computop
the payment people

3D Secure 2.0

Informationen für Händler zum neuen 3D Secure-Protokoll

Inhaltsübersicht

Was Sie als Händler zur Einführung des neuen 3D Secure-Verfahrens wissen müssen

Die Ankündigung des neuen 3D Secure 2.0-Verfahrens (3DS 2.0) hat in den vergangenen Monaten für eine erhebliche Verunsicherung aller betroffenen Akteure im E-Commerce gesorgt.

Insbesondere auf Händlerseite wächst der Unmut über die Informationspolitik der verantwortlichen Initiatoren, zumal im Zuge der neuen europäischen Zahlungsdienstrichtlinie PSD II viele Payment-Prozesse im Onlinehandel ohnehin auf den Prüfstand gestellt werden müssen.

Computop setzt sich seit der Ankündigung des Roll-outs von 3D Secure 2.0 intensiv mit den Anforderungen an das neue Verfahren auseinander und möchte seinen Kunden und allen interessierten Händlern auf den folgenden Seiten die wesentlichen Fragen zu 3D Secure 2.0 beantworten.

1 3D Secure und 3D Secure 2.0 im Überblick

Das 3D Secure–Verfahren

Das seit dem Jahr 2002 bestehende, weltweit standardisierte 3D Secure-Protokoll (3DS) bietet Händlern und Verbrauchern zusätzliche Sicherheit bei Kreditkartentransaktionen, die online getätigt werden. Mit dem Verfahren verifizieren sich Onlinekäufer gegenüber ihrer kartenausgebenden Bank (Issuer) als rechtmäßiger Karteninhaber. Im Gegensatz zu einem normalen Bezahlvorgang per Kreditkarte im Internet, für welchen lediglich die Kartendaten benötigt werden, verlangt 3D Secure die zusätzliche Eingabe eines Codes durch den Käufer, um den Bestellvorgang erfolgreich abschließen zu können. Auf diese Weise wird die missbräuchliche Verwendung von Kreditkarten deutlich erschwert.

Gleichzeitig wird die Haftung für betrügerische Transaktionen, die trotz Einsatz des Verfahrens erfolgreich ausgeführt wurden, von den kartenausgebenden Banken übernommen. Voraussetzung für den Einsatz des Verfahrens ist, dass 3D Secure sowohl von der kartenausgebenden Bank des Käufers sowie von dem betreffenden Onlineshop unterstützt wird.

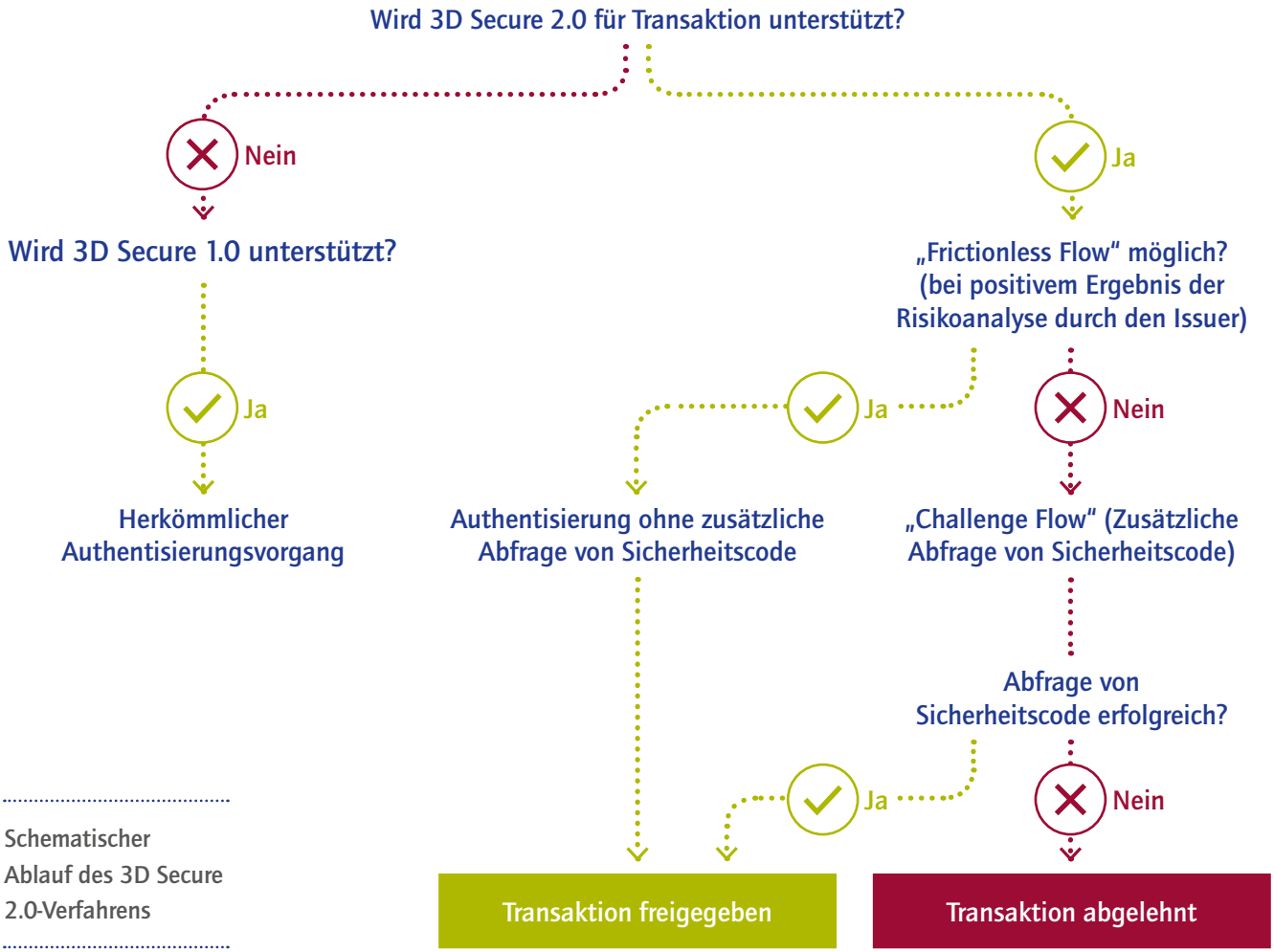
Wie unterscheidet sich 3D Secure 2.0 von dem herkömmlichen Verfahren?

Im Wesentlichen stellt 3D Secure 2.0 eine Weiterentwicklung des herkömmlichen 3D Secure-Protokolls dar. Die automatisierte Übermittlung eines bis zu 10mal höheren Volumens an transaktions- und käuferbezogenen Daten ermöglicht den Issuer-Banken künftig, die bisher statische Code-Abfrage durch eine in Echtzeit ablaufende Risikoanalyse zu ersetzen.

Jede Bestellung per Kreditkarte löst die Übermittlung von bis zu 100 Datenpunkten an den Issuer aus. Die Erfassung und Weiterleitung der Daten erfolgt sowohl über das Shop-Backend des Händlers wie auch durch den Payment Service Provider (PSP), über welchen 3D Secure 2.0 an den jeweiligen Shop angebunden ist (siehe Schaubild). Die Übergabe der Daten an den Issuer findet in der gesicherten Umgebung eines 3D Secure Servers statt.

Die anschließende Echtzeit-Risikobewertung jeder Transaktion obliegt allein dem Issuer. Eine Analyse-Software errechnet für jede Transaktion ein Scoring, basierend auf Datensignalen, die auf mögliche Betrugsversuche hinweisen. Wird eine Transaktion als risikoarm eingestuft, erfolgt eine Freigabe, ohne dass der Käufer um eine zusätzliche Code-Eingabe gebeten wird. Besteht hingegen eine erhöhte Betrugswahrscheinlichkeit (zutreffend für maximal 5 Prozent aller Kreditkartentransaktionen), wird der Käufer mittels SMS oder E-Mail zur erneuten Bestätigung seiner Identität aufgefordert.

Der Prozess der Risikobewertung läuft für den Käufer nicht wahrnehmbar im Hintergrund ab. Somit kann in der Mehrheit aller Fälle ein reibungsloser Bezahlvorgang ohne zusätzliche Abfrage von Sicherheitsinformationen gewährleistet werden.



Schematischer Ablauf des 3D Secure 2.0-Verfahrens

Weshalb wird 3D Secure 2.0 eingeführt?

Erklärtes Ziel von 3D Secure 2.0 ist es, die von Händlern und Käufern vielfach kritisierten Schwächen des herkömmlichen Verfahrens zu beheben und den Anforderungen an die Strong Customer Authentication (SCA) gerecht zu werden, welche ab dem 14. September 2019 für elektronische Zahlungsverfahren rechtlich verpflichtend wird.

Da Käufer künftig keinen 3D Secure Code mehr eingeben müssen und für die Mehrheit der Kreditkartentransaktionen keine Abfrage weiterer Informationen auf Käuferseite erforderlich ist, wird davon ausgegangen, dass das neue Verfahren keine nennenswerten Auswirkungen auf die Kaufabbruchquote im Checkout-Prozess hat. Zusätzlich verspricht die individuelle, datenbasierte Risikobewertung jeder Transaktion einen noch besseren Schutz vor Betrug.

Händler, die sich für die Integration von 3DS 2.0 entscheiden, profitieren zusätzlich von einer deutlich verbesserten Usability bei Mobile- und In-App-Käufen. Eingabefenster für 3DS-Abfragen können ab sofort in einem auf das jeweilige Endgerät angepassten Format (Responsive Design) ausgespielt werden. Gleichzeitig ist das neue Verfahren nicht mehr länger ausschließlich browserbasiert, sondern lässt sich mithilfe vorgefertigter Software Development Kits (SDKs) fortan auch in händlereigene Shopping-Apps integrieren.

Allerdings ist hierbei zu beachten, dass sich die betreffenden Formulare nur sehr eingeschränkt an das Corporate Design des jeweiligen Onlineshops anpassen lassen. Kommt es im Verdachtsfall zu einer Authentisierungsabfrage, bleibt für den Onlinekäufer die Weiterleitung zum kartenausgebenden Institut weiterhin ersichtlich.

2 Datenübermittlung im 3D Secure 2.0-Verfahren

Welche Daten werden übermittelt und wer ist für die Erfassung verantwortlich?

Daten, die vom Payment Service Provider (PSP) des Händlers erfasst, verarbeitet und anschließend an den 3D Secure Server übergeben werden, sind:

1. Kreditkartendaten,

welche gemäß den Anforderungen an PCI DSS erhoben und verarbeitet werden müssen.

2. Transaktionsbezogene Daten

Hierzu gehören die zur Zuordnung von Transaktion und Händler benötigten Identifikationsnummern sowie die Kaufbetragshöhe und Währung.

3. Browserinformationen,

die Aufschluss über das verwendete Endgerät und den Aufenthaltsort des Users geben. Diese umfassen unter anderem IP-Adresse, Bildschirmhöhe und -breite sowie die verwendete Browsersprache.

Die nachfolgenden Daten werden im Shopsystem des Händlers erfasst und über die Payment-Schnittstelle des PSPs an den 3D Secure Server übergeben. Diese sind für das 3DS 2.0-Verfahren nicht zwingend notwendig. Ihre Übermittlung wird jedoch empfohlen, um ein präzises Risiko-Scoring gewährleisten zu können:

4. Rechnungs- und Lieferadresse

Die vollständige Rechnungs- und Lieferadresse der Bestellung.

5. Kundenkonto

Daten, die im Rahmen eines bestehenden Kundenkontos erfasst wurden. Hierunter fallen u. a. Angaben zur Dauer des Bestehens des Kundenkontos, die Anzahl an durchgeführten Transaktionen innerhalb bestimmter Zeitintervalle und die Häufigkeit der Änderung von Passwörtern und Lieferadressen.

6. Lieferdetails

Daten zu Lieferdetails, wie z. B. die gewählte Versandmethode, Verfügbarkeit der Ware, das Lieferzeitfenster, die E-Mail-Adresse im Fall eines Versands digitaler Güter oder das Datum der Erstverfügbarkeit für noch nicht veröffentlichte Produkte.

Ist die Übermittlung aller möglichen Datenpunkte notwendig?

Nein. Die für die Definition des 3DS 2.0-Standards zuständige Organisation EMVCo (Branchenverband der Kreditkartenwirtschaft) unterscheidet zwischen verpflichtenden und optionalen Datenpunkten und Daten. Zu den letzteren gehören alle Daten, welche innerhalb des Bestellprozesses ausgehend vom Händler-Backend erhoben werden.

Um das neue 3DS 2.0-Verfahren sinnvoll einsetzen können, ist jedoch eine Erfassung und Übergabe aller Parameter dringend zu empfehlen: Je mehr Daten in die Transaktionsanalyse des Issuers einfließen, desto präziser fällt die Beurteilung der Betrugswahrscheinlichkeit einer Transaktion aus.

3 Wissenswertes zur Implementierung von 3D Secure 2.0

Welche Herausforderungen sind für Händler mit einer Umstellung verbunden?

Eine Umstellung auf das neue 3DS 2.0-Verfahren stellt Händler vor zwei zentrale Herausforderungen, die bei der Beurteilung des Zeitpunktes einer Integration Berücksichtigung finden sollten:

- Auch wenn der Großteil der technischen Anpassungen von den Issuern und Payment Service Providern vorgenommen werden muss, kommen Händler um die Überarbeitung ihres Bestell- und Checkout-Prozesses nicht herum: Bestehende Formulare zur Anlage von Kundenkonten und Guest-Checkouts müssen um die geforderten Datenfelder erweitert und in Abstimmung mit dem PSP konfiguriert werden, um eine reibungslose Übergabe der Daten über die Schnittstelle zu gewährleisten.
- Schwer abschätzbar ist die Reaktion der Kunden auf das neue Verfahren. Diese müssen zum einen in den AGBs und Datenschutzbestimmungen über die Art und den Umfang der zusätzlich übermittelten Daten informiert werden. Zum anderen steigt mit der wachsenden Anzahl von Pflichtangaben im Bestellprozess der kundenseitige Aufwand für eine Bestellung im Shop.

Muss eine Umstellung auf 3DS 2.0 zwingend erfolgen? Welche Fristen gilt es zu beachten?

3DS 2.0 selbst stellt keine gesetzlich vorgeschriebene Norm dar. Maßgeblich für Händler ist vielmehr die Frage, ob im eigenen Onlineshop bis zum 14. September 2019 ein Verfahren zur Abwicklung von Kreditkartentransaktionen bereitgestellt werden kann, welches den Anforderungen an eine starke Kundenauthentifizierung (Strong Customer Authentication, Abk. SCA) gerecht wird.

Als „Minimallösung" steht hierfür das bisherige 3DS 1.0-Verfahren bereit, welches in seiner grundlegenden Funktionsweise den Anforderungen an SCA genügt, jedoch zahlreiche undurchsichtige Ausnahmeregelungen enthält, unter denen eine Abfrage des 3DS-Codes nicht zwingend erfolgen muss.

Mit einer weiteren Verwendung von 3DS 1.0 laufen Händler daher Gefahr, bei einer fehlerhaften Anwendung der Ausnahmeregelungen gegen die Auflagen zur starken Kundenauthentifizierung zu verstoßen. Das in Abstimmung mit der europäischen Bankenaufsicht (EBA) entwickelte 3DS 2.0-Verfahren ist laut Aussage von EMVCo hingegen in jeder Hinsicht SCA-konform.

Händler, die die bisherige 3DS-Version 1.0 integriert haben, werden um ein „Upgrade" auf 3DS 2.0 in naher Zukunft nicht herumkommen. Grundsätzlich sollte hier die Devise gelten: Je früher desto besser. Jedoch wird das 3DS 1.0-Verfahren vermutlich auch noch nach September 2019 von den meisten Issuer-Banken auf unbestimmte Zeit als Fallback-Option akzeptiert.

Wie erfolgt eine Umstellung mit Computop?

Die gute Nachricht für unsere Kunden: Den Großteil der anstehenden Arbeit können wir Ihnen abnehmen. Wie bei allen unseren Produkten besteht der Anspruch an unsere 3DS 2.0-Lösung darin, den Integrationsaufwand für unsere Kunden so gering wie möglich zu halten.

Genauso wichtig ist für uns, bereits mit dem ersten Release eine voll funktionale Lösung bereitzustellen, die nach einmal erfolgter Integration keine erneuten Anpassungen auf Kundenseite erfordert. Deshalb arbeiten wir bereits seit der Ankündigung des neuen 3DS-Standards intensiv an einer schnellen und praktikablen Umsetzung.

Sollten Sie sich für eine zeitnahe Integration des Verfahrens entscheiden, erläutern wir Ihnen gerne im Gespräch mit Ihrem persönlichen Ansprechpartner und unseren technischen Beratern alle notwendigen Schritte und nehmen gemeinsam mit Ihnen eine Abschätzung des Aufwandes vor, der für Sie als Händler anfällt.

Gerne stellen wir Ihnen auch die technische Dokumentation zur Integration von 3DS 2.0 in das Computop Paygate bereit. Wenn Sie über aktuelle Entwicklungen zu den Themen PSD II und 3DS 2.0 informiert bleiben möchten, laden wir Sie herzlich ein, unsere Website https://www.computop.com/de/psd2-3dsecure2/ zu besuchen.

Welche Aufgaben fallen für Händler bei einer Umstellung an?

Händler, die das 3DS 2.0-Verfahren in Ihren Shop integrieren möchten, müssen

1. mit ihrem Payment Service Provider abklären, ob dieser das 3DS 2.0-Protokoll unterstützt.
2. in Abstimmung mit Ihrem Payment Service Provider eine Anpassung der im Bestell- und Checkout-Prozess betroffenen Formulare vornehmen, um die erforderlichen Kundendaten zur Übermittlung bereitzustellen.
3. das 3DS 2.0-Protokoll zusätzlich zum Onlineshop auch in ihre Mobile Shopping Apps integrieren (falls vorhanden).
4. eine Anpassung der allgemeinen AGBs und Datenschutzbestimmungen vornehmen und Ihre Kunden hierüber in Kenntnis setzen.
5. das unterstützte 3D Secure 2.0-Verfahren bei ihrem Acquirer anmelden.

4 Empfohlenes Vorgehen von Computop

Die wichtigste Regel im Umgang mit 3D Secure 2.0: Lassen Sie sich nicht aus der Ruhe bringen

Wir möchten alle unsere Kunden (und Händler, die es noch nicht sind) dazu ermutigen, sich nicht infolge der allgemeinen Verunsicherung zum Thema 3D Secure 2.0 zu überstürzten Entwicklungsprojekten hinreißen zu lassen.

Auch wenn seitens Medien, Branchenverbänden und Kartengesellschaften ein hoher Druck auf die Händler ausgeübt wird, liegt es bis zum September 2019 zunächst an Issuern und Kartengesellschaften, die technischen Voraussetzungen für das neue Verfahren bereitzustellen.

Viele kartenausgebendee Banken sind bis zum jetzigen Zeitpunkt noch nicht in der Lage, alle von der EMVCo geforderten Datenpunkte in der Transaktionsanalyse zu verarbeiten. Dies bedeutet letztendlich, dass das 3DS-Secure 2.0-Verfahren gegenwärtig noch gar nicht flächendeckend einsatzfähig ist.

Was Sie jetzt beachten müssen:

1

Sofern Sie das 3DS 1.0-Verfahren in Ihrem Shop integriert haben, besitzen Sie eine gute Ausgangsposition: In diesem Fall werden in Ihrem Onlineshop eingehende Kreditkartenzahlungen automatisch über das neue 3D Secure 2.0-Protokoll abgewickelt. Damit jedoch Ihre Käufer die Vorteile des neuen Verfahrens genießen können, müssen zusätzliche Daten aus Ihrem Shopsystem an unser Paygate übertragen werden.

2

Schätzen Sie zunächst zusammen mit Ihrem Development ab, mit welchem personellen und finanziellen Aufwand eine Durchführung der betreffenden Maßnahmen (Erhebung der Daten im Shop-Backend und Übermittlung der Daten an unsere Payment-Schnittstelle) innerhalb der nächsten Monate verbunden wäre.

3

Wenn Sie die vollständige Integration von 3DS 2.0 bis Herbst 2019 vornehmen möchten, wird Computop die Anbindung problemlos über die Paygate-Schnittstelle begleiten können.

4

Falls Sie über eine andere Weise an unser Paygate angebunden sind (z.B. über das Direct-Post- oder Server-to-Server-Verfahren), nehmen Sie bitte umgehend Kontakt mit uns auf. Um sicherzustellen, dass ausnahmslos alle Kreditkartenzahlungen in Ihrem Shop verarbeitet werden können, muss eine Anpassung Ihrer Integration bis zum 14. September erfolgen. Selbstverständlich wird Sie unser technischer Support bei der fristgerechten Umsetzung unterstützen.

Fordern Sie uns heraus

Sie haben Fragen? Löchern Sie uns! Die Payment People von Computop stehen Ihnen Rede und Antwort. Gemeinsam mit Ihnen finden wir die individuell beste Paymentlösung für Ihr Geschäftsmodell. Auch neue und anspruchsvolle Herausforderungen sind uns willkommen!

So erreichen Sie uns:

DE T: +49 (0) 951-98009-22
sales@computop.com

UK T: +44 (0) 1932 895735
uk@computop.com

USA T: +1 646-701-7045
usa@computop.com

CHINA T: +852 2918-8295
china@computop.com