BUNDESDRUCKEREI

Zertifikate für PSD2.

Was Unternehmen, Banken und FinTechs für den Einsatz von elektronischen Zertifikaten und Siegeln jetzt wissen müssen.

Welche regulatorischen Voraussetzungen müssen Drittanbieter erfüllen, die auf Konten oder Kontoinformationen der Banken zugreifen möchten?

Für ihre Geschäftstätigkeit innerhalb der EU benötigen Drittanbieter eine Lizenz der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder ihrer zuständigen nationalen Aufsichtsbehörde. Der Lizenztyp bestimmt die Zugriffsrechte des Drittanbieters, die dieser im Rahmen seines Geschäftsmodells für den Zugriff auf die Kontodaten über die Bankenschnittstelle benötigt.

Welche technischen Voraussetzungen benötigen Drittanbieter und Banken?

Um als Drittanbieter Zugang zu Bankkonten zu erhalten, müssen sich Unternehmen beim automatisierten Zugriff mit einem oder mehreren Zertifikaten identifizieren. Auch Banken weisen sich mittels Zertifikat gegenüber den zugreifenden Zahlungsdienstleistern aus. Das Zertifikat gilt als „Unternehmensausweis" im elektronischen Geschäftsverkehr. Artikel 34 der RTS (EU 2018/389) schreibt die Verwendung von qualifizierten Website-Zertifikaten (QWACs) oder qualifizierten Zertifikaten für elektronische Siegel (QSiegel) vor.

Wo bekommen Drittanbieter und Banken ein elektronisches Zertifikat nach PSD2-Vorgaben?

Die nötigen elektronischen Zertifikate werden von einem in der EU gelisteten qualifizierten Trust Service Provider (QTSP), z. B. bei der D-TRUST GmbH, einer Tochter der Bundesdruckerei GmbH, herausgegeben. Die Beantragung erfolgt online. Die Lizenz muss dem Zahlungsdienstleister zuvor durch die BaFin oder seiner nationalen Aufsicht erteilt worden sein. Wenn eine Bank als Drittanbieter agieren will, um ihrerseits auf Konten anderer Banken zuzugreifen, benötigt sie ebenfalls ein QWAC und ggf. ein QSiegel. Eine separate Lizensierung bei der BaFin oder der zuständigen nationalen Finanzaufsicht ist nicht erforderlich, wenn sie bereits eine Vollbanklizenz besitzt.

Ab wann sind Zertifikate nach den PSD2-Vorgaben verfügbar?

Echtzertifikate nach den PSD2-Vorgaben werden bei der D-TRUST GmbH rechtzeitig im Mai 2019 verfügbar sein, so dass Banken die Frist zur Vermeidung der Fallback-Lösung gemäß EU 2018/389 Artikel 33(6) einhalten können. Für den Test der Schnittstelle können Testzertifikate ohne Validierung ab sofort bereitgestellt werden. Testzertifikate mit Validierung sind ab März erhältlich. Ab spätestens 14. März müssen Banken gemäß EU 2018/389 Artikel 30(5) den vorgeschriebene Testbetrieb mit Testzertifikaten starten.

Gibt es für die Beantragung eines qualifizierten Website-Zertifikats gemäß PSD2 einen definierten, verbindlichen Prozess?

Ja, die Beantragung eines qualifizierten Website-Zertifikats erfolgt nach einem definierten Prozess. Für produktive Zertifikate muss ein Drittanbieter erst einen Antrag auf Zulassung als Zahlungsdienstleister bei der BaFin oder seiner zuständigen nationalen Finanzaufsichtsbehörde (National Competent Authority, NCA) stellen.

Nach der Erteilung der BaFin-Lizenz kann die Zertifikatsausstellung bei der D-TRUST GmbH erfolgen. Eine Beantragung ist auch bereits vor der Zulassung möglich. CRR-Kreditinstitute und Banken, die auch als Zahlungsdienstleister auftreten wollen, benötigen keine zusätzliche Zulassung und können alle Zertifikatstypen beantragen.

Ist ein Antrag bei der BaFin auch für Testzertifikate zu stellen?

Für Testzertifikate gibt es keine Lizenzverpflichtung durch die BaFin. Die D-TRUST erstellt Testzertifikate ohne weitere Prüfungen.

Wo liegen die Unterschiede im Einsatz der Zertifikatstypen und welche sind einzusetzen?

Es gibt qualifizierte Website-Zertifikate (QWACs), qualifizierte Zertifikate für elektronische Siegel (QSiegel) und Extended-Validation-Zertifikate (EV-Zertifikate). Das QWAC belegt die Identität des zugreifenden Unternehmens und sichert den Kommunikationskanal (Transportschicht). Das Siegel schützt die signierten Daten vor Veränderungen. Es macht nachträgliche Änderungen sichtbar und dokumentiert die Identität des zugreifenden Unternehmens (Anwendungsschicht). Artikel 34 der RTS (EU 2018/389) schreibt Drittanbietern die Verwendung von QWAC oder QSiegel vor. Die Empfehlung der European Banking Authority (EBA) ist, ein QWAC und ein QSiegel einzusetzen. Im Standard NextGenPSD2 der Berlin Group ist ein QWAC verpflichtend vorgesehen. Eine Bank kann sich ihrerseits durch ein QWAC oder EV-Zertifikat ausweisen, auch in diesem Fall empfiehlt die EBA ein QWAC.

Wie ist der Prozess zur Erstellung und Auslieferung der Testzertifikate?

Testzertifikate werden formlos per E-Mail an PSD2@bdr.de beantragt. Die Schlüsselerstellung erfolgt bei der D-TRUST. Die Auslieferung von QWAC und QSeal erfolgt ebenfalls per E-Mail (PKCS#12 mit PIN code).

Wie erfolgt die Integration der Testzertifikate?

Die Nutzer der Testzertifikate erhalten von der Bundesdruckerei ein Stammzertifikat, das als vertrauenswürdiges Zertifikat in den Zertifikatsspeicher einzutragen ist – dieses Zertifikat ist nur für das Testsystem zu verwenden.

Woher bekomme ich das Root-Zertifikat der D-TRUST und anderer QTSPs für den Produktivbetrieb?

Das Root-Zertifikat der D-TRUST kann direkt auf der Website der D-TRUST heruntergeladen werden, die Informationen dazu finden Sie in den Certification Practice Statements (CPS). Um die Root-Zertifikate aller eIDAS QTSPs zu erhalten, benötigen Sie zunächst die EU Trusted List aller QTSPs. Diese Liste enthält alle Root-Zertifikate.

Was bedeuten die Rollen PSP_AI, PSP_PI, PSP_AS und PSP_IC im Zertifikat?

Die PSD2 Regulierung (EU 2015/2366) unterscheidet verschiedene Rollen (Berechtigungen) für Zahlungsdienstleister. Im ETSI-Standard TS 119 495 sind die genannten Abkürzungen definiert. Die gebräuchlichen Rollen sind Kontoinformationsdienst (account information, PSP_AI) und Zahlungsauslösedienst (payment initiation, PSP_PI). Daneben gibt es noch Kontoführung (account servicing, PSP_AS) und Kartenausgabe (issuing cards, PSP_IC). Zahlungsdienstleister können die Zulassung für eine oder mehrere dieser Rollen bei ihrer nationalen Aufsichtsstelle beantragen, erscheinen dann mit diesen Rollen im Register und können Zertifikate mit diesen Rollen ausgestellt bekommen.