certSIGN

PSD2 & Open Banking

PSD2. General Considerations.

EU Directive 2015/2366 on payment services in the internal market (PSD2 Directive), is designed to regulate payment services and payment service providers throughout the EU and European Economic Area (EEA) and to ensure transparency and fair competition within the payment industry. This EU Directive requires that all transactions to be handled through secure channels and all data to be protected with respect to authenticity and integrity.

For users, payment transactions will become more convenient, cheaper and safer. Both banks and payment service providers must invest more in the security of their digital services.

The PSD2 Directive adds challenging elements that determine the change of the bank business model:

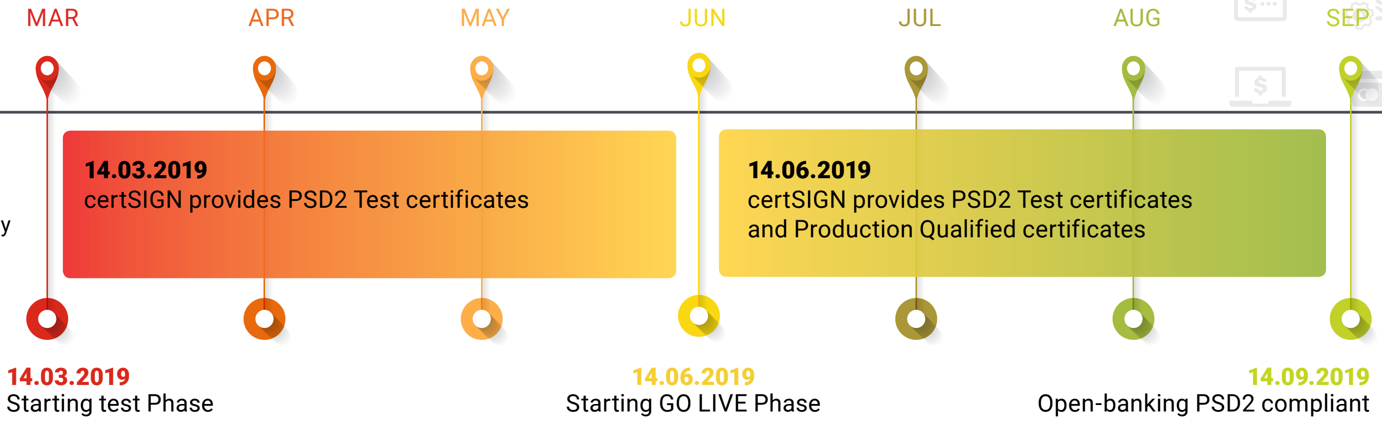
Impact for Banks

- Identifying the Third Party Financial Services Providers (TPPs)
- Strong Customer Authentication (SCA)
- Enhanced Customer Protection
- A dedicated interface (API) handling communication with TPPs
- Integration of API within core system
- Stress testing of bank systems

PSD2 & Open Banking

PSD2. Timeline.

Technical availability and testability of the so-called „open banking” concept must be established from Spring 2019. PSD2-Open banking time-line (The regulatory technical standard 2018/389 of PSD2, Article 30) is:


MAR
APR
MAY
JUN
JUL
AUG
SEP
14.03.2019
certSIGN provides PSD2 Test certificates
14.06.2019
certSIGN provides PSD2 Test certificates and Production Qualified certificates

14.03.2019
Starting test Phase

14.06.2019
Starting GO LIVE Phase

14.09.2019
Open-banking PSD2 compliant

TESTING PHASE 14.03.2019 - 14.06.2019

certSIGN provides PSD2 Test certificates

BANKS (as Account Servicing Payment Service Providers ASPSPs)

- A bank test system (test API) must be available to allows third-party providers (even if do not have a license yet), to use test certificates provided to identify themselves and to access test accounts;
- Testing facility should be made available no later than 14th of March 2019 or before the target date for market launch of the API
- Banks must document the interface and provide to licensed TTPs (at no charge); a documentation summary should be available on their website;
- Banks should prove that they had performed a test phase of at least three months before the change is implemented;
- No sensitive information should be shared through the testing facility.

THIRD-PARTY PROVIDERS (TPPs like PSP, AISP)

- Can apply for free test certificates in order to review their own system and its compatibility with the interface(s) of the banks, and to optimize it if required (even without an NCA license);
- Their own identity will be confirmed by means of a qualified website certificate;
- PSPs should document emergency situations; this documentation should be provided to NCA on request.

National Competent Authority (NCA)

- should ensure that ASPSPs comply at all times with the obligations related to the interface (s) that they put in place;
- starts to license TTPs.

OPEN-BANKING GO LIVE 14.06.2019 - 14.09.2019

certSIGN provides PSD2 Test certificates and Production Qualified certificates

BANKS (as Account Servicing Payment Service Providers ASPSPs)

- Go live with banks systems: banks open their live system with real customer accounts to licensed third-party providers, through the tested API, in similar conditions with correspondent services provided before the change;
- The bank may also require the additional use of a QSEAL to protect signed data from modification (depending on risk associated with the transaction);
- The bank should define transparent KPIs and SL targets for API provided to the TPPs (Art. 32/2);
- The bank monitors the availability and the performance of the dedicated interfaces;
- On 14th of September Banks need to comply with PSD2: banks operating in the EU will be required to provide third-party providers (TPPs) access to accounts in real-time, and to provide an interface (API) that is secured by qualified website certificates (QWACs) for this purpose.

THIRD-PARTY PROVIDERS (TPPs like PSP, AISP)

- After at least three months of testing activities, TPPs will be able to access real customer accounts, using real certificates;
- To use the bank interface (API), third-party providers require a NCA license for the access rights;
- TPP requires a QWAC to secure its communication, to identify itself to the bank as the holder of an NCA license;
- Starting on 14th of September 2019 TPPs need to comply with PSD2: access to client accounts in real-time.

National Competent Authority (NCA)

- Provides licenses to TTPs before they are accessing banks API (production);
- Should ensure that the provision of payment initiation services and account information services is not prevented;
- Monitors and stress- tests banks interfaces, performance indicators and targets.

PSD2 & Open Banking

PSD2 & eIDAS

The regulatory technical standard 2018/389 of PSD2, Article 34.1 requires that, for the purpose of identification, payment service providers rely on eIDAS Qualified Website Authentication Certificate (QWAC) and/or a eIDAS Qualified Electronic Seal Certificate (QSealC).

PSD2 is associated with eIDAS EU regulation focused on enhancing trust in electronic transactions among citizens, businesses and public authorities cross-borders. Under the law, only Qualified Trusted Service Providers (QTSPs) can provide qualified trust services and appear on the Trust List of their country of operation. If an entity is not on this list, it cannot provide qualified trust services. eIDAS requires that each EU member state maintains a Trust List of the providers and services that have received qualified status in their country.

The Qualified Website Authentication Certificate (QWAC) allows both parties (Banks and Payment Service Providers) to identify each other and build a secure channel to operate transactions. This secure channel protects the confidentiality, authenticity and integrity of the data sent over the channel. The approach is suitable when traversing a single network path between payment service providers that are communicating.

The Qualified Electronic Seal Certificate (QSealC) allows sealing of all content, including all data and transaction requests and confirmations. This protects the authenticity and integrity of the sent payload. This approach is suitable when traversing multiple network paths between communicating payment service providers.

Both types of certificates providers must be validated using the European Members States Trusted Lists.

certSIGN

PSD2 & Open Banking

CERTSIGN'S PSD2 RELATED PRODUCT AND SERVICES

PSD2 Qualified certificates

certSIGN is a Qualified Trust Service Provider (QTSP) and provides PSD2-specific Qualified Seal and Web Server Authentication Certificates (for test and production phases) for Financial Institutions (Account Servicing Payment Service Providers - ASPSP) and Third-Party Financial Service Providers (TPP) that meet the eIDAS and PSD2 requirements.

certSIGN issues certificates as specified in the „PSD2 Regulatory Technical Standards (RTS) for strong customer authentication and common and secure open standards of communication", according to the ETSI TS 119 495 standard.

certSIGN is currently the only Romanian provider listed in the EU Trusted List as a Qualified Trust Service Provider authorized to issue QWACs and QSEALs and among the few European QTSPs issuing PSD2 compliant certificates.

Consultancy services

Based on its experience as QTSP and long-term expertise in PKI, certSIGN offers consultancy services for technical and compliance assistance for the implementation of the PSD2 Directive requirements.

Verification services

Each time they receive a request, banks must validate the authenticity of the sender. This means that, for the digital certificate used to protect the transaction, it must be verified:

- if the Trust Service Provider (TSP) is Qualified (against European Trust List)
- if the certificate is technically correct and has not expired
- if the certificate is Qualified
- if the certificate contains all the required PSD2 information
- if the certificate has not been revoked since it was issued.

certSIGN provides the software required to verify that certificates used by Third Party Providers TPPs are compliant with eIDSAS & PSD2 requirements, and providing banks with the confirmation of identity of TPPs that access bank system through the dedicated interface.

References

The Revised Payment Services Directive (PSD2 - Directive (EU) 2015/2366)
The RTS for Strong Customer Authentication & Common Secure Communications Under PSD2
Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC
PRETA Open Banking Europe: Understanding Internet Security & eIDAS Certificates
Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)