Jetzt umstellen: EMV 3D Secure 2.1

Was Sie als Online-Händler über den neuen Standard zur starken Kundenauthentifizierung bei Kreditkartenzahlung wissen müssen.

VR Payment

Ein neuer Standard bei Kreditkarten-zahlungen.

Auch wenn die Bafin die Frist für Umsetzung der gesetzlichen Anforderungen zur starken Kundenauthentifizierung (gemäß PSD2) beim Bezahlen mit Kreditkarte etwas aufgeweicht hat, so trat diese dennoch am 14. September 2019 in Kraft.*

Um den Vorgaben zu genügen, haben Mastercard und Visa das Sicherheitsprotokoll EMV 3D Secure 2.1 (EMV 3DS) als neuen Standard entwickelt. EMV 3DS liefert zusätzliche Sicherheitsmechanismen wie z. B. Biometrie. Zudem unterstützt es die Anwendung der im Regulatorischen Technischen Standard (RTS) vorgesehenen Ausnahmeregeln. EMV 3DS verbessert so die Sicherheit und reduziert Kaufabbrüche auf ein Minimum. Das bedeutet für Sie: höherer Umsatz und eine höhere Convenience für Ihre Kunden.

Nach dem Stichtag 31.12.2020 können die europäischen Kartenherausgeber Transaktionen ohne den neuen Standard ablehnen. Zögern Sie also die Umstellung nicht hinaus und nehmen Sie zeitnah die Anpassungen vor.

* Grundlage ist die EU-Richtlinie 2015/2366, Art. 97 „Starke Kundenauthentifizierung“

Mehr Sicherheit für Sie und Ihre Kunden.

Ziel der gesetzlichen Änderungen ist es, innovative Bezahlverfahren zu fördern und Verbraucher in der digitalen Welt besser zu schützen. Formuliert sind die Vorgaben in der zweiten Payment Service Directive, kurz PSD2, und dem dazugehörigen Regulatorischen Technischen Standard, kurz RTS, der für die 28 EU-Länder sowie für Norwegen, Island und Liechtenstein gilt.

Was ist eine starke Kundenauthentifizierung?

Mindestens 2 der folgenden 3 Faktoren müssen gegeben sein, damit eine starke Authentifizierung vorliegt:

Wissen
(etwas, das nur Ihr Käufer weiß)
z. B. das Passwort oder die PIN

Besitz
(etwas, das nur Ihr Käufer besitzt)
z. B. die Kreditkarte oder das Mobiltelefon

Inhärenz
(etwas, das ein Teil Ihres Käufers ist)
z. B. Face-ID, Gesichts-ID oder Gesichtszüge

Wichtige Ausnahmen.

Die gesetzliche Regelung kennt auch Ausnahmen. Unter bestimmten Voraussetzungen können Zahlungsdienstleister die Ausnahmen anwenden, um von der starken Kundenauthentifizierung abzusehen:

- **Kleinstbeträge bis 30 €**
- **Abonnements sowie von Ihnen als Händler initiierte Transaktionen**
- **Zahlungen mit niedrigem Betrugsrisiko bis maximal 500 €**
- **Listung bei der Bank Ihres Kunden als vertrauenswürdiger Empfänger der Kartenzahlung (Whitelisting)**

Mehr Infos zu den Ausnahmen finden Sie auf unserer Webseite:

:vr-payment.de

Der neue Standard: EMV 3D Secure 2.1

EMV 3D Secure 2.1 (EMV 3DS) ist die Weiterentwicklung des bisherigen Sicherheitsstandards bei Kreditkartenzahlungen. Die neuen gesetzlichen Anforderungen inklusive der Ausnahmen sind darin berücksichtigt. Zudem unterstützt EMV 3DS neue Bezahlwege wie z. B. die Zahlung innerhalb von Apps und mobile Zahlungen.

Neue Markenauftritte bei Mastercard und Visa
Durch die Einführung von EMV 3DS ändern sich auch bisherige Markenbezeichnungen.
Aus „Secure Code" wird bei Mastercard „Identity Check".
„Verified by Visa" wird abgelöst durch „Visa Secure".

Ihre Vorteile mit EMV 3DS:
- Durchschnittlich 10 % höhere Akzeptanz beim Bezahlen mit Kreditkarte**
- Bis zu 50 % geringere Betrugsraten**
- Etwa 50 % geringere Abbruchraten**

** laut Erhebung im Mastercard Netzwerk über Chip und PIN

Der Grund, warum im Vergleich zum bisherigen Sicherheitsstandard mit EMV 3DS deutlich mehr Zahlungen erfolgreich abgeschlossen werden, liegt in der Optimierung des Transaktionsvorgangs. Denn bei EMV 3DS werden mehr Daten erhoben. Das führt dazu, dass die Ausnahmeregelungen öfter angewandt werden können.

Das Ergebnis: Es kommt seltener zu Zahlungsabbrüchen als bisher.

Was müssen Sie bei der Umstellung beachten?

1

Präsentieren Sie die aktuellen Logos

Als Online-Händler müssen Sie Ihre Webseiten auf EMV 3DS umstellen. Dazu gehört auch, dass Sie die bisherigen Programmlogos von Mastercard und Visa ersetzen. Laden Sie dafür die neuen Logos für **Mastercard Identity Check** und **Visa Secure** herunter und präsentieren Sie die neuen Logos anstelle der bisherigen auf Ihrer Webseite.

Eine Möglichkeit zum Download der Logos finden Sie unter **vr-payment.de**

2

Passen Sie die Schnittstelle an

EMV 3DS benötigt für die Kommunikation zwischen Ihrem Online-Shop und dem Kartenherausgeber Informationen, die Ihre bisherige Schnittstelle nicht liefern kann.

3

Aktualisieren Sie Ihre Datenschutzhinweise

Stellen Sie sicher, dass Ihre Vertragsbedingungen die Erhebung und Weitergabe von Kundendaten entsprechend der Datenschutzgrundverordnung (DSGVO) erlauben.

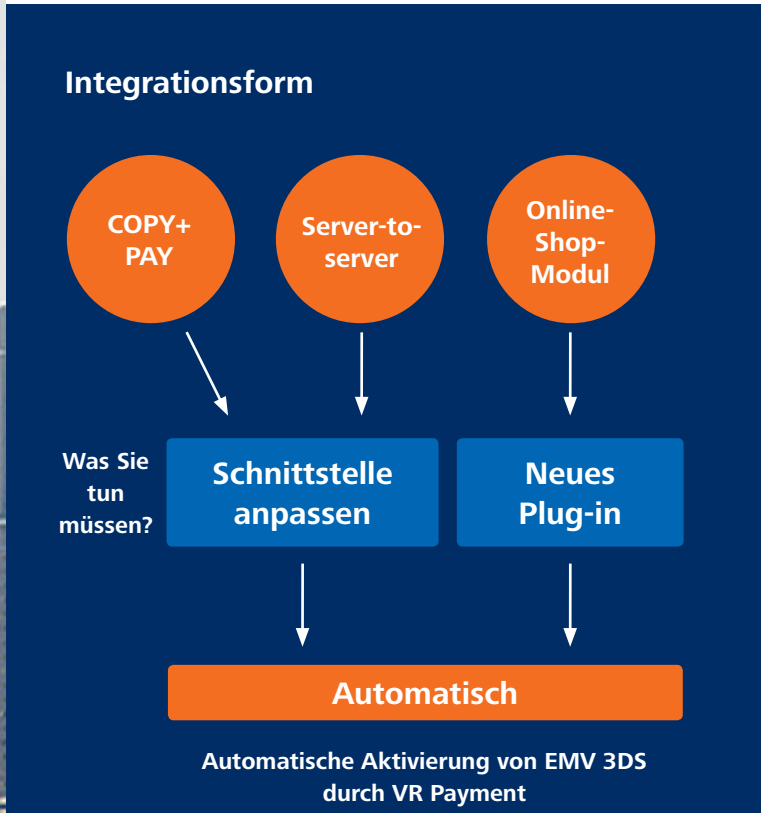
Die technische Umstellung

Die Umstellung auf den neuen Standard für die Abwicklung von Kreditkartenzahlungen EMV 3DS hängt davon ab, wie das VR pay Internet Gateway in Ihren Online-Shop integriert ist. Dafür gibt es prinzipiell 3 Möglichkeiten:

1. **Integration über das von Ihnen genutzte COPY+PAY**
2. **Integration per Server-to-Server**
3. **Integration im von Ihnen genutzten Online-Shop-Modul**

Nur wenige Arbeitsschritte für Sie

Unsere Grafik gibt Ihnen einen Überblick über die Anpassungen, die Sie vornehmen müssen. Die dazugehörigen Einzelschritte werden auf den folgenden Seiten für jeden der drei Anwendungsfälle des VR pay Internet Gateway gesondert beschrieben.



1. COPY+PAY

Wenn Sie COPY+PAY nutzen, müssen Sie die Schnittstelle so anpassen, dass folgende Werte zusätzlich übermittelt werden:

Feld	API Feld Name	Beschreibung
Billing City	billing.city	Stadt der Rechnungsadresse des Karteninhabers. **Beispiel: Musterstadt**
Billing Country	billing.country	Land der Rechnungsadresse des Karteninhabers. **Beispiel: DE**
Billing Street	billing.street1	Straße der Rechnungsadresse des Karteninhabers. **Beispiel: Musterstr. 1**
Billing Postcode	billing.postcode	Postleitzahl der Rechnungsadresse des Karteninhabers. **Beispiel: 12345**
Customer Email	customer.email	E-Mail-Adresse des Karteninhabers. **Beispiel: max.mustermann@muster.de**
Customer Given Name	customer.givenName	Vorname des Karteninhabers. **Beispiel: Max**
Customer Surname	customer.surname	Nachname des Karteninhabers. **Beispiel: Mustermann**

Diese Werte müssen Sie bei Ihren Kunden abfragen und bei der Zahlung mit Kreditkarte mit der Transaktion mitgeben. Hierfür müssen Sie Ihre Schnittstelle um die entsprechenden Felder ergänzen.

Die hier aufgeführten Werte sind Pflicht. Daneben gibt es noch optionale Werte, die abgefragt werden können, um die Wahrscheinlichkeit der positiven Authentifizierung zu erhöhen.

Mehr dazu unter:
https://vrpayecommerce.docs.oppwa.com/support/3d-secure-2.0-guide

2. Server-to-Server-Integration

Wenn Sie das VR pay Internet Gateway per Server-to-Server-Anwendung in Ihrem Online-Shop integriert haben, müssen folgende Werte zusätzlich übermittelt werden:

Feld	API Feld Name	Beschreibung
Accept header	customer.browser.acceptHeader	Inhaltstypen des Clients im Accept Header, gesendet vom Browser des Karteninhabers. **Beispiel: text/html**
Language	customer.browser.language	Die Sprache des Browsers des Karteninhabers. **Beispiel: DE**
Screen height	customer.browser.screenHeight	Dieses Feld enthält die Höhe des Bildschirms des Karteninhabers in Pixeln. **Beispiel: 640**
Screen width	customer.browser.screenWidth	Dieses Feld enthält die Breite des Bildschirms des Karteninhabers in Pixeln. **Beispiel: 1024**
Browser timezone	customer.browser.timezone	Dieses Feld enthält die Zeitzone des Browsers des Karteninhabers. **Beispiel: UTC+1**

Weitere optionale Felder finden Sie in der Dokumentation unter:
https://vrpayecommerce.docs.oppwa.com/support/3d-secure-2.0-guide

Feld	API Feld Name	Beschreibung
User agent	customer.browser.userAgent	Dieses Feld enthält den genauen Inhalt des HTTP User-Agent Header. **Beispiel: Mozilla/5.0**
IP address	customer.browser.ipAddress	Angabe der IP-Adresse des Browsers des Karteninhabers. **Beispiel: 89.15.236.75**
Java enabled	customer.browser.javaEnabled	true / false – Java-Fähigkeit des Browsers des Karteninhabers.
Screen color depth	customer.browser.screenColorDepth	Dieses Feld gibt die Anzahl der verfügbaren Farben auf dem Bildschirm des Karteninhabers, in Bits per Pixel an.
Authentication window size	customer.browser.challengeWindow	Größe des iFrames der 3D-Secure Authentifizierungsseite.

Bitte senden Sie einen Zahlenwert zwischen 1–5.
Der Wert entspricht einer der Auflösungen:

1	2	3	4	5
250 x 400	390 x 400	500 x 60	600 x 400	Full screen

3. Online-Shop-Module

Wenn Sie ein Online-Shop-Modul nutzen, müssen Sie nur das Modul aktualisieren, um EMV 3DS als neuen Standard für Kreditkartenzahlungen einzuführen. Die Anpassungen der Schnittstelle erfolgen automatisch.

Die neuen Online-Shop-Module für das VR pay Internet Gateway stehen unter **https://vr-payment.de/onlineshop-module/** für Sie zum Download bereit.

Wichtig!

Bitte nehmen Sie die Anpassungen zeitnah vor und warten Sie nicht zu lange mit der Umstellung. Nur so können Sie schnellstmöglich von den vielen Vorteilen von EMV 3DS profitieren können, und stellen sicher, dass Sie **vor dem 31. Dezember 2020** die neue Schnittstelle nutzen. Schauen Sie sich auch die optionalen Felder an und bewerten Sie, inwieweit diese Daten für Sie sinnvoll sind.
Diese Daten erleichtern es den kreditkartenausgebenden Banken, Zahlungen zu autorisieren.

Weitere Informationen zur starken Kundenauthentifizierung, zu EMV 3DS und zur technischen Integration des neuen Standards finden Sie auf unserer Webseite unter:

:vr-payment.de

:vr-payment.de

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken