Mastercard® Identity Check™ / EMV 3D-Secure

Das Betrugsrisiko verringern und unnötige Kartenzahlungsabbrüche durch optimierte Bezahlprozesse im E-Commerce vermeiden.

Antworten auf häufige Fragen und wichtige Handlungs-empfehlungen für Händler

August 2020

Das Wichtigste im Überblick

Am 14. September 2019 traten neue technische Regulierungsstandards der Europäischen Bankaufsicht in Kraft, welche die Sicherheit von Online-Transaktionen und Kundenkontenzugängen erhöhen sollen.

Die neue Richtlinie beinhaltet unter anderem die Forderung nach einer starken Kundenauthentifizierung. Bis auf die vom Gesetzgeber definierten Ausnahmen müssen dann Zahlungstransaktionen aller von der Regulierung erfassten Zahlungssysteme mit einer Zwei-Faktor-Authentifizierung abgesichert werden.

Für die Kartenzahlung hat Mastercard daher ein neues Sicherheitsprotokoll (EMV 3DS 2.1) als Standard eingeführt.

Aktuell werden, um Störungen im E-Commerce zu vermeiden, Kartenzahlungen im Internet ohne starke Kundenauthentifizierung nicht beanstandet. Diese Übergangsfrist endet am 31. Dezember 2020.

Es wird keinen weiteren Aufschub der EU-Kommission geben. Ab dem 1. Januar 2021 ist die Zwei-Faktor-Authentifizierung für alle Online-Händler verpflichtend. Daher sollten Sie am besten sofort mit der Implementierung und Testphase starten.

Was Sie jetzt tun sollten:

Erkundigen Sie sich bei Ihrem Acquirer oder Payment Service Provider,

- ob Ihre Kreditkartenzahlungs-Lösung auf EMV 3DS und Mastercard® Identity Check™ vorbereitet ist,
- welche Daten bereitzustellen sind und welche Änderungen von Ihnen vollzogen werden müssen,
- welche Ausnahmen und Sonderfälle bei Ihnen zutreffen.

EBA RTS: die Hintergründe

EBA RTS steht für die Anfang 2018 herausgegebenen Regulatory Technical Standards der EU Payment Services Directive 2 (PSD2), also die technischen Regulierungsstandards zur EU-Richtlinie zu Zahlungsdiensten der Europäischen Bankenaufsichtsbehörde.

Nach Maßgabe der EBA RTS sind seit 14. September 2019 sämtliche elektronischen Zahlungen (insbesondere E-Commerce-Zahlungen) mit einer starken Kundenauthentifizierung (Strong Customer Authentication, kurz SCA) abzusichern, sofern keine Ausnahmeregelung greift (Details siehe unten).

Händler müssen daher über das EMV 3D-Secure-Protokoll (kurz EMV 3DS oder 3D-Secure) Authentifizierungsanfragen senden, damit die Kartenherausgeber keine E-Commerce-Transaktionen ablehnen. Nach Umfragen wollen etwa 20 % der großen kartenherausgebenden Institute nach Inkrafttreten der RTS zur Einhaltung der gesetzlichen Vorlagen Transaktionen ohne starke Kundenauthentifizierung ablehnen.

Ziel der RTS ist es, über den obligatorischen Einsatz der starken Kundenauthentifizierung (SCA) für elektronische Zahlungen (hierbei insbesondere Zahlungen im Internet) und innerhalb von Apps auf Endgeräten aller Art, Betrugsversuche noch weiter zu reduzieren. Die RTS beschreiben detailliert, wann die SCA erforderlich ist und welche Ausnahmen bestehen.

Die RTS gelten für die 30 Länder des Europäischen Wirtschaftsraums (EWR), also die 27 EU-Länder sowie Norwegen, Island und Liechtenstein.

EMV 3DS: die Hintergründe

EMV 3DS ist die Weiterentwicklung des bisherigen Sicherheitsprotokolls (3DS 1.0) und stellt den neuen Branchenstandard zur Absicherung von Kartenzahlungen aller Kartensysteme (Amex, Mastercard, Visa) dar:

- Es ermöglicht den Austausch von mehr Transaktions- und Kundendaten (wie Gerätedaten, Versand- und Rechnungsadresse) und gewährleistet damit, dass Kartenherausgeber SCA-Ausnahmen anwenden und Entscheidungsprozesse sowie Betrugserkennung verbessern können.
- EMV 3DS unterstützt neue Bezahlwege, wie z. B. Zahlung innerhalb von Apps und mobile Zahlungen.
- Es deckt zusätzliche Geschäftsvorfälle ab, wie etwa:
    - registrierte Kunden, die beim Händler/Einzelhändler eine Karte hinterlegt haben und entsprechend auf der Website oder in der App nicht für jeden Einkauf erneut ihre Zahlungsinformationen angeben müssen.
    - E-Wallets z. B. die Wallets von Google oder Apple
    - Tokenisierung: Hierbei ersetzt eine verschlüsselte Datei, ein sogenannter Token, die hinterlegte Kartennummer, damit Hacker keine Kreditkartendaten abgreifen können.

Mastercard® Identity Check™: das neue Programm für Händler und die Regulatory Technical Standards (RTS)

Hinter Mastercard Identity Check verbergen sich das neue Programm und die neue Marke für Mastercard Authentifizierungen auf Basis des EMV 3DS-Standards. Er ersetzt die bisherige Marke Mastercard® SecureCode™ und die bisherige Version des 3DS-Protokolls (3DS 1.0).

Mastercard Identity Check stellt an alle E-Commerce-Akteure – Händler, Acquirer und Kartenherausgeber – Mindestanforderungen in Sachen Autorisierungsfreigabe, Betrugsbekämpfung und Zahlungsabbruch.

Seit April 2019 (bzw. in einigen Ländern seit September oder Dezember 2019) müssen europäische Kartenherausgeber ihren Karteninhabern zusätzlich biometrische Authentifizierungslösungen über das Smartphone anbieten, bei denen sowohl die Transaktionsabbrüche als auch die Betrugsquoten am geringsten sind und die daher auch die höchsten erfolgreichen Kaufabschlüsse erzielen.

EMV 3DS und Mastercard Identity Check: eine Chance für Händler

Mit EMV 3DS und Mastercard Identity Check können E-Commerce-Händler jetzt dieselben erfolgreichen Kaufabschlüsse erreichen wie im stationären Handel (laut Erhebung im Mastercard Netzwerk über Chip & PIN*).

- durchschnittlich 10 Prozentpunkte höhere Annahmequoten
- bis zu 50 % geringere Betrugsraten
- etwa 50 % geringere Abbruchraten

Möglich wird dies durch eine Optimierung des Transaktionsvorgangs, im Zuge dessen Kartenherausgeber für jeden Online-Kauf eine starke Kundenauthentifizierung (SCA) durchführen können und so ausreichende Daten zur Rechtfertigung der SCA-Ausnahmen erhalten. Online-Händler müssen EMV 3DS-Authentifizierungsanfragen unterstützen, um den Anforderungen der EBA RTS und den Mastercard Regeln, die (länderabhängig) zwischen April und Dezember 2019 in Kraft traten, zu genügen.

* Mastercard Transaktionsdaten Chip & PIN 2017

SCA-Ausnahmen: Wann und wie greifen sie?

Die RTS erlauben Zahlungsdienstleistern (also Kartenherausgebern und Acquirern) für elektronische Zahlungen (hier insbesondere E-Commerce-Zahlungen) Ausnahmen von SCA:

- für Kleinstbetragszahlungen bis 30 €. (Allerdings ist hier bei aufeinanderfolgenden Vorgängen für jede sechste Transaktion eine SCA erforderlich. Gleiches gilt, wenn seit der letzten SCA ein Gesamttransaktionsbetrag von 100 € überschritten wurde.)
- für wiederkehrende Zahlungen in gleicher Höhe an dieselben Zahlungsempfänger. Die SCA ist im Vorfeld erforderlich, also bei Vereinbarung der wiederkehrenden Zahlung unter korrekter Angabe der Höhe, Laufzeit und Häufigkeit der Zahlung. Nachfolgende wiederkehrende Zahlungen müssen auf die ursprüngliche Vereinbarung verweisen.
- wenn ein Zahlungsvorgang mithilfe einer Transaktionsrisikoanalyse als Zahlung mit niedrigem Betrugsrisiko eingestuft wird, weil er auf Basis der RTS vorab definierte monetäre Schwellenwerte und Betrugsraten nicht überschreitet (keine früheren Betrugsszenarien durch eine vom Karteninhaber ausgelöste Zahlung, Transaktion über ein für frühere Käufe verwendetes Endgerät, z. B. maximaler Betrag von 100 € und Acquirer-Betrugsraten von maximal 13 Basispunkten).
- für Transaktionen mit Händlern, die auf einer zuvor vom Zahler erstellten Liste vertrauenswürdiger Empfänger (Positivliste) geführt werden (sogenannte Positivlisten-Ausnahme). Für die Erstellung sowie Änderungen der Positivliste vertrauenswürdiger Empfänger ist eine starke Kundenauthentifizierung erforderlich. Die Anwendung dieser Ausnahme ist den Kartenherausgebern vorbehalten.

Händlern wird empfohlen, die Ausnahmen (Acquirerausnahmen) mittels des EMV 3DS-Protokolls dem Kartenherausgeber mitzuteilen und entsprechend die Authentifizierungsnachrichten zu markieren. Diese markierten Authentifizierungen erfordern in der Regel keine Karteninhaberprüfung (könnten also nicht zum Abbruch führen), erlauben dem Kartenherausgeber aber die Kontrolle des Risikos, sodass die Annahmerate steigt.

Wichtigste Handlungsempfehlungen für Händler

Technische Voraussetzungen schaffen, Daten bereitstellen, Ausnahmen nutzen, Mastercard® Identity Check™ konsequent nutzen und Sonderfälle beachten!

1. **Technische Voraussetzungen schaffen:** Händler sollten sich bei ihrem Zahlungsdienstleister (Payment Service Provider (PSP), genannt 3DS-Server-Provider) erkundigen, ab wann der PSP EMV 3D-Secure unterstützt. **Planen Sie ausreichende Testzeiträume für die Umsetzung der technischen Anpassungen ein!** Händler müssen ihre Webseiten auf EMV 3DS und Mastercard Identity Check anpassen. Dazu gehört die Aufnahme des Mastercard Identity Check Programmlogos, das Sie **hier** finden.

   Für eine optimale Kundenfreundlichkeit empfehlen wir die Implementierung des Authentifizierungsprozesses in die Händler-App über eine native Nutzerschnittstelle (User Interface, UI). Dies gewährleistet ein einheitliches Erscheinungsbild innerhalb der Händler-App.

2. **Daten bereitstellen:** Händler sollten mit ihrem PSP besprechen, welche zusätzlichen Transaktions- und Karteninhaberdaten erfasst bzw. identifiziert werden müssen (z. B. Rechnungs- und Lieferadresse, E-Mail, Mobilfunknummer oder Geräte-ID) und diese an den PSP weiterleiten, der diese Daten für seine Anwendungsprogrammierschnittstelle im EMV 3D-Secure-System (Application Programming Interface, kurz API) benötigt. Händler müssen (z. B. über ihre Datenschutzhinweise) sicherstellen, dass ihre Vertragsbedingungen die Erhebung und Weitergabe von Kundendaten entsprechend der Datenschutzgrundverordnung (DSGVO) erlauben.

3. **Ausnahmen nutzen:** Händler sollten in Abstimmung mit ihrem PSP und Acquirer eine Ausnahmeregel-Strategie entwickeln, um den Anforderungen der RTS für ihre gewählten Ausnahmen zu genügen – besonders hinsichtlich der Anwendung von Transaktionsrisikoanalyse-Ausnahmen unter Berücksichtigung der entsprechend anwendbaren Betrugsraten.

4. **Mastercard® Identity Check™ konsequent nutzen:** Händlern wird empfohlen, immer EMV 3D-Secure-Authentifizierungsanfragen zu senden. Besonders gilt dies gegenüber Kartenherausgebern, die Autorisierungen ohne vorherige Authentifizierung ablehnen.
5. **Sonderfälle beachten:** Bei Ablehnung einer Zahlung wegen einer fehlenden Authentifizierungsanfrage sollte vom Händler ein Mechanismus eingebaut werden, bei dem mithilfe von EMV 3DS erneut die Zahlung eingeleitet wird. Auch sollte ein Mechanismus vorhanden sein, um bei einer Nichtunterstützung von EMV 3DS des Kartenherausgebers auf das 3D-Secure 1.0.2 Protokoll ausweichen zu können.
6. **Verarbeitung von weichen Ablehnungen:** Dieser neue Ablehnungstyp zeigt eine Forderung nach starker Kundenauthentifizierung auf und muss von Händlern spätestens ab Januar 2021 unterstützt werden, um die Konversionsraten weiterhin hoch zu halten.

Darüber hinaus sollten Händler

- die Einheitlichkeit und Einzigartigkeit der Händlernamen sicherstellen, um die Positivlisten-Ausnahme nutzen zu können.
- die erste wiederkehrende Zahlung mit einer starken Kundenauthentifizierung (SCA) absichern. Um die Annahmeraten zu erhöhen, empfiehlt sich für jede Folgezahlung der Versand einer EMV 3DS-Authentifizierungsanfrage an den Kartenherausgeber, die auf die ursprüngliche SCA verweist. Im Falle wiederkehrender Zahlungen mit variablen Beträgen oder Zahlungen, deren endgültiger Betrag unbekannt ist, sollte der Händler dem Karteninhaber klar kommunizieren und erläutern, warum der authentifizierte Betrag vom autorisierten Betrag abweichen kann.
- sicherstellen, dass der Authentifizierungsbetrag gleich oder höher ist als der Autorisierungsbetrag.