

# Was Sie über die Compliance Ihrer Zertifikate mit der zweiten Zahlungsdiensterichtlinie wissen müssen

Neue regulatorische Bestimmungen in der EU fordern von Banken und Zahlungsdienstleistern zusätzliche Sicherheitsmaßnahmen, darunter die Verwendung besonderer qualifizierter digitaler Zertifikate.





## Hintergrund: die zweite Zahlungsdiensterichtlinie (PSD2)

Im Rahmen langfristiger Bemühungen, Sicherheit, Datenschutz und Zuverlässigkeit bei grenzüberschreitenden elektronischen Zahlungen zwischen EU-Ländern zu verbessern, hat die Europäische Kommission die novellierte Zahlungsdiensterichtlinie (EU-Richtlinie 2015/2366, auch als PSD2 für „Payment Services Directive“ bekannt) verabschiedet, die bis Januar 2018 in nationales Recht umgesetzt werden musste.

Ziel der Richtlinie ist es, ...

- den europäischen Zahlungsmarkt weiter zu integrieren und effizienter zu machen,
- in der gesamten EU gleiche Bedingungen für Zahlungsdienstleister (ZDL) zu schaffen,
- die Sicherheit elektronischer Zahlungen zu erhöhen,
- einen konsistenteren Verbraucherschutz zu gewährleisten.

Die PSD2 betrifft viele Aspekte des elektronischen Zahlungsmarktes, führt aber insbesondere verschärfte Maßnahmen für den Datenschutz und die Online-Sicherheit ein, die von Banken und ZDL mit Geschäftsaktivitäten in der EU umgesetzt werden müssen.

## Was sind eIDAS-qualifizierte Zertifikate?

Die eIDAS-Verordnung (EU-Verordnung 910/2017) legt den Rechtsrahmen für und definiert die Anforderungen an digitale Zertifikate, die Validierung der Identität des Zertifikatsinhabers und die Arbeitsweise der qualifizierten Vertrauensdiensteanbieter (VDA), die Zertifikate ausstellen.

Von qualifizierten VDA in Übereinstimmung mit der eIDAS-Verordnung ausgestellte Zertifikate werden „qualifizierte Zertifikate“ genannt und haben in bestimmten rechtlichen und regulatorischen Zusammenhängen EU-weit einen besonderen Status.

## Warum erfordert die PSD2 qualifizierte Zertifikate?

Gemäß der PSD2 werden digitale Zertifikate genutzt, um Banken und ZDL zu identifizieren, die Rollen, für die sie lizenziert sind, zu verifizieren, elektronische Nachrichten zu verschlüsseln und in manchen Fällen Daten bzw. Transaktionen mit einem manipulationssicheren Siegel zu versehen.

Wegen der Sensibilität von Finanztransaktionen bestimmen die technischen Regulierungsstandards (TRS) der PSD2, dass zur Identifizierung von ZDL nur von einem qualifizierten Vertrauensdiensteanbieter (VDA) ausgestellte eIDAS-Zertifikate verwendet werden dürfen.

## Ist DigiCert + QuoVadis für die Ausstellung qualifizierter Zertifikate zugelassen?

QuoVadis ist ein Tochterunternehmen von DigiCert und ein eIDAS-qualifizierter VDA mit Niederlassungen in Belgien, Deutschland, Großbritannien, den Niederlanden und der Schweiz. QuoVadis stellt für Kunden in ganz Europa PSD2-Zertifikate aus.



## Welche Art qualifizierter Zertifikate werden von DigiCert + QuoVadis ausgestellt?

DigiCert + QuoVadis stellt qualifizierte Zertifikate für elektronische Signaturen und Siegel, qualifizierte Zertifikate für die Authentifizierung im Internet (TLS/SSL) und qualifizierte Zeitstempel aus. Außerdem bietet DigiCert + QuoVadis die speziellen qualifizierten Zertifikate gemäß der PSD2 an.

## Welche Zertifikatstypen sind zur Einhaltung der PSD2 erforderlich?

Es werden zwei digitale Zertifikatstypen für die sichere Datenübermittlung genannt:

- **Qualifizierte Zertifikate für die Website-Authentifizierung** (QWAC = Qualified Website Authentication Certificate) werden zusammen mit dem TLS-Protokoll (Transport Layer Security) wie etwa in IETF RFC 5246 oder IETF RFC 8446 definiert verwendet, um Daten bei der Peer-to-Peer-Übertragung zu schützen und zu identifizieren, wer die Endpunkte steuert.
- **Qualifizierte Zertifikate für elektronische Siegel** (QsealC) dienen zur Erstellung elektronischer Siegel, mit denen Daten oder Dokumente geschützt werden und ihr Ursprung von einem legitimen Absender bestätigt wird. Dabei werden Standards wie etwa PAdES, CAdES oder XAdES gemäß ETSI verwendet.

## Welche Zertifikatstypen sind gemäß der PSD2 erforderlich?

Die beiden PSD2-Zertifikatstypen bieten unterschiedlichen Schutz, je nach Anwendungsfall.

|                                                                         | QWAC TLS/SSL                                                   | Elektronisches Siegel/QsealC                                                                                                 |
|-------------------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Einsatzgebiet                                                           | identifiziert Endpunkte, schützt Daten während der Übertragung | identifiziert den Ursprung des Dokuments bzw. der Daten und schützt vor Manipulation während der Übertragung und Speicherung |
| Sicherheitsfunktionen                                                   | Vertraulichkeit, Authentifizierung und Integrität              | Authentifizierung und Integrität                                                                                             |
| Rechtliche Nachweiskraft für Transaktionen                              | nein                                                           | ja, gemäß eIDAS-Verordnung                                                                                                   |
| Schutz der Daten bei Weiterleitung über eine zwischengeschaltete Stelle | schützt bei direkter Peer-to-Peer-Übertragung                  | End-to-End, auch bei Weiterleitung über eine zwischengeschaltete Stelle                                                      |



Der TRS der Europäischen Bankenaufsichtsbehörde (EBA) beschreibt verschiedene Szenarien, die ZDL bei der Nutzung von Zertifikaten für die sichere Kommunikation in Erwägung ziehen können. Zum Beispiel wird in Artikel 34 des TRS eine sichere Option beschrieben, bei der parallel sowohl die Transaktionsdaten von Zahlungen als auch die Übertragungskanäle geschützt werden:

- QWAC zur gegenseitigen Bestätigung der Identität und der Rollen der ZDL und zur sicheren Kommunikation mittels TLS-Verschlüsselung und
- QsealC zur Gewährleistung, dass die übermittelten Anwendungsdaten von einem bestimmten ZDL stammen und nicht manipuliert wurden.

Banken, die APIs von lizenzierten Drittanbietern für den Echtzeitzugriff auf Kundendaten bereitstellen, geben im Normalfall an, welche Zertifikate die ZDL gemäß der PSD2 verwenden müssen. ZDL werden in der Regel beide benötigen.

## Gibt es spezielle Anforderungen für das Management privater Schlüssel?

Zwar verlangt die eIDAS-Verordnung zum Schutz privater Schlüssel in vielen Fällen die Nutzung einer qualifizierten Signaturerstellungseinheit (QSEE), doch ist spezielle kryptographische Hardware gemäß der PSD2 weder für QWA- noch für Qseal-Zertifikate erforderlich.

Vielmehr lässt die PSD2 fortgeschrittene elektronische Siegel gemäß den Definitionen der eIDAS-Verordnung zu, die mittels Qseal-Zertifikaten erstellt wurden.

## Welcher Zeitplan gilt für die Einführung von PSD2-Zertifikaten?

### Phase 1: März 2019

- In dieser Anfangsphase muss eine PSD2-Testumgebung bereitgestellt werden, in der auch nicht lizenzierte Drittanbieter sich mit Probezertifikaten identifizieren und auf Testkonten zugreifen können.

- DigiCert + QuoVadis kann zu diesem Zweck in einem vereinfachten Registrierungsverfahren PSD2-Zertifikate zur Probe ausstellen.

### Phase 2: Juni 2019

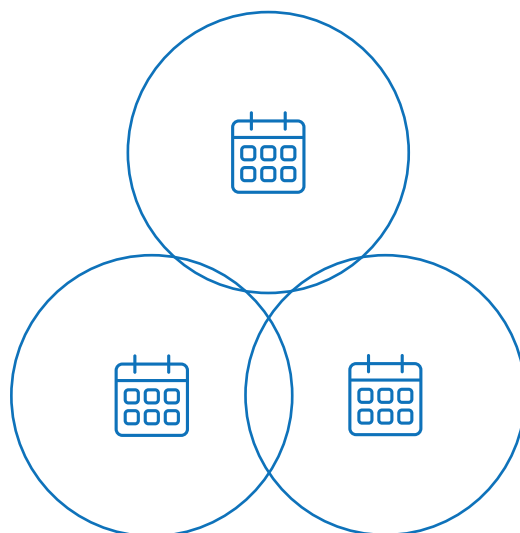
- In dieser Phase müssen Banken ihre Live-Systeme mit echten Kundendaten für lizenzierte Drittanbieter mit uneingeschränkten PSD2-Zertifikaten öffnen.
- Finanzinstitute, die diese Fristen nicht einhalten können, müssen eine Ausweichlösung gemäß der delegierten Verordnung (EU) 2018/389 Artikel 33 (6) implementieren.
- DigiCert + QuoVadis ist in der Lage, uneingeschränkte qualifizierte PSD2-Zertifikate auszustellen, die eine ausführlichere Validierung der Angaben zur Identität des ZDL und seiner bevollmächtigten Vertreter umfassen.

### Phase 3: September 2019

- Finanzinstitute sind verpflichtet, einen vollständigen, realen Service in Einklang mit den Anforderungen der PSD2 bereitzustellen.

## Wie erhält man ein PSD2-Zertifikat zum Testen?

Probezertifikate können auf unserer Website angefordert werden. Füllen Sie dazu das Formular unter [www.digicert.com/psd2-compliance-security-solutions/](http://www.digicert.com/psd2-compliance-security-solutions/) aus. Diese Zertifikate werden von einer Testhierarchie erstellt, die im Testsystem zum Speichern vertrauenswürdiger Root-Zertifikate hinzugefügt werden muss.



## Was ist zur Registrierung für ein PSD2-Zertifikat notwendig?

Im Großen und Ganzen sind die Validierungsschritte für PSD2-Zertifikate ähnlich denen für TLS mit Extended Validation (EV). Allerdings legen die Vorgaben für eIDAS-qualifizierte Zertifikate besonderen Nachdruck auf die Identitätsprüfung, was üblicherweise die persönliche Validierung der offiziellen Dokumente des Zertifikatsinhabers durch den qualifizierten VDA erfordert.

Da PSD2-Zertifikate an Unternehmen ausgestellt werden, muss die Person, deren Identität überprüft wird, als bevollmächtigter Vertreter des Unternehmens bekannt sein, zum Beispiel ein in einem offiziellen Handelsregister eingetragener Geschäftsführer. Dieser bevollmächtigte Vertreter kann dann andere Mitarbeiter, zum Beispiel aus der IT-Abteilung, dazu berechtigen, mit dem VDA beim Lebenszyklusmanagement der digitalen Zertifikate zusammenzuarbeiten.

Hinweis: Der Prozess der persönlichen Validierung bevollmächtigter Vertreter kann durch Hinzuziehen europäischer Notare erleichtert werden.

ZDL, die PSD2-Zertifikate beantragen, müssen das Land ihrer zuständigen nationalen Behörde oder Finanzaufsichtsbehörde angeben. Der qualifizierte VDA prüft vor dem Ausstellen der Zertifikate die Lizenz und die Rollen des ZDL.

In der Norm ETSI TS 119 495 für die PSD2 sind u. a. die folgenden ZDL-Rollen definiert:

- PSP\_AI Kontoinformationsdienst
- PSP\_PI Zahlungsauslösedienst
- PSP\_AS Kontoführung
- PSP\_IC Ausgabe kartengebundener Zahlungsinstrumente

## Gibt es eine Norm für PSD2-Zertifikate?

Eine neue ETSI-Norm (ETSI TS 119 495) definiert aufbauend auf den anderen Normen zur eIDAS-Verordnung die VDA-Richtlinien und Zertifikatsprofile, die die TRS-Anforderungen gemäß der PSD2 erfüllen. Dies umfasst die Definition von Feldern für Zertifikate mit den folgenden Angaben:

- die zuständige nationale Behörde oder Finanzaufsichtsbehörde, bei der der ZDL registriert ist,
- die dem ZDL von der zuständigen nationalen Behörde zugewiesene Zulassungsnummer,
- die regulierten PSD2-Rollen, für die der ZDL von der zuständigen nationalen Behörde lizenziert wurde.

DigiCert hat im CA/Browser Forum Ballot SC17 eingebracht. Damit können Felder für PSD2- und andere Unternehmenskennzeichen zu TLS-Zertifikaten mit Extended Validation (EV) hinzugefügt werden.



Weitere Informationen erhalten Sie von DigiCert + QuoVadis  
unter +31 30 232 43 20 oder schreiben Sie an [Psd2@quovadisglobal.com](mailto:Psd2@quovadisglobal.com).

© 2019 DigiCert, Inc. Alle Rechte vorbehalten. DigiCert ist eine eingetragene Marke von DigiCert, Inc. in den USA und in anderen Ländern.  
Alle anderen Marken und eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber.