



# Certificates for PSD2.

What companies, banks and FinTechs need to know to use electronic certificates and seals.

## What are the regulatory requirements for third-party providers that want to access bank accounts or bank account data?

To operate in the EU, third-party providers need a license from their National Competent Authority (NCA). The license type determines the access rights of the third-party provider, which it requires to access account data through the bank interface within the scope of its business model.

## What are the technical requirements for third-party providers and banks?

In order to gain access to bank accounts as a third-party provider, a company must identify itself with one or more certificates during automated access. Likewise, banks use a certificate to identify themselves to the accessing payment service providers. The certificate serves as a "company ID" in electronic business transactions. Article 34 of the RTS (EU 2018/389) requires the use of qualified website certificates (QWACs) or qualified electronic seal certificates (QSEALs).

## Where can third-party providers and banks obtain electronic certificates in accordance with PSD2 requirements?

The required electronic certificates are issued by a qualified trust service provider registered in the EU, such as D-TRUST GmbH, a subsidiary of Bundesdruckerei GmbH. The application process takes place online. The NCA license must have been issued to the payment service provider prior to this. If a bank wants to act as a third-party provider in order to access accounts with other banks, it also needs a QWAC and possibly a QSEAL. If the bank already possesses a full banking license, it does not require separate licensing from its National Competent Authority.

## When will certificates in accordance with PSD2 requirements be available?

On 17 May 2019, Bundesdruckerei introduced live certificates (QWAC and QSEAL) in line with PSD2 requirements in order to

ensure that banks can meet the deadline to benefit from an exemption from the fallback option under Article 33(6) of Regulation EU 2018/389. To test the interface, validated test certificates are also available. In accordance with EU 2018/389 Article 30 (5), banks must start the prescribed test operation with test certificates from 14 March at the latest.

## Does the application for a qualified website certificate in accordance with PSD2 follow a defined, binding process?

Yes, the application for qualified website certificates follows a defined process. For real certificates, a third party must first apply for authorization as a payment service provider with its National Competent Authority (NCA). After the NCA license has been granted, the certificate can be issued by D-TRUST GmbH. It is possible to apply even before authorization. CRR credit institutions and banks that also want to act as payment service providers do not require additional approval and can apply for all types of certificates.





## Do I have to submit an application to my NCA to receive test certificates?

Test certificates do not require an NCA license. D-TRUST issues test certificates without further examination.

## What are the differences between the various certificate types and which one do I need?

There are qualified website certificates (QWACs), qualified electronic seal certificates (QSEALs) and extended validation (EV) certificates. The QWAC registers the identity of the accessing company and secures the communication channel (transport level). The seal protects the signed data from modification. It makes subsequent changes visible and documents the identity of the accessing company (application layer). Article 34 of the RTS (EU 2018/389) requires third-party providers to use QWACs or QSEALs. The EBA recommends the use of both a QWAC and a QSEAL. The Standard NextGen PSD2 of the Berlin Group requires a QWAC. Banks can identify themselves using a QWAC or EV certificate. In the latter case, the EBA recommends a QWAC.

## How does the process of creating and delivering the test certificates work?

Since July 2019, test certificates can be purchased from Bundesdruckerei: [bundesdruckerei.de/en/Ordering](https://bundesdruckerei.de/en/Ordering). The key for QWAC test certificates is generated at the customer end. You can upload the Certificate Signing Request (CSR) during the request process. The certificate

will then be delivered in an e-mail (PKCS#12 with PIN code). The key for QSEAL test certificates (on a seal card) is generated at D-TRUST. A seal card on which your key is stored will be sent to you by post.

## How are test certificates integrated?

Test certificate users receive the required issuer and root certificates from Bundesdruckerei which they must then enter into the certificate store as trustworthy certificates. These certificates are designed for use with the test system only.

## Where can I obtain the root certificate from D-TRUST or other QTSPs for the live operation?

D-TRUST's root certificate can be downloaded directly from D-TRUST's website. More information can be found in the [Certification Practice Statements \(CPS\)](#). To obtain the root certificates of all eIDAS QTSPs, you first need the [EU Trusted List of QTSPs](#). This list contains all root certificates.

## What is the meaning of the abbreviations PSP\_AI, PSP\_PI, PSP\_AS and PSP\_IC on the certificate?

The PSD2 regulation (EU 2015/2366) recognizes different roles (entitlements) for payment service providers. The aforementioned abbreviations are defined in ETSI standard 119 495. Common roles are account information service (PSP\_AI) and payment initiation service (PSP\_PI). Other roles include account services (PSP\_AS) and issuing of card-based payment instruments (PSP\_IC). Payment service providers may apply for one or more of these roles with their National Competent Authority (NCA), after which they will be registered and can be issued certificates with these roles.

