The Constantia Institute

Review of Priviti PSD2 Use Case and its positioning compared to alternative marketplace offerings

The revised Payment Service Directive (PDS2) is a directive focused on better integration of an internal market in payment services. Third parties (Account Information Services Providers or AISPs and Payment Initiation Service Providers or PISPs) will have access to transactional data to either analyse the data and/or to execute payments. The PSD2 is a directive that EU member states need to implement into national legislation. The implementation deadline for EU member states is the **13th of January 2018.** The key changes of this directive are clear: financial institutions will need to give access to bank accounts to third parties when double consent is obtained.

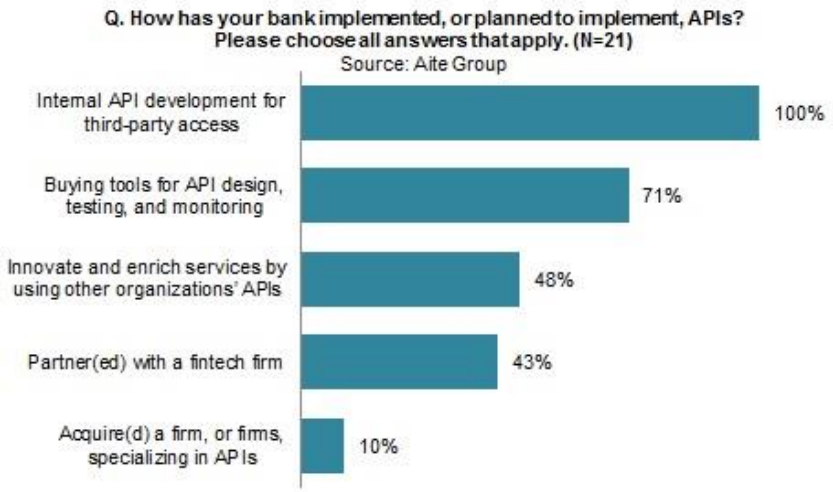
This revision of the PSD directive also follows the General Data Protection Regulation (GDPR), which focuses on the protection of personal data and the transparency towards the natural person and enters enforcement on the **25th of May 2018**, which is not excluded from the PSD2.

The PSD2 stipulates even further requirements regarding transparency towards the natural person, especially when he/she interacts with a PISP. The natural person should be informed about the (executed) payment transactions. The general obligations regarding the information to be provided are the same for both the GDPR and the PSD2: the information needs to be concise, transparent, and presented in an intelligible and easily accessible form, using clear and plain language.

Drivers for third party authentication solutions

With the revised Payment Services Directive (PSD2) at the doorstep, banks in Europe are working to allow third-party providers free access to payment accounts for payment initiation and account information services. Concentrating on compliance with PSD2 regulatory requirements at present, banks may move from a payment-centric API strategy to a wider transaction banking-based API strategy—if they open their APIs to fintech partners.

Meanwhile, transaction banking is receiving heightened attention from fintech companies, and this inevitable march to greater levels of automation and more open APIs might well lead to a restructuring of traditional banks' IT staff resources.



APIs are the conductor of all transactions and the objective for financial institutions right now is to develop and implement APIs that will be secure and agile. APIs will be used in every situation where banks must share data.

At its core, PSD2 is about enabling payments. It will create a shared, common experience for both banks and users that ensures data protection and customer privacy. It is based on common standards that encourage sharing of information between and among account information service providers (AISPs) and payment initiation service providers (PISP).

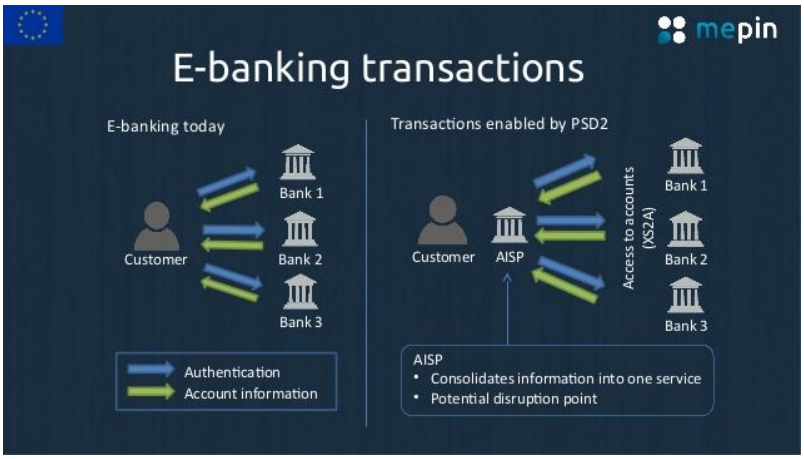
The significance of PSD2 is that it will connect financial organisations to provide a better experience for all in the financial ecosystem. Any financial institution that wants to conduct business with European banks, brokerages, insurance firms, or any company or government group that handles financial data, must comply with the PSD2 framework for its data to be shared and used. PSD2 promotes an openness not now normally seen among the banking industry, and because it leverages innovative technology, it is unique opportunity in how progressive it is.

Guaranteed entry for third-party providers (TPP)

To improve transparency and security in the single market and to create a more level playing field, the PSD was expanded to include third-party providers (TPPs) as well as the Payment Service Providers (PSPs). A major component of PSD2 is Open Access to Customer Accounts (XS2A), which requires banks and other institutions to share payment account information with TPPs via open APIs. TPPs include Payment Initiation Service Providers (PISPs), such as Sofort in Germany, IDeal in the Netherlands and Trustly in Sweden, and Account Information Service Providers (AISPs) that aggregate customer information from multiple accounts and make it accessible from a single portal. Identification of the end-user in XS2A (Access to account) must be solved on a European basis. Identification could be solved by using eID Hubs, such as Signicat.

E-commerce gateways play an integral role in online payments as they help connect merchants to acquirers and processors. Over the years, these providers have accelerated digital commerce by providing secure solutions to accept both traditional payments (like debit and credit cards) and alternative payment methods (like PayPal and iDeal). With the availability of open APIs through PSD2, existing gateway providers—such as Global Collect, Ogone and Adyen—can leverage on their existing merchant relationships to offer PISP or AISP services. This will enable repositioning of the gateway providers within the payments value chain and open up new revenue potential.

- **PISPs:** XS2A will cut out the "middleman" in electronic payments by allowing merchants to use a customer's account details to initiate a payment directly from the bank. From the customer standpoint, this puts the shop, mobile app or online service at the forefront of the transaction, relegating the bank to the role of invisible PSP. But these services need better security.
- **AISPs:** XS2A will enable consolidation of information from multiple accounts and multiple banks, giving consumers real-time visibility into cash flow and payment transactions in one place. This will give AISPs access to a data goldmine for cross-selling and personalization of offers that threaten to undermine the bank's customer relationships. But for the consumer, there needs to be more protection of the data and how it is used.

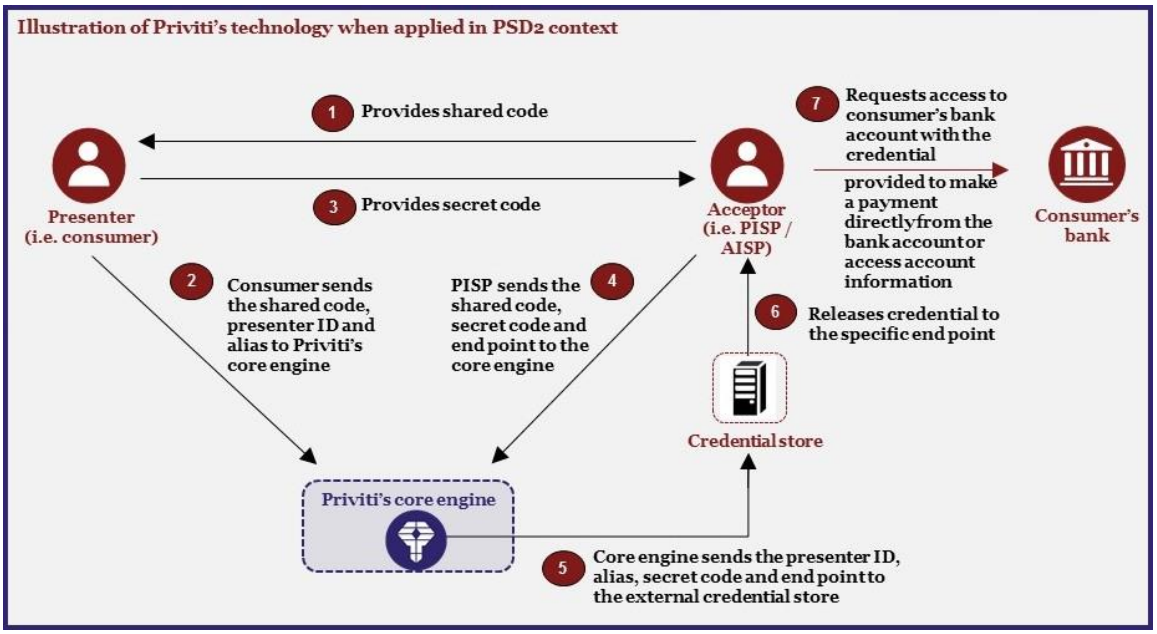


Source: Meontrust

To make electronic payments safer, PSD2 introduces enhanced security measures (including Strong Customer Authentication, with some exceptions based on context) to be implemented by all PSPs, including banks, payment institutions and TPPs. The technical requirements will be issued by the European Banking Authority (EBA).

Digital identity: Protected by Priviti

With the need for enhanced security measures, there is an exciting opportunity for a third-party entrant who provides a strong authentication mechanism that is agnostic to the provider and easily accessible and usable for the consumer. This is the aim of Priviti: to provide strong authentication between the AISP/PISP and the consumer, giving the consumer more peace of mind in the transaction. Priviti becomes a security gateway to consolidated services and account verification, protecting the digital identity of the consumer and aiding the transaction verification process.



Source: Priviti

Priviti sits between the AISP and the consumer, allowing a more secure transaction where the security is more transparent to the user. Priviti could also sit between the PISP or PSP/bank and the consumer, authenticating both the transaction and the user. Per the GDPR, a controller is the entity that determines the purpose and means for processing personal data. By consequence, in the case of the third parties stipulated in the PSD2 both are controllers, as they alone determine what will happen with the personal data, and how it occurs.

With the GDPR, third parties processing the payment information will need to receive consent from the natural person. Financial institutions as we know them today will also ask consent from the natural person to give the third parties access to the financial account of the natural person. Double consent will thus be necessary by the requirements of the PSD2. Keep in mind that the GDPR not only stipulates general requirements to protect the personal data, but also provides specific requirements about the way consent is obtained and how the controller should document that consent was in fact obtained. This is also useful for digital identity in other institutions, such as government, for issuance of documents such as passports, health care records or tax returns, and for payments such as welfare or social security.

The Constantia Institute

Priviti: Financial use case examples

There are several use cases that show the value of Priviti to both the consumer and the financial service provider in the banking transaction:

- ✓ As an enabler to share account information with third party services while establishing a new PSP relationship (adding a payment service provider);
- ✓ Combined with aggregator / gateway for pre-authorising payment permissions;
- ✓ Assisting in account management within a financial institution for multiple consumer accounts;
- ✓ Changing authorization codes in case of loss of card or hardware token; or
- ✓ Disabling accounts or revoking access once the relationship is terminated for consumer peace of mind and definitive closure.

Competitive advantage

The mission of Priviti is to be the global leader in digital identity by providing best-in-class secure authentication technology to Priviti partners for their customers' deployment. Priviti's product vision of delivering a globally trusted service which, through user authentication, allows an individual to release credentials securely through its messaging service. This service provides a simplified means of accessing customer information in a secured and trusted way, releasing access to a Presenter's bank information, to a permitted party, for a specific purpose and time.

Why is this enhanced process different than other solutions currently available in the market? This is not token-based, it is developed based on secure shared code, and Priviti has a central role as the authenticator, having created a platform of trust. Priviti provides a unique combination of push-based dual channel authentication and built-in "credential hub" functionalities to deliver a more secure and versatile solution that can be employed across a broad range of industry applications utilising API authentication.

Dual authentication now occurs with a pull-based authentication where the user first provides credentials to the third party and subsequently authenticates the transaction via other forms of notification, such as SMS. In an approach with elements that are comparable to both blockchain and public key infrastructure, the quality of authentication with Priviti is different as it is dual channel and to both parties in the transaction. Dual access with secure shared code provides authentication that is:

- Time stamped
- Irrevocable
- Secure

Priviti has designed and patented a Dual Channel Authentication (DCA) system which has an equally innovative backend infrastructure that offers seamless, secure payment transaction times that meets and exceeds regulatory requirements.

The Constantia Institute

Summary

Banks cannot afford to wait and see what the PSD2 legislation will mandate them to do. PSD2/XS2A opens new opportunities to aggregate services, create more distribution channels and share information with partners (who might have otherwise been competitors). By migrating to API-centric partner integration, banks can manage and use multiple interaction channels consistently therefore creating new revenue streams by using APIs to securely access partner services. Banks need to start reacting with open APIs and trusted third-party authentication providers to ensure they are not relegated to "plumbing" in the new payments world. Given that the EBA requirements for strong authentication will depend on the nature of the transaction, an agile security implementation strategy, particularly for identity federation, is a must. A solution such as Priviti that assists with authentication will help the banks manage the underlying account management and payment processing capabilities that the banks would otherwise have to pay to build and operate.