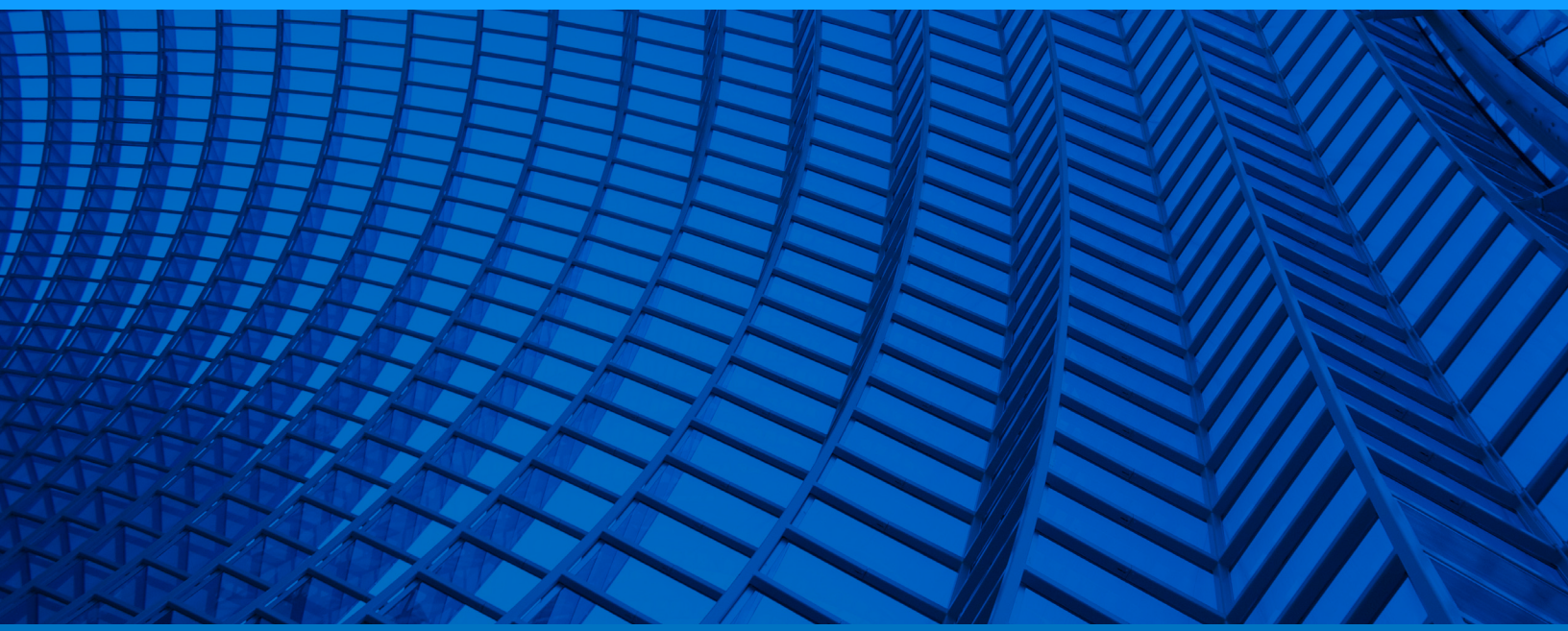
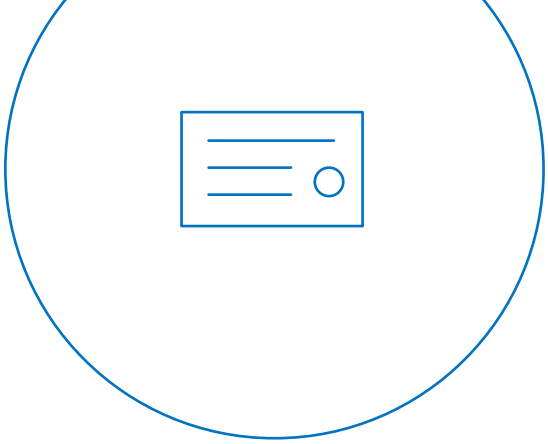
What you need to know about PSD2 certificate compliance

A new regulatory standard in the EU mandates additional security measures for banks and Payment Service Providers, including the use of special Qualified digital certificates.





What is the revised Payment Services Directive (PSD2)?

As part of a long-time effort to increase the security, privacy and reliability of electronic payments crossing the borders of EU nations, the European Commission developed the revised Payment Services Directive (EU Directive 2015/2366, also known as PSD2) which came into effect in January 2018.

The directive is intended to…

• Contribute to a more integrated and efficient European payments market

• Create a level playing field for Payment Service Providers (PSPs) across the EU

• Make electronic payments more secure

• Provide more consistent consumer protection

PSD2 covers many facets of the electronic payments market, but notably introduces enhanced privacy and online security measures that must be implemented by banks and PSPs doing business in the EU.

What are eIDAS Qualified Certificates?

eIDAS (EU Regulation 910/2014) is a set of EU regulatory standards that defines requirements for digital certificates, the validation of their holders' identity, and the operation of the Qualified Trust Service Providers (TSPs) that issue them.

Certificates issued by Qualified TSPs in accordance with eIDAS standards are known as "Qualified Certificates," and provide special status in certain legal and regulatory contexts across the EU.

Why do I need Qualified certificates for PSD2?

Under PSD2 digital certificates are used to identify banks and PSPs, to verify the roles for which they are licensed, to encrypt communications, and, in some cases, to provide tamperproof seals on data or transactions.

Due to the sensitivity of financial services transactions, the PSD2 Regulatory Technical Standards (RTS) specify that only eIDAS certificates issued by a Qualified Trust Service Provider (TSP) may be used for the identification of PSPs.

Is DigiCert + QuoVadis accredited to provide Qualified Certificates?

DigiCert's European subsidiary QuoVadis is a eIDAS Qualified TSP operating in the Netherlands and in Belgium, as well as in Switzerland.

What kind of Qualified certificates are issued by DigiCert + QuoVadis?

DigiCert + QuoVadis issues Qualified Certificates for e-signature and e-seal, Qualified Web Authentication Certificates (TLS/SSL), and Qualified Time Stamps. DigiCert + QuoVadis also provide the specific Qualified Certificates required for PSD2.

What types of certificates do I need for PSD2 compliance?

PSD2 specifies two types of digital certificate for secure communications:

- **Qualified Certificate for Website Authentication** (QWAC) used with Transport Layer Security (TLS) protocol such as is defined in IETF RFC 5246 or IETF RFC 8446 to protect data in peer-to-peer communications and to identify who controls the end points.
- **Qualified Certificate for Electronic Seals** (QSealC) create e-seals used to protect data or documents using standards such as ETSI's PAdES, CAdES or XAdES, and assert their origin from a legal entity.

What types of certificates do I need for PSD2 compliance?

Each type of PSD2 Certificate offers different protection depending on the use case.

	QWAC TLS/SSL	**e-Seal / QSealC**
Where is it used?	Identifies end points, protects data during communication	Identifies origin of document or data and makes it tamperproof in communication and storage
What are the security features?	Confidentiality, authentication, and integrity	Authentication and integrity
Provides legal evidential value for transactions?	No	Yes under eIDAS
Is data protected when passed through an intermediary?	Protects in direct peer-to-peer communications	End-to-end, even if passed through intermediary

The EBA's RTS describes different scenarios that PSPs can consider in their use of certificates for secure communication. For example, Article 34 of the RTS describes a secure option with parallel protection of both the payment transactions data and their communications channels:

- Using QWACs to assert the PSPs' identity and roles to each other and to communicate securely using TLS encryption; and
- Using QSealCs to ensure that the application data submitted originates from a particular PSP and has not been tampered with.

Banks providing APIs for real-time access to customer information by licensed third-party vendors will typically specify which PSD2 certificates they require to be used by PSPs. PSPs will typically require both.

Are there special requirements for private key management?

Though in many cases eIDAS requires the use of a Qualified Signature Creation Device (QSCD) to protect private keys, special cryptographic hardware is not required for either QWAC or QSealC certificates under PSD2.

Instead, PSD2 allows Advanced e-seals under the eIDAS definitions, created using the QSealC certificates.

What are the timelines for PSD2 Certificates?

Phase 1: March 2019

- In this initial phase, a PSD2 test environment must be provided in which even non-licensed third-party vendors can identify themselves with test certificates and access test accounts.
- DigiCert + QuoVadis are able to issue test PSD2 Certificates, with simplified registration, for these purposes.

Phase 2: June 2019

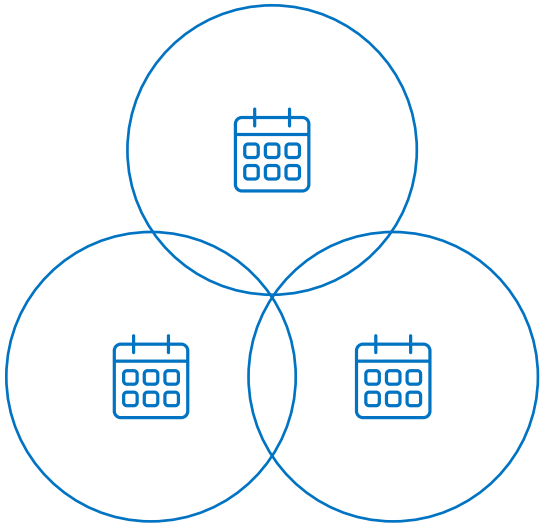
- In this phase, banks must open their live system with real customer accounts for licensed third-party vendors with production PSD2 Certificates.
- Financial institutions that are unable to meet these deadlines must implement a fallback solution according to EU 2018/389 Article 33 (6).
- DigiCert + QuoVadis are ready to issue production Qualified PSD2 Certificates, which involve more detailed validation of identity information of the PSP and its Authorised Representatives.

Phase 3: September 2019

- Financial institutions are committed to full, live operation in compliance with PSD2 requirements.

How can I get a test PSD2 Certificate?

Test certificates may be obtained by filling out the form on www.digicert.com/psd2-compliance-security-solutions/. These certificates are created from a test hierarchy that must be added to the test systems' trusted root certificate store.



What will I need to register for a PSD2 Certificate?

In general, the validation steps for PSD2 Certificates are similar to those required for Extended Validation (EV) TLS. However, the eIDAS Qualified standards place additional emphasis on identity verification, which typically requires face-to-face validation of the certificate holder's official documents by the Qualified TSP.

Because PSD2 Certificates are issued to companies, the individual whose identity will be validated must be a known Authorised Representative for the company, such as a director noted in an official Trade Register. That Authorised Representative may then approve other personnel, such as IT staff, to interact with the TSP in managing the digital certificate lifecycle.

NOTE: The face-to-face validation process for Authorised Representatives may be facilitated using accredited European Notaries.

The PSP applicant will need to identify the country of their National Competent Authority (NCA) or financial regulator. The Qualified TSP will confirm the PSP's license and roles before issuing the certificates.

The PSP roles defined in the ETSI TS 119 495 standard for PSD2 include:

- PSP_AI Account information service
- PSP_PI Payment initiation service
- PSP_AS Account services
- PSP_IC Issuing of card-based payment instruments

Is there a standard relevant to PSD2 Certificates?

A new ETSI standard (ETSI TS 119 495) builds on the other eIDAS Qualified standards to define the TSP policies and certificate profiles that meet PSD2 RTS requirements. This includes defining fields for certificates to identify:

- the National Competent Authority (NCA) or financial regulator where the PSP is registered
- the Authorisation Number issued to the PSP by the NCA
- the regulated PSD2 roles for which the PSP is licensed by the NCA

DigiCert proposed Ballot SC17 in the CA/Browser Forum which enables PSD2 and other organisational identifier fields to be added to Extended Validation (EV) TLS certificates.

For more information, contact DigiCert + QuoVadis
at +31 30 232 43 20 or email Psd2@quovadisglobal.com

digicert® + QuoVadis