

FAQs zur Starke Kundenauthentifizierung (SCA) nach der PSD2 –

November 2019

Was ist die PSD2 und was bedeutet Starke Kundenauthentifizierung (SCA)?

Die PSD2 (Zweite Zahlungsdienste-Richtlinie) wurde 2015 als Richtlinie der Europäischen Union (EU) 2015/2366 veröffentlicht. Die Richtlinie musste in jedem Land der EU bis zum 13. Januar 2018 in nationales Recht umgesetzt werden. In Deutschland wurde die PSD2 unter anderem im Zahlungsdiensteaufsichtsgesetz (ZAG) umgesetzt.

Die Starke Kundenauthentifizierung (englisch „Strong Customer Authentication“, abgekürzt „SCA“) ist eine Anforderung aus der PSD2, die festlegt, dass beispielsweise die Auslösung elektronischer Zahlungsvorgänge durch Zahler mittels Authentifizierung durch mindestens zwei voneinander unabhängige Elemente aus verschiedenen Kategorien erfolgen muss, um die Sicherheit der Zahlung zu erhöhen und das Betrugsrisiko zu reduzieren. Die SCA-Anforderungen sind am 14. September 2019 in Kraft getreten und haben in Deutschland die bisher geltenden Mindestanforderungen an die Sicherheit von Internetzahlungen abgelöst. Die aktuelle Position der Europäischen Bankenaufsichtsbehörde (EBA) ist unten angefügt.

Wer ist für die Anwendung von SCA verantwortlich?

Zahlungsdienstleister (englisch „Payment Service Providers“, abgekürzt „PSPs“) sind für die Anwendung von SCA verantwortlich. Zahlungsdienstleister sind beispielsweise Kartenherausgeber (Issuer) und Acquirer.

Die Zahlungsdienstleister müssen sicherstellen, dass Händler SCA umsetzen. Sollten Händler sich gegen die Umsetzung von SCA entscheiden, tragen sie selbst das Risiko von Verlusten, die auf betrügerische Transaktionen zurückzuführen sind, und sind möglicherweise auch (Haftungs-) Ansprüchen ihres Dienstleisters ausgesetzt.

Seit wann gelten die SCA-Anforderungen nach der PSD2?

Die SCA-Anforderungen nach der PSD2 gelten seit dem 14. September 2019. Die Europäische Bankenaufsichtsbehörde (EBA) hat in einer Opinion vom Juni 2019 jedoch die Komplexität der

First Data GmbH • www.telecash.de

Geschäftsadresse: Marienbader Platz 1 • 61348 Bad Homburg v. d. Höhe

Sitz: Bad Homburg v.d.H. • Handelsregister Amtsgericht Bad Homburg v.d.H. HRB 14567

Geschäftsführer: Jörg Brand (Sprecher), Thomas Bürger

Zahlungsverkehrsmärkte in der EU und die Herausforderungen im Zusammenhang mit der Implementierung von SCA anerkannt und nationalen Aufsichtsbehörden daher die Möglichkeit eingeräumt, dass diese Issuern und Acquiren für kartenbasierte Zahlungen begrenzte zusätzliche Zeit zur Umsetzung einräumen dürfen.

Von dieser Möglichkeit hat unter anderem die BaFin in Deutschland Gebrauch gemacht. Am 16. Oktober nun hat die EBA den nationalen Aufsichtsbehörden empfohlen, dass die Übergangsfristen spätestens Ende 2020 enden und die vollständige Implementierung der SCA-Vorgaben bis dahin abgeschlossen sein sollen. Die BaFin hat daraufhin am 17. Oktober mitgeteilt, dass sie es nicht beanstanden wird, wenn Zahlungsdienstleister mit Sitz in Deutschland Kartenzahlungen im Internet bis zum 31. Dezember 2020 auch ohne SCA ausführen. Mehr Details zur Haltung der EBA und den gesetzten Eckdaten finden Sie unter folgender Internetadresse:

<https://eba.europa.eu/documents/10180/2622242/Opinion+on+the+deadline+for+the+migration+to+SCA.pdf>

Für welche First Data TeleCash-Leistungen sind Updates betreffend SCA nötig?

First Data TeleCash bietet Händlern einige Leistungen an, die vom SCA-Erfordernis nach der PSD2 betroffen sind:

- I. Acquiring
- II. Gateway Services ("Internet Payment Gateway", abgekürzt "IPG")
- III. Transaktionsverarbeitung

Was ist EMV 3D Secure?

EMV 3D Secure ist die aktualisierte Version von 3-D Secure 1.0, die seit einiger Zeit im Rahmen von Brands wie Verified by Visa®, MasterCard SecureCode® und SafeKey by American Express® angeboten wird. EMV 3-D Secure ist eine neue Version zur Authentifizierung, deren Ziel es ist, reibungsloser, schneller und sicherer zu sein, indem sie die frühere Weiterleitung bei 3-D Secure 1.0 durch eine dynamische Brücke zwischen Issuern und Händlern ersetzt.

Unterstützt First Data TeleCash EMV 3D Secure?

First Data TeleCash unterstützt EMV 3D Secure im Internet Payment Gateway (IPG) und in den Zahlungsverarbeitungssystemen. Händler, die unser IPG nutzen, können unser integriertes Händler-Plugin über unsere gehosteten Zahlungsseiten oder über unsere Web Service API-Schnittstelle nutzen. Händler können auch ein MPI eines Drittanbieters verwenden und einfach über das IPG autorisieren. Wir möchten unseren Händlern und Zahlern dabei helfen, dass der Zahlungsvorgang unter SCA hohe Sicherheit bietet und reibungslos von Statten geht. Der korrekte Umgang mit solchen Zahlungsvorgängen, die keiner SCA bedürfen, ist ein wesentliches Element hierfür.

Was können Sie als Händler als nächstes tun?

IPG-Händler können unsere EMV 3D Secure-Lösung nutzen, bei der sie Transaktionen, die aus ihrer Sicht außerhalb des Anwendungsbereiches von SCA liegen oder für eine Ausnahme in Betracht kommen, kennzeichnen können.

Die IPG-Integrationsdokumentation für EMV 3D Secure finden Sie unter folgender Internetadresse: <https://docs.firstdata.com/org/gateway/node/456>.

Wir empfehlen Ihnen, die Dokumentation abzurufen und die überschaubaren Anpassungen an Ihrer Integration in unser IPG vorzunehmen, um EMV 3D Secure zu implementieren, bzw. sich mit Ihrem IT-Dienstleister in Verbindung zu setzen, und auf unsere Dokumentation zu verweisen, damit dieser die Updates an Ihrer Integration vornehmen kann.

Fragen zur Integration in das IPG richten Sie bitte an internet.support@telecash.de.

Allgemeine Fragen zu PSD2 SCA & EMV 3D Secure richten Sie bitte an PSD2FirstDataGermanyGmbH@firstdata.com.

Wie kann First Data TeleCash helfen, wenn Sie ein Gateway von Drittanbietern verwenden?

Wenn Sie das First Data TeleCash IPG nicht nutzen, ist es wichtig, dass Sie sich so schnell wie möglich an Ihren Gateway-Provider (oder an Ihren Zahlungsdienstleister (z.B. Acquirer)) wenden, damit Sie die Änderungen nächstmöglich vornehmen können.