Open Banking make it interesting to a broader, global audience.

PSD2 not only simplifies electronic payments but also mandates critical organizational changes across the entire retail-banking value-chain.

This paper discusses the implications of PSD2 from an end-user standpoint. As we will see, the introduction of dedicated entities to manage front-office transactions across banks results in simplified end-user experiences with increased backend banking transaction throughputs and efficiencies.

PSD2: the fundamental value

To understand the essential value of PSD2, one must review the state of retail banking today. A typical retail customer today has accounts at multiple (two or more) banks. Each bank issues its own security token to the user, has unique security/sign-on procedures and requires the user to learn specific methods to create new beneficiaries, send international payments, check exchange rates, etc. Moreover, each bank has different ways of storing the transaction-history of each account, different guarantees of delivery (time taken for payments to complete) and different jurisdictions of operation, to cover just a few parameters.

Today's banking experience thus requires users to store multiple security tokens, memorize multiple passwords, learn multiple different screens/methods for basic payment and other banking operations with no guarantee of consistency for any transaction history. For a user with two or more bank accounts, the complexity of normal transactions soon becomes overwhelming. Managing multiple bank accounts is far from a pleasant experience in this scenario.
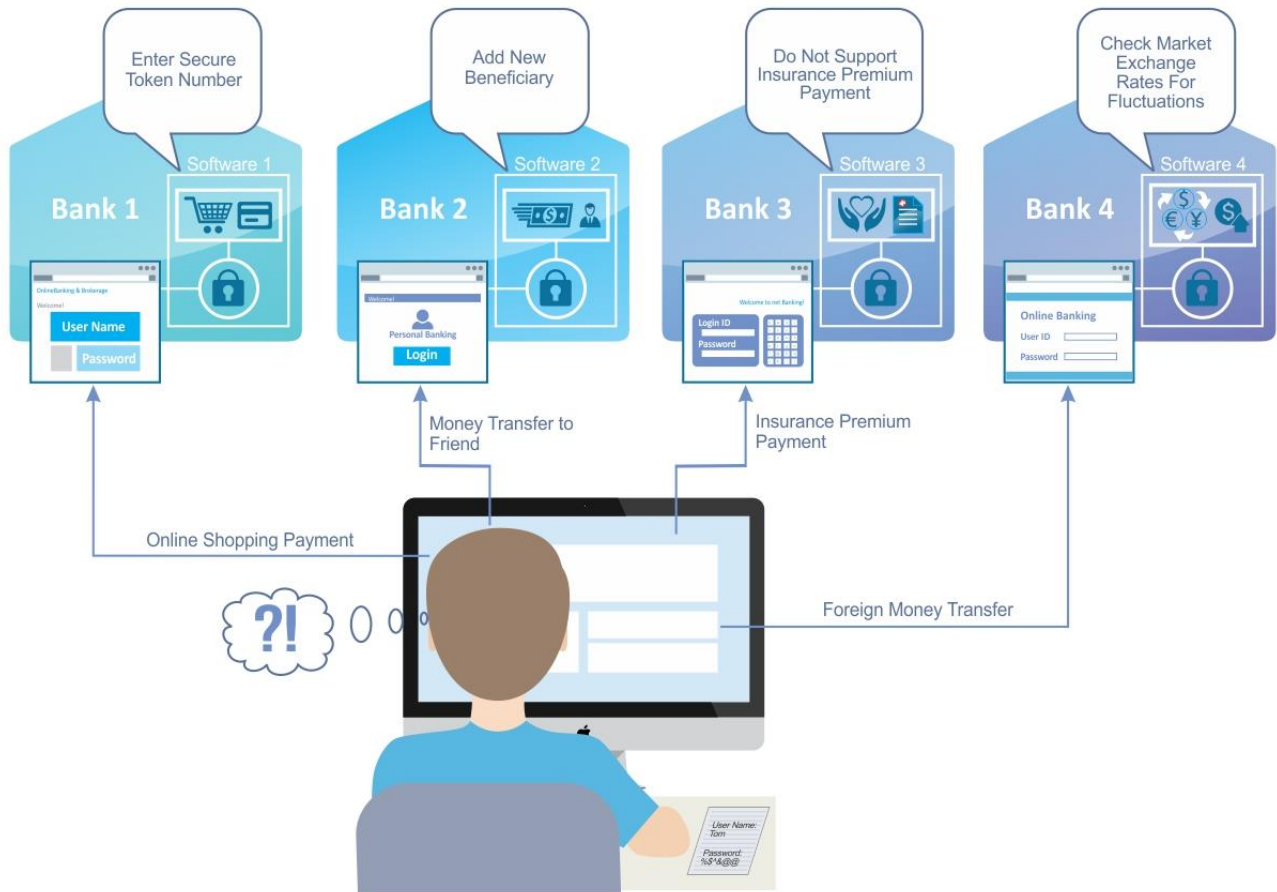
Figure 1: Current Retail banking ePayments setup

PSD2 dramatically simplifies the current issues in retail banking by mandating the creation of a third-party - the Payment Initiation Service Provider (PISP) - to manage payments consistently across multiple banks.

The PISP serves as a single entity to manage entire attributes of an end-user's bank accounts. End-users provide details of all their bank accounts to the PISP and authorize the PISP to perform payment, transfer and (as necessary) other operations at the respective bank on behalf of the end-user. Moreover, the transaction history of each operation performed by the PISP on behalf of the end-user is stored at the PISP. The PISP thus becomes an aggregator of all transactions for a given user for all accounts pertaining to the user across multiple banks. With PISPs in place, banks no longer need storing front-office transactions as these are outsourced to the third-party PISP.

This "separation of responsibilities" between the PISP and the retail bank dramatically simplifies the overall banking value-chain.
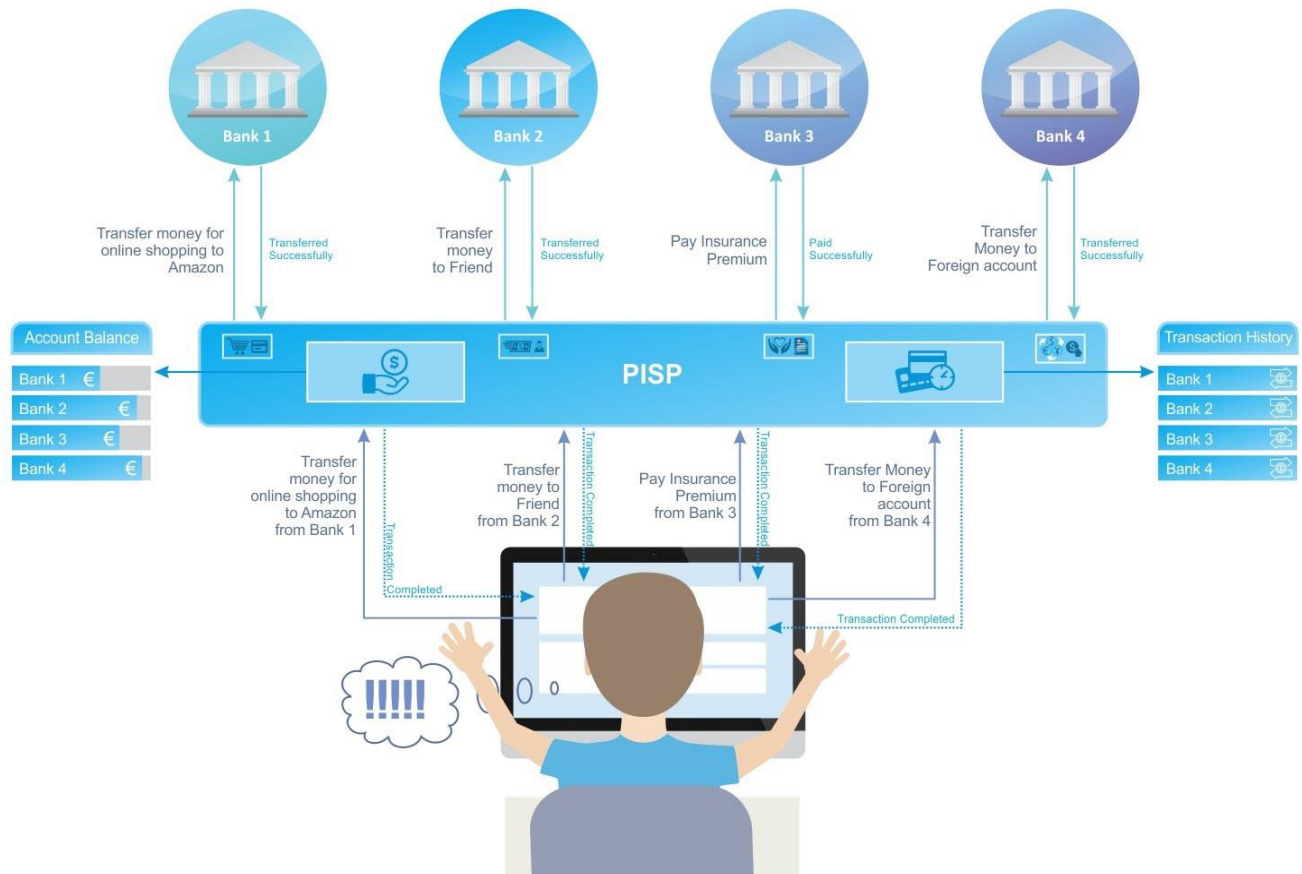
Figure 2: PSD2 Aggregates Security, Workflows and Front-office Transactions

With PSD2 in place, the end-user immediately experiences several benefits:

- **Single login to access all bank accounts:** The user only logs into the PISP. Since the PISP stores all details of each of the users' bank-accounts, there is no longer any need to login separately into each bank.

- **Single consistent format to make payment from any Bank to any beneficiary:** Each user with a PISP account creates a single list of beneficiaries. The user can then direct the PISP to pay any beneficiary from any of the Users' bank-accounts at the PISP by just selecting the appropriate Bank/Beneficiary pair.

- **Simplified transaction history:** PSD2 mandates that the PISP store the history of each transaction made by a user. The history of each banking transaction (payment, transfer, etc.) performed by the end-user is stored by the PISP, regardless of the bank with which the transaction was done. The user has efficient access to a comprehensive transaction history from the time of inception of the account in a single, consistent format.

From figure 2, it should be obvious that PSD2 brings dramatic structural and organizational changes to retail-banking. Besides the obvious simplification of payments processing, PSD2 also brings several other benefits to end-users including

- **Exchange rates, Time Guarantees**: For each payment transaction, PSD2 mandates that the bank provide the exchange-rate (if the target currency is different from the source) and a time-guarantee for the completion of the transaction.

- **Time-based access to payment services**: For enhanced security, systems can be configured to allow access to banks based on specific time frames. Similarly, quota-based policies can be set up to limit consecutive accesses by the same user.

- **2-factor Authentication**: The directive mandates that for any payments over a certain limit (currently 30 Euros, subject to revision), banks must get the user's permission via a 2-factor authentication, ensuring better protection for all consumers. In the 2-fractor authentication process, the bank gets the permission of the consumer via an encrypted communication channel, typically from the consumer's mobile phone.

- **Assured Security**: PSD2 mandates 2-way SSL connections and other sophisticated security standards between all third-parties and banks.

Third-party providers in the PSD2 world

As explained above, all consumer benefits of the PSD2 directive are delivered by introducing third-party providers ("TPP"s) between consumers and Banks. The third-party providers (TPPs) mandated by the directive include PISPs (Payment Initiation Service Providers), AISPs (Account Information Service Providers) and ASPSPs (Account-Servicing Payment Service Providers).
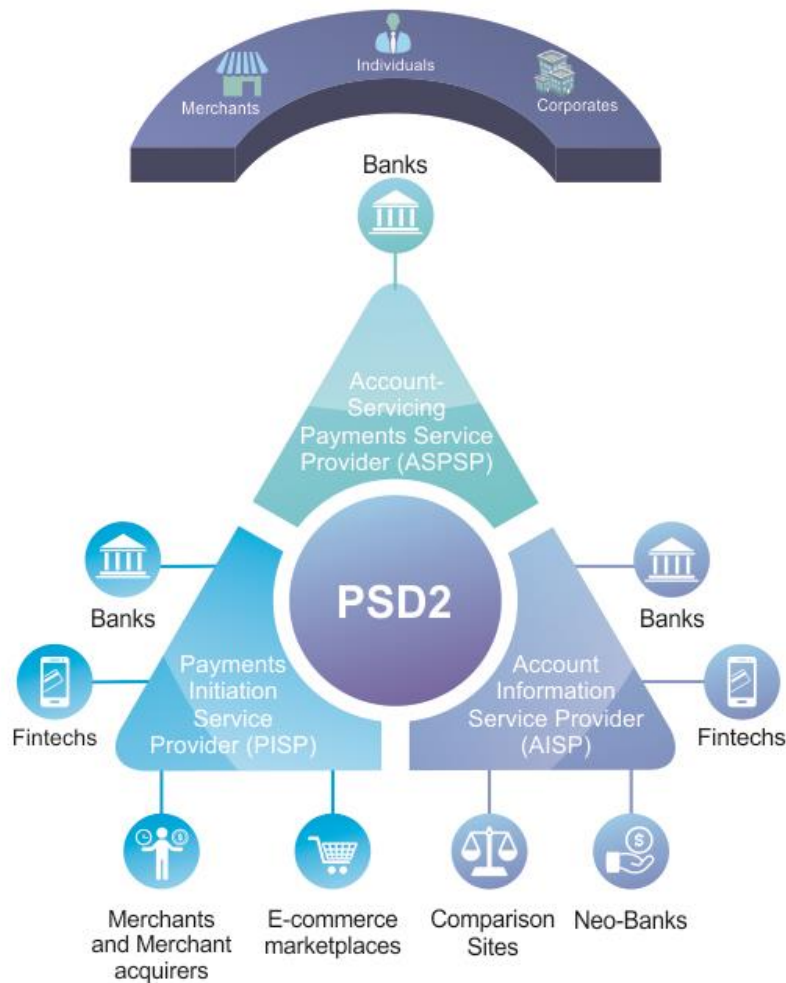
Figure 3: Third-Party Providers (TPPs) in the PSD2 world

Figure 3 illustrates the various third-party providers in the PSD2 world. The simplest provider is an AISP, whose function is just to aggregate the account information of consumers, like an ATM in the cloud where one can check one's consolidated bank balances at any time. Banks, FinTechs and Comparison sites may choose to be AISPs. PISPs are more sophisticated, with the ability to initiate payments on the behalf of consumers via any bank account the consumer holds, provided that the consumer has authorized the particular bank with the PISP. Banks, FinTechs, Merchants and eCommerce Marketplaces may choose to become PISPs. ASPSPs perform the functions of both AISP and PISP together and this function is necessarily restricted to Banks.

So, where's the complexity?

Now that the reader has understood the basic organizational structure and some of the benefits of PSD2, one begs the question: so, where's the complexity? The complexity around PSD2 relates not to its semantics (which are relatively simple as far as consumers are concerned) but to the fact that implementation of the directive requires interactions between Banks and the multiple third-party providers (TPPs) mandated by the directive.

PSD2 complexity centers around the security and communication operations between a particular TPP, for instance a PISP, and the target Bank(s) that the PISP interacts with. These issues are best illustrated with an example such as a typical funds-transfer performed by a TPP (AISP, PISP or ASPSP) on behalf of an end-user. A typical funds transfer involves the following steps:

1. **Bank-TPP connections**: A TPP typically connects to the Bank via a secure, time-bound 'tunnel'. This requires the Bank to expose its internal interfaces for those operations that the TPP requires: user authentication, checking account balances, Transfer instructions, etc. Exposing interfaces cleanly and consistently to all PISPs is a fairly complex challenge, since the current PSD2 standard only states that the interfaces are to be exposed and *does not define **how*** the interfaces are to be exposed. As such, if two Banks expose the interfaces slightly differently, a PISP must access these two banks differently. As the number of banks increases, the access-process can get complicated. The PSD2 directive requires that all banks connect to TPPs via secure APIs, using API-Management technology. Medium sized banks will have to understand, acquire and implement this technology.

2. **Execute instructions with particular time-bounds**: The Bank must ensure that all the operates related to the funds-transfer are performed within a stipulated time, since PSD2 mandates that the Bank initiate the funds-transfer with specific time-guarantees. While several banks have good-enough 'back-end' technology to meet these guarantees, many others are not organized enough to meet the (relatively strict) time bounds. As such, many banks will have to upgrade their internal technology with modern integration engines such as ESBs (Enterprise Service Buses).

3. **Cryptographic traces of all transactions with 'non-repudiation'**: The PSD2 directive requires banks and TPPs to maintain a full cryptographic trace of each transaction carried out on behalf of a consumer. Moreover, the directive mandates that certain operations between TPPs and Banks be based on assured "once and only once" delivery semantics using positive acknowledgements, typically delivered using "B2B" (Business to Business) integration technology.

PSD2 thus requires several relatively sophisticated technologies including API Management, Enterprise Service Bus and B2B Integration. While ESB and B2B technology are relatively mature, API Management, which forms the most critical element of the PSD2 implementation from the standpoint of a Bank, is relatively recent and is currently implemented only by some of the larger, more sophisticated banks. Most small/medium sized institutions, which form the majority of banks in the European Union, do not implement API, ESB and B2B technology to the level required for an efficient PSD2 implementation that scales with the growing consumer demand.

To conclude, while the semantics of PSD2 are relatively straight-forward, the challenges and complexities around the implementation of the directive are primarily of a technical nature. These challenges are the subject of a separate Whitepaper.

ABOUT FIORANO SOFTWARE

Founded in 1995, Silicon Valley based Fiorano is a USA (California) Corporation, a trusted provider of Digital Business Backplane and enterprise integration middleware, high performance messaging and peer-to-peer distributed systems. Fiorano powers real time, digital enterprises with bimodal integration and API Management strategy that leverages the best of systematic (centralized, high-control) and adaptive (federated, high-speed) approaches to deliver solutions across cloud, on-premise and hybrid environments.

Fiorano operates through its worldwide offices and a global network of technology partners and value-added resellers.

Global leaders including AT&T Wireless, Boeing, British Telecom, Federal Bank, L'Oréal, McKesson, NASA, POSCO, Rabobank, Royal Bank of Scotland, Schlumberger, US Coast Guard and Vodafone have deployed Fiorano to drive innovation through open, standards-based, event-driven real-time solutions yielding unprecedented productivity.

To find out more about how Fiorano can help you meet your enterprise integration objectives, visit **www.fiorano.com** or e-mail **sales@fiorano.com**

www.fiorano.com

AMERICAS
Fiorano Software, Inc.
230 S. California Avenue,
Suite 103, Palo Alto, CA 94306
USA Tel: +1 650 326 1136
Fax: +1 646 607 5875
Toll-Free:+1 800 663 3621
Email:info@fiorano.com

EMEA
Fiorano Software Ltd
3000 Hillswood Drive
Hillswood Business Park
Chertsey Surrey KT16 0RS UK
Tel: +44 (0) 1932 895005
Fax: +44 (0) 1932 325413
Email: info_uk@fiorano.com

APAC
Fiorano Software Pte. Ltd.
Level 42, Suntec Tower Three
8 Temasek Boulevard
038988 Singapore
Tel: +65 6829 2234
Fax: +65 6829 2235
Email: info_asiapac@fiorano.com