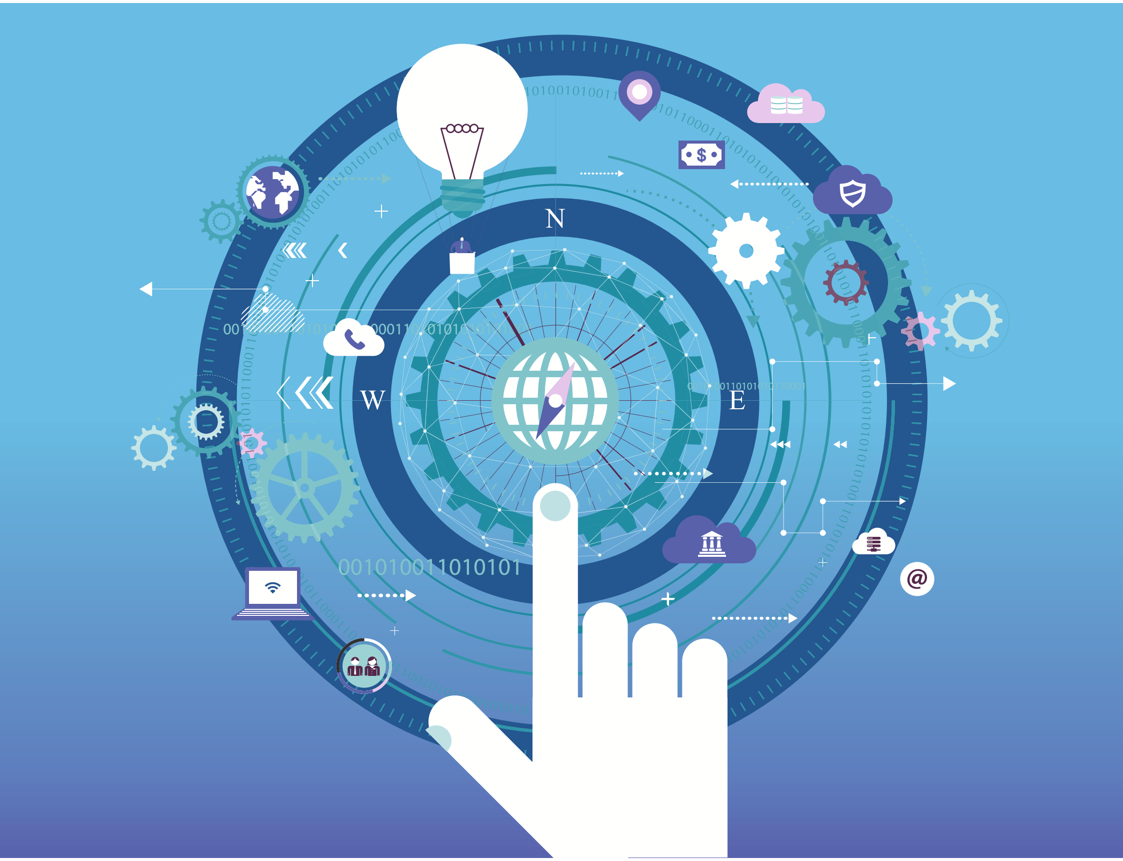
ZORP
API GATEWAY

Implementation of PSD2 Regulatory Technical Standards using Zorp technology



BALASYS

What is PSD2?

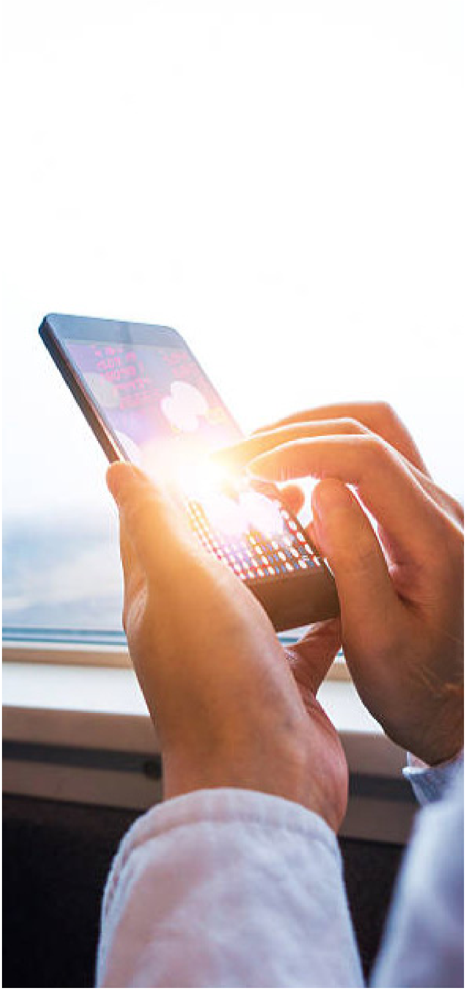
PSD2 is the second edition of the European Union’s Financial Services Directive, which is likely to turn the entire industry upside-down in the EU and even beyond. Its impact is rather wide, ranging from how we pay online - what information we see and what security tools should we use while we pay - to the extent what services of which businesses can be used and at what costs. Compliance with the requirements of PSD2 depend upon serious investment from both existing and new players of the market.

Although the old players may not be happy with the new terms, this regulation opens the channel for new entrants, new business models, as well as currently unknown services. Which is basically a positive news for society.

What changes?

PSD2 breaks down the banks' monopoly on customer data. The new regulation allows, even almost compels that traders, such as FMCG companies have access to account data with customer approval and withdraw money from their account in real time without the need for an intermediary service provider (eg. Visa, MasterCard, PayPal , etc.).

PSD2 also allows customers to exchange their online user interfaces optionally, such as web bank and mobile apps, offered by the banks. These expectedly rapidly spreading new applications will be able to handle all accounts of bank customers, even if these are kept in different banks. Companies that develop these apps are not necessarily considered as financial service providers, therefore small businesses can also enter the market with lower entry barriers.



Another important achievement of PSD2 is that it places greater emphasis on users' secure online identification.

What is RTS?

Regulatory Technical Standards are actually a collection of specifications of the regulatory implementation of technology, which prescribes the rules of communication between the parties. While PSD2 basically contains the most general principles, the RTS provides more accurate recommendations and specifications. Another peculiarity of RTS is that it can be used in all EU Member States without the need to be transposed into local law.

What is Zorp API Gateway?

Zorp API Gateway is an application-level transparent proxy which is perfectly capable of ruling network traffic that flows through it. This means that it can log, interpret, validate, filter and overwrite any element of even an encrypted network communication through the APIs. This all-know and omnipotent characteristic is exactly what banks need when they open their systems for third-party applications following the laws.

What is SCA?

Strong Customer Authentication is one of the main principles of RTS, which is designed to ensure an enhanced level of security for the payer client when making electronic payments. SCA will be used in many cases when the customer has an electronic access to his account; pays electronically; or perform any other transaction electronically which may be targeted by abuse. SCA clearly requires **two-factor authentication**, which must be two of the following three main types: 1, what the user knows (eg. password); 2, what the user owns (eg. mobile phone); 3, what identifies the user (eg. fingerprint). In addition, SCA requires the use of a unique (pseudonymous) **transaction ID code** that dynamically links the payee, the amount, and the transaction. PSD2 requires **full compensation** for all innocent users in case SCA was not applied in the event of a loss.

RTS also provides many exceptions for SCA for convenient and smooth payment:

- Online payment of less than EUR 30. Unless the cumulative amount exceeds EUR 100 or the number of consecutive micro transactions reaches five.
- Non-contact payment below 50 EUR. Unless the cumulative amount exceeds EUR 150 or the number of consecutive micro transactions reaches five.
- Unattended Payment Terminals in Transport.
- Online transaction for a trusted beneficiary.
- In case of inter-company transactions, in compliance with a strictly regulated protocol.
- In case of online information request SCA use is adequate up to 90 days.
- In all other cases where the abuse rate is lower than a certain reference value

The role of the Zorp API Gateway in delivering PSD2 RTS / SCA

Zorp has a strong authentication and authorization capability that enables Zorp API Gateway to fully integrate existing databases, such as LDAP, PAM, AD or RADIUS. In this solution, complex authentication methods can be used, and multifactor authentication is also available. The latter feature is offered as a native Zorp service and as well as through an integrated solution developed by third-party. Both password and strong authentication technologies (S/Key, SecureID, X.509, ...) are supported. Additionally, Zorp technology is also suited for supporting legacy systems, therefore authentication and authorization functionality can be easily implemented for devices that are no longer supported by others.

This solution has a very strong logging and log collecting capability, which can provide tamper proof evidence of a customer authentication level required by Community law. The highly developed logging capability can be an indispensable tool of testing security updates for newer and newer API integrations.

What is CSC?

Common and Secure Communication is the other key principle of RTS. This is responsible for stimulating competition and innovation on the market of financial transactions, by creating two new market players: the Payment Initiation Service Provider (PISP) and the Account Information Service Provider (AISP). The term which includes them both is Third-party Payment Service Provider (TPP). By the CSC banks are called Account Servicing Payment Service Provider (ASPSP).

CSC regulates how customer account information is shared between banks (ASPSPs) and new fintech entrants (TPPs). CSC sets strict requirements for both parties: TPPs can have access to account information or initiate a payment transaction solely with the explicit consent of their customers. The ASPSPs are required to operate a secure communication channel for the TPPs to provide service.

CSC describes two permitted ways of communicating between ASPSPs and TPPs: 1 through a dedicated communication interface (API); 2 through the online banking interface.

The PSD2 API is prescribed to provide at least the same level of availability and performance as the traditional online interface, without any artificial barriers. ASPSP must offer back-up access if the API is unavailable for any reason. In case of strict compliance with safety criteria the latter may be waived.

The use of the online banking interface by TPPs is only permitted by CSC if it is used clearly distinguishably from normal use of the interface, with the approval and knowledge of the user.

The role of the Zorp API Gateway in delivering PSD2 RTS/CSC

1. Logging:

PSD2 RTS/CSC has very strict expectations regarding the bank APIs' logging. Balasys has nearly 20 years of experience in the development of log management and perimeter protection technologies. Based on these expertise Zorp API Gateway has powerful log creation, generation and log collection capabilities. The solution is, among other things, suitable for reliable logging of data access through all APIs with timestamping. The generated log files are safely stored, indexed and to be accessed by the supervisory authorities without delay.

The Zorp API Gateway can generate log files based on the following parameters: IP, certificate, target micro service, client, content, debug logging, audit, compliance, etc ...

2. Access control:

The Zorp API Gateway provides advanced access control functions that enables to define the range of available API calls in detail, even at the security border point at user level, as it is required by PSD2 RTS/CSC.

The solution is capable of API call validation, in-depth message analysis, and the interpretation of JSON and XML files. Content filtering makes it possible to access only permitted formats and content through the gateway, eliminating a significant number of threats.

3. Data protection:

By using this product, it can be guaranteed that, communication is carried out through secure encrypted channels, in accordance with PSD2 RTS / CSC, enforcing TLS / SSL and data encryption. Timestamped and signed messages guarantee the intactness of the data. There is also a possibility that external services only access encrypted files – through the gateway encryption.

By using this method, the cloud-based external services are also safe to use. Zorp's data manipulation capability enables the anonymization or pseudonymization of sensitive data that promotes compliance with various privacy standards (such as GDPR). Data may thus be transferred anonymously to third parties (for security or business analysis purposes).

4. Availability:

PSD2 RTS imposes a very high, practically constant availability for banks. Zorp can not only provide high availability for itself, but also for the entire system, as the solution has advanced load balancing (traffic control) functionality. This feature of Zorp API Gateway allows periodic peak loads to be handled easily, because traffic can be evenly distributed between micro services. Additionally, in case of overload, Zorp enables the running of ongoing transactions while rejecting new requests with standard messages without publishing system information.

Entry into force

Although, PSD2 entered into force on 13 January 2018, and in February the European Parliament and the Commission endorsed the RTS, the latter will only enter into force in September 2019. During the transition period the rapid propagation of APIs cannot be expected and also temporary exemption can be requested for strong authentication. Nevertheless, what can motivate states and market players to implement the legislation quickly, is the process of 'passporting' that allows a lawful TPP fintech company operating in a EU Member State to operate freely in all EU countries, even in those countries where PSD2 has not yet been transposed to national law.