bevh | basics

computop
the payment people

- Q&A -

Starke Kundenauthentifizierung im Rahmen der Umsetzung der PSD2

Version | Stand: 1.1 | 15.07.2019
Ansprechpartner: Birgit Janik ✉info@bevh.org ☎ 030-40 36 751-71

Historie: 15.07.2019 V1.1

Die im Januar 2016 in Kraft getretene Payment Services Direktive 2 (PSD2) soll eine europaweit einheitliche Rechtsgrundlage für Online-Zahlungen schaffen, unabhängigen Zahlungsdienstleistern den Zugang zu Informationen sichern, die für die sichere Abwicklung der Zahlung notwendig sind, und mehr Sicherheit im Online-Payment ermöglichen. Mit Stichtag 14. September 2019 müssen Onlinehändler die PSD2 durch Einführung der sogenannten Starken Kundenauthentifizierung (strong customer authentication, SCA) im E-Commerce-Vertriebskanal umsetzen. Dieses Q&A beantwortet grundlegende Fragen. Gemeinsam mit unserem Preferred Business Partner Computop ergänzen wir das Papier laufend und nehmen auch Ihre Fragen gerne auf.

---

1. Was wird in der PSD2 geregelt?

Die Payment Services Directive 2 (Zahlungsdiensterichtlinie 2) wurde im Oktober 2015 verabschiedet und ist eine Regelung zur Regulierung von Zahlungsdiensten und -dienstleistern, die von der Europäischen Kommission als EU-Richtlinie verabschiedet wurde. Sie ist eine Weiterentwicklung der ersten PSD und gilt dementsprechend in der gesamten Europäischen Union sowie dem Europäischen Wirtschaftsraum. Sie soll mehr Sicherheit und höhere Transparenz im Zahlungsverkehr schaffen sowie für niedrigere Einstiegshürden für Zahlungsdienste und einen fairen Wettbewerb sorgen.

Die Regulierung betrifft im Wesentlichen zwei Bereiche: die Zahlungsbranche und den Verbraucher. Für die Zahlungsbranche schafft sie klare Regeln, die dafür sorgen sollen, den Wettbewerb innerhalb der EU zu stärken, indem sie die Position von Zahlungsdienstleistern

Impressum Herausgeber: Bundesverband E-Commerce und Versandhandel Deutschland e.V., Friedrichstr. 60, 10117 Berlin
V.i.S.d.P.: Christoph Wenk-Fischer (Hauptgeschäftsführer), info@bevh.org

verbessert. Sie beendet das Monopol der Banken auf Kontoinformationen und erlaubt es Drittanbietern, sogenannte Third Party Provider (TPP), Kunden Zugriff auf deren eigene Kontoinformationen zu geben. Darüber hinaus schafft sie die Voraussetzungen, die es TPP erlauben, Bezahlvorgänge direkt auszulösen, ohne dass eine Bank direkt in den Vorgang involviert ist.

Zwei neue TPP sind in der PSD2 reguliert: der Payment Initiation Service Provider (PISP), auch Zahlungsauslösedienst genannt, und der Account Information Service Provider (AISP), auch Kontoinformationsdienst genannt. Um diesen Anbietern ihre Arbeit zu ermöglichen, müssen Banken ihre APIs (Application Programming Interfaces) denjenigen öffnen, die sie für diese regulierten Dienstleistungen anfragen und die gemäß der Vorgaben reguliert sind.

Für Verbraucher und Händler soll sich zudem die Sicherheit bei Transaktionen erhöhen, indem sie eine starke Authentifizierung (Strong Customer Authentication/SCA), auch Zwei-Faktor-Authentifizierung (2FA) bei E-Commerce-Transaktionen verlangt. Daraus ergeben sich strengere Regelungen für Kartenzahlungen und für die Betrugsprävention.

2. Welche Zahlverfahren werden von der PSD2 erfasst?

Alle Zahlverfahren für elektronische Fernzahlungen.

3. In welchem Zusammenhang steht die „Starke Kundenauthentifizierung“ (SCA) mit der PSD2?

Die Erfordernis nach SCA (Strong Customer Authentication) /Zwei-Faktor-Authentifizierung (2FA) ist Bestandteil der Zahlungsrichtlinie PSD2. SCA wird immer dann gefordert, wenn ein Nutzer eine elektronische Zahlung auslösen möchte und verlangt für die Authentifizierung mindestens zwei der drei Faktoren Wissen, Inhärenz und Besitz. SCA findet bei E-Commerce-Zahlungen Anwendung, die von Kundenseite angestoßen wurden. Eine SCA fragt also mindestens zwei der Faktoren ab. Kann sie der Nutzer korrekt vorlegen, wird die Zahlung genehmigt.

Der Faktor Wissen wird mit einem Passwort oder einer PIN abgedeckt, die nur der Konto- oder Karteninhaber kennt.

Der Faktor Besitz kann das Smartphone des Users sein. Das Eigentum muss der Nutzer dann über eine Verifizierungsnachricht innerhalb einer App auf dem Smartphone beweisen. In der Praxis findet diese Herangehensweise beispielweise in Banken-Apps statt. Hierbei fragt die Bank eine TAN ab, die direkt in der Banking-App erzeugt und angezeigt wird. Es handelt sich hierbei zwar um ein sogenanntes Einmalpasswort/One Time Password (OTP), doch bei diesem Vorgang ist das mobile Endgerät, auf das es geschickt wird, der entscheidende Faktor: Besitz.

Nach PSD2 sind SMS-TANs übrigens sind nicht mehr zulässig. PSD2 schreibt vor, dass die Banken die Kontrolle über die Kanäle wahren müssen. Bei über SMS verschickten TANs ist diese Voraussetzung nicht gewährleistet. In TAN-Apps generierte TANs hingegen erfüllen die Standards.

Der Faktor Inhärenz wird durch biometrische Daten abgedeckt. Dabei authentifiziert sich der

User beispielsweise auf seinem Smartphone über einen Fingerabdruck-, Gesichts- oder Iris-Scan.

4. **Betrifft die SCA alle Arten von Distanzhandel, oder gibt es Einschränkungen nach Zahlart, Vertriebsweg oder Zielgruppe (z.B. B2B)?**

   Die SCA ist verpflichtend für die Auslösung elektronischer Zahlungen und für den Zugang zu Anwendungen, die elektronische Zahlungen auslösen und/oder Zugang zu Kontoinformationen ermöglichen. Eine Unterscheidung nach Handelsform oder Vertriebsweg ist nicht vorgesehen. Inwiefern eine Zahlart der SCA unterliegt, hängt davon ab, ob eine Kartenzahlung involviert ist bzw. ob der Verbraucher die Möglichkeit hat, die Zahlung nach Warenerhalt auszuführen oder zu widerrufen.

   B2B-Zahlungen unterliegen der SCA genauso wie B2C-Zahlungen, mit einer Ausnahme: wenn die Zahlungen in einem typischerweise nur von Unternehmen benutzten Prozess ausgeführt werden, der nicht auf die Authentifizierung einer Einzelperson setzt und eine Behörde die Vergleichbarkeit der Sicherheit mit den Maßstäben der PSD2 bestätigt hat.

5. **Wer ist rechtlich verantwortlich für die Umsetzung der Regelungen im Shop: Nur die (e-)Geldinstitute/PSP (gemäß Verweisen in den RTS SCA), oder auch die Händler selbst?**

   Verantwortlich für die Umsetzungen sind die Zahlungsdienstleister, die die Zahlungsauslösung ausführen bzw. den Zahlungspflichtigen authentifizieren. In der Regel die Anbieter der Zahlarten, also die Acquirer oder alternativen Zahlarten. Sie sind verpflichtet, den Prozess der SCA bereitzustellen.

   Händler sind nur verantwortlich, wenn sie selbst die Zahlungsauslösung vornehmen, zum Beispiel über eine Schnittstelle zu den Banken. Dann müssen sie sicherstellen, dass die Maßnahmen der Bank zur SCA in den Prozess eingebunden sind.

6. **Kann nur ein PSP die SCA für Händler übernehmen?**

   Nein. Grundsätzlich ist festzuhalten, dass für die SCA immer die Zahlungsart zuständig ist. Der PSP übernimmt die SCA nicht. Lediglich bei der Lastschrift könnten der Händler oder der Zahlungsdienstleister eine SCA durchführen, allerdings ist sie derzeit für Lastschriften nicht erforderlich. Ein weiterer Sonderfall sind Instant Payments. Hierbei wären der PSP oder der Händler Zahlungsauslöser und müssten die Authentifizierungsverfahren der über eine Schnittstelle angebundenen Kundenbank ausführen sowie als Zahlungsauslösedienst reguliert sein.

   Festzuhalten ist, dass der Händler keine Entscheidungsfreiheit hinsichtlich der SCA hat. Sie ist zwingende Voraussetzung im elektronischen Zahlungsverkehr. Der Händler bindet den SCA-Prozess lediglich ein. Die Abfrage findet technisch gesehen nie auf der Webseite des Händlers statt, sondern wird dort nur über ein iframe eingebunden.

7. **Wer speichert welche Daten?**

Die Speicherung der Authentifizierungsdaten hängt vom verwendeten Verfahren ab. Bei der Verwendung von **In-App-TAN** erfolgt keine Speicherung, da die TAN für jede Zusendung neu erzeugt werden. Die **biometrischen Daten** werden nur im Gerät des Besitzers in einem geschützten Bereich gespeichert. Es erfolgt keine Übertragung von biometrischen Daten, zur Authentifizierung wird lediglich ein nicht rückentschlüsselbarer Hashwert abgeglichen. **PIN und Passwörter** werden wie bisher auf geschützten Servern der Zahlungsdiensteanbieter gespeichert. Sensible Daten wie **Kartennummern** dürfen nur PCI-zertifizierte Unternehmen speichern, viele Händler vertrauen dabei auf Payment Service Provider wie Computop. Der Handel kann dabei ganz auf die Speicherung der Originalnummern verzichten und speichert nur **Pseudokartennummern**, die im Fall des Datenverlustes keine Zahlung ermöglichen. Weitere Transaktionsdaten sind ebenfalls bei PSPs gespeichert sowie bei den Banken.

8. **Wie erfolgt die Zwei-Faktor-Identifizierung im Onlineshop?**

Das hängt vom gewählten Zahlarten-Anbieter ab. Apple Pay beispielsweise authentifiziert Online-Einkäufe über ein verbundenes iPhone mit biometrischer Erkennung. Online-Überweisungsverfahren verwenden häufig eine TAN aus einer geschützten App auf dem Smartphone. Erfolgt der Online-Einkauf auf einem Mobilgerät eines nachgewiesenen Besitzers, sind auch weiterhin als zweiter Faktor eine PIN oder ein Passwort möglich.

9. **Wie und wo erfolgt das „dynamic linking“ (Verknüpfung mit Betrag und Zahlungsempfänger)?**

Das Dynamic Linking erfolgt bei der kontoführenden Bank des Kunden und wird im Zuge der Authentifizierung an den Kunden übertragen.

10. **Was sind „trusted beneficiaries“ und wie erfolgt das Whitelisting?**

Vertrauenswürdige Zahlungsempfänger, sogenannte Trusted Beneficiaries können vom User innerhalb seines Online-Banking-Portals gekennzeichnet werden, sofern die Bank diesen Service anbietet. Dazu legt er eine Liste mit vertrauenswürdigen Empfängern an, die sogenannte Whitelist. Dieser Vorgang, das Whitelisting, sorgt dafür, dass Transaktionen an die gelisteten Empfänger nicht stark authentifiziert werden. Eine SCA findet lediglich einmalig statt, um die angelegte Whitelist oder den jeweiligen Trusted Beneficiary zu bestätigen. Alle folgenden Transaktionen an den Empfänger werden ohne SCA realisiert, sofern die Transaktionen keine allgemeinen Auffälligkeiten aufweisen.

11. **Micropayments: Gibt es analog zum stationären Handel Grenzen (z.B. 50 Euro), bis zu denen auf eine SCA verzichtet werden kann?**

Von der SCA befreit sind bei Fernzahlungen Kleinbeträge bis zu 30 Euro, solange seit der letzten SCA Transaktionen von insgesamt 100 Euro Volumen oder mehr als fünf Zahlungen ohne Anwendung der SCA nicht überschritten wurden. Allgemeine Voraussetzung auch für diese Ausnahme ist, dass die Transaktion keine offensichtlichen Risikomerkmale aufweist, wie z.B. eine gesperrte Kartennummer.

12. Müssen wiederkehrende Zahlungen (Abo-Modell) jeweils authentifiziert werden?

Bei wiederkehrenden Zahlungen erfolgt die Zahlungsauslösung durch den Händler, es handelt sich um sog. MIT (Merchant Initiated Transactions). Diese sind laut EBA (European Banking Authority) von der SCA befreit, wenn die ursprüngliche Autorisierung des Abonnements gemäß SCA authentifiziert wurde.

Diese Regelung zu wiederkehrenden Zahlungen schließt auch Abweichungen bei den Zahlungsbeträgen oder -zeitpunkten ein, sofern diese in einem vom Kunden erwartbaren Bereich liegen. Nicht abgedeckt ist die Zahlungsauslösung mit Card on File (COF), bei der der Händler dem Kunden eine vorhandene Kartennummer vorblendet, die der Kunde nur bestätigt, denn hier ist der Kunde der letztliche Zahlungsauslöser.

Vereinbarungen zu wiederkehrenden Zahlungen, die bereits vor Wirksamwerden der PSD2 getroffen wurden, gelten weiter und erfordern keine nachträgliche Starke Authentifizierung.

13. Unter welchen Bedingungen kann nach Transaktionsrisikoanalysen auf SCA verzichtet werden?

Nach §§ 18,19 der RTS kann der Issuer auf SCA verzichten, wenn

a) die Betrugsrate für die entsprechende Art von Zahlungen (Karten bzw. Überweisungen) über die Gesamtheit des Zahlungsdienstleisters gerechnet bestimmte Werte nicht überschreitet (Tabelle),
b) die Zahlungen nicht über die zugehörigen Schwellenwerte hinausgehen und
c) keine ungewöhnlichen Szenarien wie z.B. abweichendes Zahlungsverhalten oder Ort mit hohem Risiko festgestellt werden.

	Referenzbetrugsrate (%) für:	
Ausnahmeschwellenwert	Kartengebundene elektronische Fernzahlungsvorgänge	Elektronische Überweisungen über einen Fernzugang
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015

14. Kann der Händler im Callcenter weiterhin Kreditkartenzahlungen abwickeln, wenn KK und CVC allein online zur SCA nicht mehr genügen (MOTO-Transaktionen)?

MOTO-Transaktionen werden in der PSD2 nicht als elektronische Transaktionen betrachtet und fallen daher nicht unter die Verpflichtungen zur SCA.

15. In welchem Zusammenhang steht SCA mit 3D Secure 2.0?

Die PSD2 erfordert in vielen Fällen eine SCA/2FA. 3D Secure (3DS) erfüllt die Anforderungen an SCA. Kreditkartenfirmen wie VISA, Mastercard, American Express und JCB nutzen die Technologie, um Missbrauch von Kreditkartendaten zu verhindern. Für den Händler reduzieren sich das Betrugsrisiko und mögliche Zahlungsausfälle. Wer als Händler 3D Secure einsetzt, erhält einen garantierten Zahlungseingang, denn wird die Transaktion trotz 3DS-Abfrage genehmigt und erweist sich dennoch als Betrug, haftet die herausgebende Bank der Kreditkarte (Issuerbank) für den Schaden.

3DS 2.0 beinhaltet eine Reihe von Verbesserungen gegenüber 3D Secure 1.0, die den Einkaufsprozess für Kunden und Händler einfacher gestalten. Wie auch schon bei dem Vorgänger identifizieren sich Onlinekäufer gegenüber ihrer Issuerbank per 3D Secure als rechtmäßige Karteninhaber. In der Version 2.0 wird die bisher statische Abfrage eines Sicherheitscodes durch eine in Echtzeit ablaufende Risikoanalyse ersetzt. Bei jeder Bestellung per Kreditkarte werden bis zu 100 Datenpunkte und damit bis zu 10mal mehr Informationen an die Issuerbank übermittelt. Die Erfassung und Weiterleitung der Daten erfolgt über das Shop-Backend des Händlers und durch den PSP. Die Übergabe der Daten findet in der gesicherten Umgebung des 3D Secure Servers statt. Wenn die anschließende Echtzeit-Risikobewertung durch den Issuer das Risiko niedrig einstuft, wird die Transaktion bewilligt. Sollte ein erhöhtes Betrugsrisiko bestehen, muss der Käufer seine Identität bestätigen.

Hinsichtlich der Fristen zu 3D Secure 2.0 ist zu beachten: Weder von Seiten des verantwortlichen Branchenverbands EMVCo noch seitens der Kreditkartengesellschaften wurde eine verbindliche Frist zur Integration des neuen Standards in Onlineshops gesetzt. Fakt ist: 3DS 2.0 selbst stellt keine gesetzlich vorgeschriebene Norm dar. Maßgeblich für den Händler ist die Frage, ob im eigenen Onlineshop bis zum 14. September 2019 ein Verfahren zur Abwicklung von Kreditkartentransaktionen bereitgestellt werden kann, welches den Maßgaben der SCA genügt.

Als Minimallösung ist hierbei auch 3D Secure 1.0 zulässig.

16. **Wie wird die SCA bei Voice-Anwendungen (Google Home, Alexa) durchgeführt?**

    Für Amazons Echo sind Zahlungen über Spracherkennung standardmäßig aktiviert. Amazon löst das Problem der Bestätigung aktuell über einen optionalen vierstelligen Code, den der Nutzer entweder vor jedem Einkauf aufsagen muss oder (sofern er seine Stimme von Alexa registrieren lässt) nur einmalig aufsagen muss und danach barrierefrei über seine Stimme einkaufen kann.

    Für Google Home ist das Einkaufen über die Stimme bisher nur in den USA freigeschaltet. Um Zahlungen zu ermöglichen, muss der Nutzer sie in der Google-Home-App auf dem Smartphone oder dem Tablet aktivieren, die Zahlmethode festlegen und dann manuell in der App die Google-Home-Geräte auswählen, die berechtigt sind, Käufe zu tätigen.

    Google erlaubt dem User zusätzlich eine optionale Bestätigung von Käufen über den Fingerabdruck auf dem Smartphone oder Tablet oder der Eingabe des Passwortes des Google-Kontos auf dem Smartphone oder Tablet.

17. **Ab September 2019 muss der Händler mit der neuen Version 2.0 der 3D Secured arbeiten, ansonsten übernimmt der Händler im Falle eins Betrugs - auch wenn die Transaktion 3D gesichert ist- die Haftung**

    Ohne 3D Secure wird eine Zahlung generell abgelehnt, die Version 3DS 1.0 reicht jedoch weiterhin als Minimallösung aus. Mittelfristig ist allerdings damit zu rechnen, dass die Einreichung mit 3DS 2.0 verbindlich wird.

18. **Ist das Thema 3D-Flex aufgrund der neuen PSD2 Regelung nicht mehr möglich, oder muss die 3D Secure nur ab einem gewissen Betrag abgewickelt werden (50 Euro?)?**

    Der Händler kann weiterhin Zahlungen unter 30 Euro ohne 3D Secure an den Issuer senden. Der Issuer muss allerdings prüfen, dass seit der letzten 2FA-Authentifizierung mit dieser Karte nicht mehr als 100 Euro in Beträgen unter 30 Euro ausgegeben wurden oder nicht mehr als 5 Zahlungsvorgänge mit Kleinbeträgen vollzogen wurden. Trifft eines dieser Merkmale zu, muss er von sich aus eine 2FA ausführen. Eine völlige Befreiung von Kleinbeträgen ist nicht mehr möglich.

    Beträge oberhalb von 30 Euro können nicht mehr ohne 3DS eingereicht werden. An die Stelle einer festen, vom Händler eingestellten Grenze kann allerdings die Ausnahme auf Basis der Transaktionsrisiko-Analyse (TRA) treten. Dabei kalkuliert der Acquirer die Betrugswahrscheinlichkeit einer Transaktion und kann unterhalb bestimmter Grenzwerte das Risiko übernehmen. Der Issuer hat in diesem Fall die Wahl, diesen Vorschlag zu akzeptieren oder auf eine 2FA zu bestehen und diese auszuführen.

19. **Ist es richtig, dass der Kunde sich bei seinen Banken auf eine „Whitelist“ setzen kann, um grundsätzlich für 3D Secure Verfahren ausgeschlossen zu werden? Bei Betrugsfällen haftet er; wie soll dies umgesetzt werden?**

    Ein Kunde kann sich nicht selbst auf die Liste der vertrauenswürdigen Empfänger setzen, sondern nur Händler, denen er vertraut. Eine Generalbefreiung für alle Händler ist nicht möglich, die Händler müssen einzeln benannt werden. Zudem kann seine Bank im Einzelfall weiterhin das 3DS durchführen, wenn sie Hinweise auf ein erhöhtes Risiko der entsprechenden Transaktion hat. Generell sind die Banken außerdem nicht verpflichtet, eine Whitelist zu führen.

20. **Erfolgt die Anmeldung bei PayPal zukünftig ebenfalls via 2FA und wer ist für diese Umstellung zuständig; PayPal oder der Händler?**

    PayPal wird nach der neuen PSD2 Richtlinie in Zukunft nicht mehr über eine reine Passwortanmeldung (TAN) funktionieren. Die Umstellung auf die Zwei-Faktor-Authentifizierung, die PayPal bereits jetzt als freiwillige Lösung anbietet, wird mit Wirksamwerden der PSD2 verpflichtend werden. Sie obliegt PayPal und nicht dem Händler.

21. **Die EBA hat am 21.6. eine Übergangsfrist für die PSD2 eingeräumt – haben wir jetzt mehr Zeit für die Umstellung?**

    Die Übergangsfrist bedingt bestimmte Voraussetzungen. Zunächst liegt es im Ermessen der nationalen Aufsichtsbehörden, sich dieser Ansicht anzuschließen, sie können also auch davon absehen. Die BaFin hat deutlich gemacht, dass sie sich der Auffassung der EBA anschließt. Allerdings wird keine konkrete Fristverlängerung eingeräumt, sondern lediglich „Flexibilität gewährt“. Voraussetzung dafür ist jedoch das Vorliegen eines expliziten Migrationsplans für die Umstellung auf die Starke Kundenauthentifizierung, der klar definierte Zwischenziele enthält. Händler sollten sich daher weiterhin am Umstellungsdatum 14.9. orientieren, denn eine verspätete Bereitschaft für SCA bedeutet weiterhin einen nicht rechtskonformen Zustand und bringt die Gefahr einer höheren Ablehnungsrate mit sich.

22. **Wir haben gehört, dass 3D Secure 1.0 ab dem 14.9. nicht mehr zulässig sein soll?**

    Die EBA hat klargestellt, dass 3DS 1.0 nicht an alle Anforderungen der PSD2 angepasst ist. Diese Aussage bezog sich auf das Fehlen bestimmter Formulare oder die Möglichkeit, von Ausnahmen der PSD2 Gebrauch zu machen. Zugleich gilt die Abfrage eines Passworts im E-Commerce aber weiterhin als Element des Faktors Wissen, daher kann unserer Auffassung nach die Verwendung einer Passwortabfrage zur Authentifizierung nach 3DS 1.0 weiterhin unterstützt werden, sofern die Übertragung des Passworts an den Issuer PSD2-konform geschieht. Wir empfehlen, 3DS 1.0 dennoch nur als Fallback-Lösung einzusetzen, da es in jedem Fall zur Challenge, also zur Präsentation der Passwort-Abfrage kommt und durch die fehlenden Ausnahmen zu einer geringeren Konversionsrate im Checkout führen wird. Zudem haben die Kartenmarken bereits durchblicken lassen, dass das 3DS 1.0-Protokoll auf mittlere Sicht vom Markt genommen werden wird.