EMV 3D-Secure (EMV 3DS) und Mastercard® Identity Check™

Fragen und Antworten

F: Was verbirgt sich hinter EMV 3D-Secure?

A: EMV 3D-Secure (EMV 3DS) ist ein globaler Branchenstandard, der Händler und Kartenherausgeber bei der Authentifizierung von E-Commerce-Zahlungen unterstützt. Die jüngste Generation der EMVCo-Branchenstandards – EMV 3D-Secure oder EMV 3D-Secure 2.0 – ist ein robusteres Protokoll und bietet eine stärkere Authentifizierung als die aktuelle Version (3D-Secure 1.0). EMV 3DS entspricht den Bedürfnissen der modernen Zahlungsverkehrslandschaft und verbessert den digitalen Bezahlvorgang, weil das Betrugsrisiko weiter gesenkt, irrtümliche Ablehnungen verringert und unnötige Irritationen vermieden werden.

Das neue EMV 3D-Secure hilft dabei, Verbraucher bei E-Commerce-Zahlungen und anderen Prozessen wie wiederkehrenden Vorgängen und Zahlungen mit bereits registrierten Kundendaten korrekt zu identifizieren. Mastercard und die Zahlungsverkehrsbranche implementieren EMV 3DS und setzen damit neue Authentifizierungsstandards, die die Sicherheit weiter erhöhen und den Bezahlvorgang für Nutzer aller digitalen Kanäle vereinfachen. Und das über die traditionellen Web-Browser-/PC-Schnittstellen hinaus auch überall dort, wo Karteninhaber einkaufen – mit dem Mobiltelefon, dem Tablet oder anderen smarten Geräten sowie bei In-App Käufen.

F: Warum wird EMV 3D-Secure aus der Version 1.0 in EMV 3D-Secure 2.0 überführt?

A: 3DS 1.0.2-Protokolle wurden 2002 eingeführt, um das Betrugsrisiko im E-Commerce (Card-Not-Present, kurz CNP) zu senken. Mastercard und andere Mitglieder der EMVCo-Normenorganisation haben erkannt, dass sie den technologischen Veränderungen und den gewandelten Verbraucher-anforderungen der letzten Jahre Rechnung tragen müssen. Daher haben sie einen überarbeiteten Normenkatalog, genannt EMV 3D-Secure, entwickelt, der digitale Zahlungen sicherer macht und den Einkaufsvorgang für Verbraucher vereinfacht.

F: Welche Vorteile bringt EMV 3D-Secure 2.0 gegenüber 3D-Secure 1.0?

A: Die neuen Standards und der neue Leistungskatalog im Rahmen von EMV 3D-Secure tragen zu mehr Sicherheit, Rentabilität und optimalem Nutzerkomfort bei. Ganz konkrete Änderungen im Rahmen des neuen Standards beinhalten:

- Den Ersatz statischer Passwörter durch eine stärkere Zwei-Faktor-Authentifizierung
- Die Unterstützung neuer Bezahlmöglichkeiten z. B. In-App- und mobile Zahlungen
- Die Möglichkeit, zehnmal mehr Daten auszutauschen als unter 3DS 1.0

- Die Unterstützung weiterer Verwendungsfälle wie etwa hinterlegte Karten registrierter Nutzer, elektronische Börsen, Tokenisierung (also der Einsatz verschlüsselter Dateien, sogenannter Tokens, anstelle der hinterlegten Kartennummer) etc.
- Verbesserte Entscheidungsfindung dank zusätzlich vom Händler übermittelter Daten

Weitere Informationen zu den EMVCo-Ressourcen finden Sie unter: EMV 3-D Secure Page – **https://www.emvco.com/emv-technologies/3d-secure/**.

F: Was bedeutet EMV 3D-Secure für die Karteninhaber?

A: Verbraucher wünschen sich maximale Sicherheit bei ihren digitalen Einkäufen, sind aber gleichzeitig frustriert, wenn sich der Bezahlvorgang von Gerät zu Gerät unterscheidet, nicht überall reibungslos funktioniert und sie sich zudem Dutzende statische Passwörter merken müssen. EMV 3DS erleichtert Karteninhabern das Leben – Zahlungen werden sicherer und folgen immer dem gleichen Schema – auf dem PC ebenso wie auf allen anderen Geräten und Kanälen.

Weil die neuen Standards die Weitergabe umfangreicherer Authentifizierungsdaten ermöglichen, können viele Transaktionen an der virtuellen Kasse in Echtzeit unterbrechungsfrei authentifiziert werden. Wenn eine Authentifizierung nötig wird, können sich Karteninhaber über benutzerfreundliche Methoden wie Einmalpasswörter oder biometrische Verfahren ausweisen und müssen sich keine Passwörter merken.

F: Wie unterstützen zusätzliche, umfangreichere Authentifizierungsdaten die risikobasierte Authentifizierung (RBA)?

A: Das EMV 3DS-Nachrichtenprotokoll unterstützt einen umfangreicheren Datenaustausch zwischen dem Händler und dem Kartenherausgeber, bei dem unter anderem der Kategoriecode des Händlers (Merchant Category Code, kurz MCC), der Risikoindikator des Händlers, wichtige Adressen (z. B. Liefer-, Rechnungs-, E-Mail-Adresse etc.) sowie Gerät, Standort und Verhaltensmuster übermittelt werden. Diese umfangreicheren Daten ermöglichen zusätzliche RBA-Entscheidungen, d. h. Kartenherausgeber können jede Authentifizierungsanfrage überprüfen, ihre Anstrengungen zur Betrugsprävention aber auf die risikoreichsten Vorgänge konzentrieren. Welche dies sind, ermitteln sie über Verhaltens- und Transaktionsinformationen, die durch ein Risikomodell validiert werden. Als sicher eingestufte Vorgänge werden ohne Weiteres authentifiziert, während für Transaktionen mit potenziell höherem Risiko eine Authentifizierung verlangt wird.

Die RBA soll:
- die Zahl der reibungslos erfolgenden Transaktionen für Karteninhaber erhöhen
- die Zahl der Transaktionen, die eine aktive Authentifizierung erfordern, minimieren
- den Kundenkomfort an der virtuellen Kasse steigern

Mastercard empfiehlt Kartenherausgebern, den Anbieter ihres Zugriffs-Kontroll-Servers (ACS-Anbieter) hinsichtlich der von ihm unterstützten Optionen zu kontaktieren. Weiterführende Informationen über die risikobasierte Authentifizierung enthält das Grundlagenpapier, das Sie über den folgenden Link herunterladen können: **https://www.mastercard.com/us/company/en/docs/rba_secure_code_HR.pdf**.

F: Wie passt EMV 3D-Secure in die Sicherheitsstruktur von Mastercard?

A: Alle Mastercard Produkte und Dienstleistungen, die eine Authentifizierung verlangen, profitieren von EMV 3DS und dem hierdurch gesteigerten Kundenkomfort. Mastercard hilft Kartenherausgebern und Händlern dabei, den kartenbasierten Bezahlvorgang mithilfe des zusätzlichen Datenaustauschs für die Karteninhaber reibungsloser, einfacher und sicherer zu gestalten. Die neuen Standards erweitern auch die Strategien von Mastercard für die Entscheidungsfindung mittels risikobasierter Authentifizierung (RBA) und unterstützen Identifizierungs- und Legitimationsprozesse (Identity and Verification, kurz ID&V).

F: Was verbirgt sich hinter Mastercard® Identity Check™?

A: Mastercard Identity Check ist ein globales Authentifizierungsprogramm und setzt auf dem Mastercard® SecureCode™ Programm auf. Es arbeitet mit den neuen EMV 3D-Secure-Standards, um digitale Transaktionen sicher und einfach zu gestalten und einen gesteigerten Anteil an genehmigten Transaktionen zu erreichen, indem die Authentifizierung für Karteninhaber und Händler über alle E-Commerce-Kanäle hinweg verbessert wird. Das Programm nutzt ausschließlich branchenführende, nutzerfreundliche Verifizierungsmethoden und kombiniert diese mit wichtigen Leistungsindikatoren, um die Betrugsraten niedrig zu halten und den Kundenkomfort zu optimieren.

F: Welches Problem löst Mastercard Identity Check für Kartenherausgeber und Händler?

A: Mastercard Identity Check adressiert zentrale Sicherheits-, Ertrags- und Regulierungsbedürfnisse.

- **Schneller Anstieg der Betrugsraten im E-Commerce (Card-Not-Present, kurz CNP)**
  Nachdem Chipkarten im stationären Geschäft mittlerweile zum fest etablierten Sicherheitsstandard geworden sind, konzentrieren sich Betrüger nun auf die digitale Welt. Hinzu kommen die heute üblichen schwachen Authentifizierungsmethoden (wie z. B. statische Passwörter). Daher dürfte CNP-Betrug die Betrugsraten im stationären Handel im Jahr 2018 um das Vierfache übersteigen.[1] Für Kartenherausgeber und Händler kann CNP-Betrug zu Einkommensverlusten und höheren Kosten führen.

- **Viele irrtümliche Ablehnungen**
  Um den hohen Verlusten aus CNP-Betrug vorzubauen, lehnen Kartenherausgeber im E-Commerce derzeit viermal häufiger Karten ab als bei Präsenzgeschäften. Die Verluste der Kartenherausgeber aus irrtümlich abgelehnten Transaktionen und sinkenden künftigen Ausgaben verärgerter Karteninhaber übersteigen die Verluste aus Betrug beinahe um das Vierfache.[2]

- **Hohe Abbruchraten**
  Im Durchschnitt verwenden Verbraucher pro Woche mehr als 10 passwortgeschützte Konten, Geräte oder Applikationen, und weil nach eigenen Angaben 84 % ihre Passwörter vergessen, nutzt mehr als jeder fünfte Verbraucher ein und dasselbe Passwort für mehrere Webseiten. Tatsächlich brechen Verbraucher etwa ein Drittel ihrer Online-Käufe an der virtuellen Kasse einfach deshalb ab, weil sie sich nicht mehr an ihr Passwort erinnern. Ein weiteres Drittel gibt an, dass sie aus diesem Grund eine Rabattaktion oder ein exklusives Angebot nicht wahrnehmen konnten.[3]

- **Neuer Regulierungsdruck**
  Die Europäische Bankenaufsicht (EBA), die technischen Regulierungsstandards (Regulatory Technical Standards, RTS) und die überarbeitete Zahlungsdiensterichtlinie (Payment Services Directive, PSD2) schreiben zur Bekämpfung von CNP-Betrug stärkere Authentifizierungsmethoden vor. Entsprechend sind Kartenherausgeber und Händler gefordert, eine sicherere und verbraucherfreundliche Lösung zu finden.

F: Welche Vorteile hat Mastercard Identity Check für Kartenherausgeber und Händler?

A: Mit Mastercard Identity Check können Kartenherausgeber und Händler die einfachen Bezahllösungen anbieten, die sich Verbraucher wünschen, und gleichzeitig das Betrugsrisiko senken und mehr genehmigte Transaktionen erreichen:

- neue Standards in Sachen Kundenfreundlichkeit beim digitalen Bezahlen setzen
- die betrugsanfälligen statischen Passwörter und Sicherheitsfragen abschaffen
- risikobasierte Klassifizierung fördern – nur besonders riskante Transaktionen müssen überprüft werden, während andere ohne Einbeziehung des Verbrauchers bearbeitet werden

[1] JAVELIN STRATEGY & RESEARCH, 2015 DATA BREACH FRAUD IMPACT REPORT, 2015.
[2] JAVELIN STRATEGY & RESEARCH, 2015 THE IMPACT OF FRAUD AND CHARGEBACK MANAGEMENT ON OPERATIONS, 2015.
[3] KETCHUM GLOBAL RESEARCH & ANALYTICS, SURVEY OF CONSUMERS IN 17 COUNTRIES COMMISSIONED BY MASTERCARD, 2015.

- zur Verringerung der Transaktionsabbruchraten beitragen und die Abschlussraten im Distanzgeschäft verbessern
- mehr Akzeptanz für digitales Bezahlen schaffen und Transaktionswachstum generieren
- mobile Geräte, über die künftig die meisten E-Commerce-Geschäfte abgeschlossen werden, als Authentifizierungsmedium nutzen

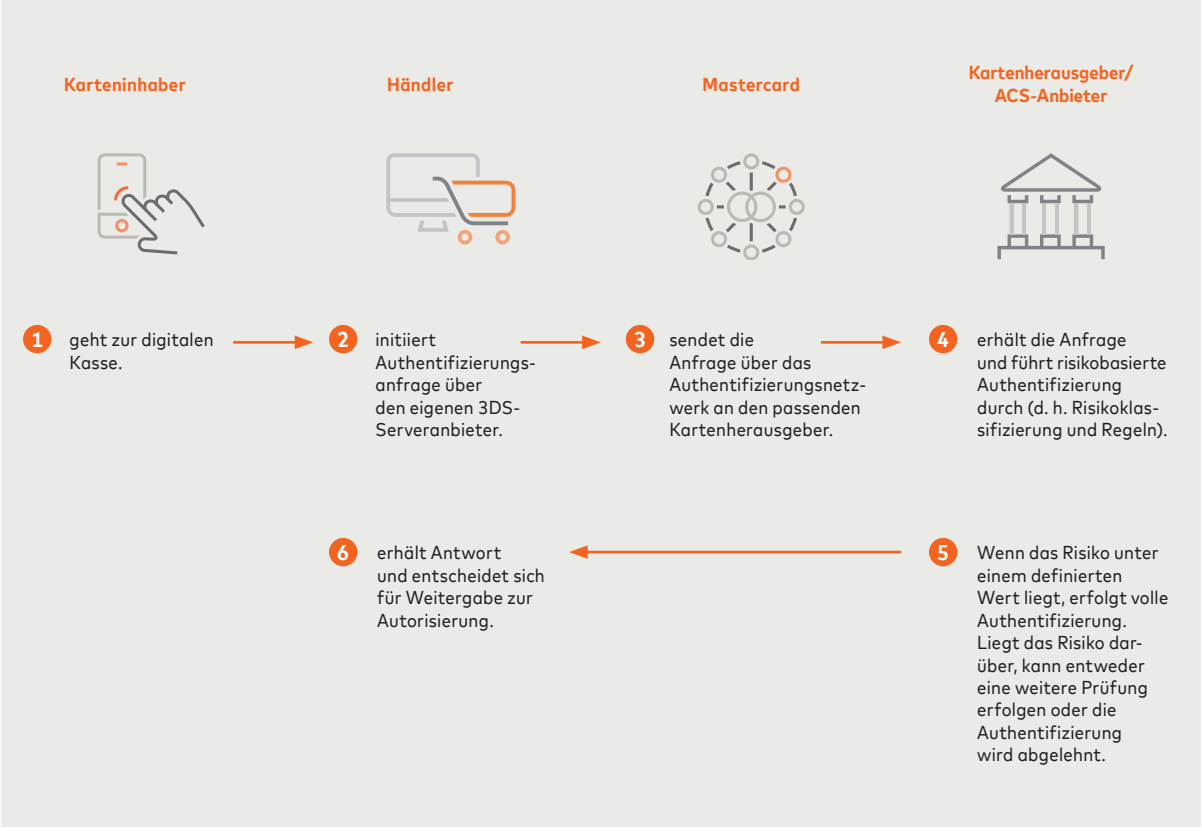
F: Was unterscheidet Mastercard® Identity Check™ von Mastercard® SecureCode™?

A: Mastercard Identity Check baut auf dem bestehenden Mastercard SecureCode Programm auf und wird mithilfe des bestehenden 3DS 1-Protokolls eingeführt. Anders als bei SecureCode müssen sich die Verbraucher bei Mastercard Identity Check jedoch kein statisches Passwort merken und dieses verwenden. Durch den Wegfall vieler ärgerlicher Begrenzungen, die durch statische Passwörter entstehen, gewinnen die Verbraucher eine einfache und sichere Möglichkeit, Online-Käufe zu tätigen. Das hilft Kartenherausgebern und Händlern dabei, die Kundenbindung zu erhöhen, Betrug zu verringern und Einnahmen zu steigern.

Mastercard Identity Check beinhaltet das neue EMV 3D-Secure-Protokoll: Es ermöglicht E-Commerce-Transaktionen über noch mehr Geräte und Anwendungen, die Verwendung umfangreicherer Daten für risikobasierte Authentifizierung anstelle von weiteren Interaktionen mit dem Karteninhaber und gibt Kartenherausgebern und Händlern größere Kontrolle.

F: Wie funktioniert Mastercard Identity Check?

A: Mastercard Identity Check arbeitet mit einem neuen Regelwerk und fördert geeignete Vorgehensweisen für optimalen Zahlungskomfort:



In den meisten Fällen werden die Transaktionen unterbrechungsfrei ablaufen. Dennoch zeigen wir hier auf, wie das Programm mit intelligenten Stopps funktioniert: Stellen Sie sich eine Karteninhaberin vor, die online über ein Gerät oder einen Browser einkauft. Nach Eingabe der Zahlungsinformationen meldet sich ihr Smartphone und fordert sie auf, die Transaktion zu dem Kaufvorgang auf zwei mögliche Arten abzuschließen:

1. Die Karteninhaberin legt einen Finger auf den Smartphone-Scanner oder schaut mit dem Auge in ihre Kameralinse und macht ein „Selfie", um ihre Identität zu bestätigen. Sobald ihre Identität überprüft wurde, kann die Karteninhaberin auf die Bestellbestätigungsseite des Händlers zurückkehren.
2. Ein einmaliger Code wird vom Kartenherausgeber als SMS-Nachricht auf das Mobilgerät der Karteninhaberin gesendet (das erfordert unter Umständen einen zusätzlichen „Wissensfaktor", um den technischen Regulierungsstandards (RTS) der EBA zu genügen). Sobald sie den Code in der Authentifizierungsseite eingibt und dieser als korrekt bestätigt wird, wird die Karteninhaberin auf die Bestellbestätigungsseite des Händlers zurückgeleitet.

F: Entfällt damit die Pflicht des Händlers, die Identität eines Verbrauchers vollständig zu authentifizieren oder zu überprüfen?

A: Nein, aber Mastercard® Identity Check™ setzt den Anspruch von Mastercard an eine höhere Benutzerfreundlichkeit um, bis hin zu einer Bezahlauthentifizierung, ohne ein ausschließlich wissensbasiertes Merkmal (z. B. Passwort) des Verbrauchers zu benötigen. Stattdessen werden Dinge oder Merkmale genutzt, die Verbraucher besitzen (z. B. Mobiltelefone) und biometrische Kennzeichen wie etwa ein Fingerabdruck.

F: Ist die Teilnahme an Mastercard Identity Check verpflichtend?

A: Mastercard Identity Check ist der Programmnachfolger von Mastercard® SecureCode™. Alle Kartenherausgeber/Acquirer in Europa müssen bis April 2019 (in Zentral- und Osteuropa bis September 2019) Mastercard Identity Check konform sein.

F: Warum ist Mastercard Identity Check der beste Weg, um Konformität mit den neuen EMV 3D-Secure 2.0-Standards zu erreichen?

A: Die digitale Harmonisierung ist eine enorme Chance für Kartenherausgeber und Händler. Infolgedessen kann die Auswahl des richtigen Partners erfolgsentscheidend sein. Mastercard Identity Check baut auf Branchenstandards und eine langfristigen Vision von Mastercard auf und liefert einen gesamtheitlichen Ansatz für EMV 3D-Secure. Mit Investitionen in modernste Technologien wie Biometrik, risikobasierte Authentifizierung und künstliche Intelligenz kann Mastercard Kartenherausgebern und Händlern dabei helfen, ihre Ergebnisse zu verbessern.

F: Welche übergeordneten Implementierungsfragen sind für Mastercard Identity Check wichtig (Codierung, Systemänderungen etc.)?

A: Mastercard Identity Check beinhaltet Anforderungen und geeignete Vorgehensweisen für Kartenherausgeber und Händler. Kartenherausgeber müssen ihre Karteninhaber über eine vom Programm unterstützte Methode verifizieren: dynamisches Passwort, biometrische Prüfung oder eine vergleichbare Methode. Zudem wird dringend empfohlen, im Interesse des optimalen Kundenkomforts einen risikobasierten Ansatz zu wählen.

Händler und Bezahlsystemabwickler haben darüber hinaus eigene Anforderungen, etwa die Bereitstellung eines Konteninhaber-Authentifizierungswerts (Accountholder Authentication Value, AAV) für jede Transaktion.

Teilnehmende Kartenherausgeber und Händler müssen zudem wichtige Leistungsindikatoren erfüllen. Dazu gehören eine jährliche Höchstgrenze für Betrugsfälle trotz vollständig durchgeführter Authentifizierung, ein Mindestmaß an Zahlungsgenehmigungen für ihre eigene Lösung, zwingende Weitergabe von Authentifizierungsdaten und andere Maßnahmen.

Details hierzu finden Sie im Global Operation Bulletin und im Programm Guide, die über **Mastercard Connect** erhältlich sind.

F: Für welche Transaktionen ist Mastercard® Identity Check™ verfügbar?

A: Mastercard Identity Check wurde entwickelt, um alle Mastercard Marken (also Mastercard, Maestro etc.), alle Segmente (also Verbraucher, Geschäftskunden) und Produkte (also Kredit, Debit und Prepaid) abzudecken.

F: Verschiebt sich die Haftung und ändert sich die Interchange-Gebühr?

A: In Europa haften die Acquirer (unabhängig davon, ob der Händler eine EMV 3D-Secure-Nachricht schickt), wenn sie eine nach den technischen Regulierungsstandards (RTS) der EBA geltende Ausnahme von der starken Kundenauthentifizierung anwenden.

F: Welche mobile biometrische „Plug and Play"-Lösung bietet Mastercard Identity Check?

A: Mit der biometrischen Authentifizierung können Finanzinstitute dem Wunsch der Verbraucher nach Sicherheit und Einfachheit über alle Geräte und Kanäle entsprechen. Mastercard Identity Check bietet eine App-basierte mobile biometrische Authentifizierungslösung, mit der die Karteninhaber „Biometrie", wie etwa die Fingerabdrucks-, Gesichts- oder Stimmerkennung, auswählen können, um sich über ihr stets mitgeführtes mobiles Gerät einfach und zugleich sicher ausweisen zu können. Verbraucher werden während jeder Transaktion durch die Messung und Analyse ihrer einzigartigen physischen Merkmale und die Authentizität des im Besitz des Verbrauchers befindlichen Geräts überprüft.

Diese biometrische Lösung besteht aus zwei Komponenten: einer mit dem Benutzer kommunizierenden biometrischen App und einer im Hintergrund arbeitenden biometrischen Authentifizierungsplattform. Sie ist verfügbar als Softwareentwicklungspaket (Software Development Kit, SDK), das in die mobile App eines Kartenherausgebers integriert und für mobiles Banking, Callcenter, verdächtige Transaktionen und digitale Zahlungen benutzt werden kann.

F: Wie funktioniert der Mastercard Identity Check mit anderen Mastercard Produkten?

A: Mastercard unterstützt Händler und Kartenherausgeber dabei, die Chancen der Umstellung auf EMV 3D-Secure optimal zu nutzen. Für Händler bedeutet dies Unterstützung durch APIs im Rahmen des Mastercard Payment Gateway, die zur Unterstützung von EMV 3DS-Transaktionen integriert werden können. Für Kartenherausgeber arbeitet die risikobasierte Authentifizierung (Stand-in-RBA) mit den umfangreichen Daten aus EMV 3DS, um Unterbrechungen bestmöglich zu vermeiden, Risiko zu senken und besser sicherzustellen, dass die Authentifizierungsanfragen von Händlern stets beantwortet werden. Weitere Informationen zu diesen Dienstleistungen erhalten Sie von Ihrem Mastercard Ansprechpartner.

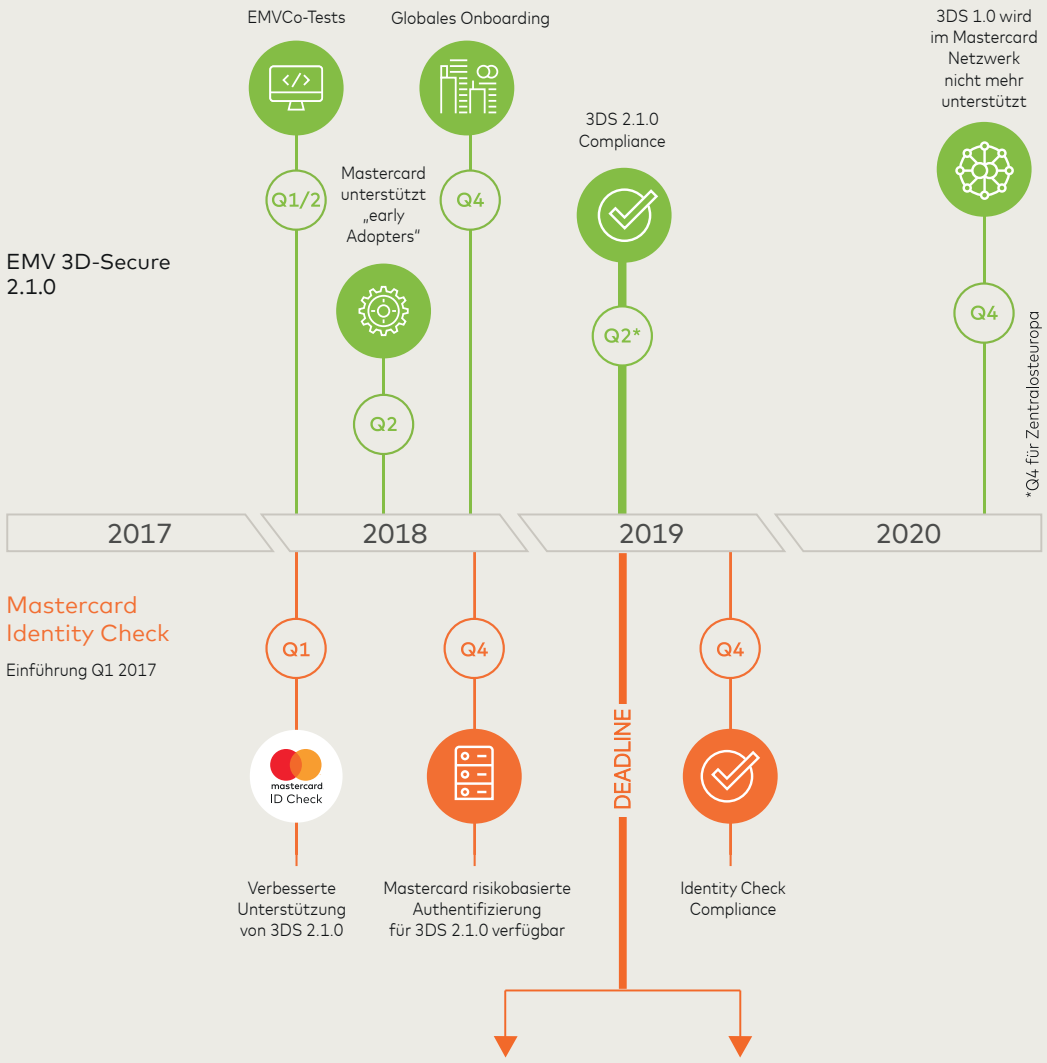
F: Welche Zeitfenster stehen Kartenherausgebern, Händlern und Acquirern zur Verfügung?

A: Die neuen Protokolle werden parallel zu 3DS 1.0 verwendet, um den Übergang zu dem neuen EMV 3DS so reibungslos wie möglich zu gestalten. Dank dieses Ansatzes können die ACS-Anbieter Händlern, die sowohl die alten als auch die neuen Nachrichtenübertragungswege nutzen, besser unterstützen.

Kartenherausgeber und Händler sind damit in der Lage, die Implementierung flexibel an ihre Geschäftsziele und Zeitvorgaben anzupassen.

Mastercard arbeitet wie gewohnt mit Interessensgruppen und Dienstleistern weltweit zusammen, um die Umstellung zu begleiten. Der folgende Fahrplan soll dabei helfen, die Umsetzung bis hin zur vollständigen Konformität mit EMV 3D-Secure 2.0 zu planen.

Zeitschiene: Umstellung von Mastercard® SecureCode™/3D-Secure 1 auf Mastercard® Identity Check™ und das neue EMV 3D-Secure



Region Europa	Deadline Acquirer	Deadline Kartenherausgeber
Großbritannien und nordische Länder	1. April 2019	1. April 2019
Westeuropa	1. April 2019	1. April 2019
Deutschland und Schweiz	1. April 2019	1. April 2019
Zentralosteuropa	1. September 2019	1. September 2019
HGEM (Wachstumsmärkte)	31. Dezember 2019	31. Dezember 2019

Um das Zusammenspiel zwischen 3DS 1.0 und dem neuen EMV 3DS, 3DS-Servern sowie ACS zu gewährleisten, müssen die Anbieter sowohl 3DS 1.0 als auch EMV 3DS-Prozesse unterstützen, bis Mastercard SecureCode und 3DS 1.0 abgelöst werden.

- 3DS-Server (früher unter der Abkürzung MPI bekannt), werden so konzipiert, dass sie für Händler sowohl 3DS 1 als auch EMV 3DS unterstützen
- Zugriffs-Kontroll-Server (Access Control Servers) werden so konzipiert, dass sie für Karten-herausgeber sowohl 3DS 1 als auch das neue EMV 3DS unterstützen
- Kartenherausgeber müssen für sämtliche Karten sowohl 3DS 1 als auch das neue EMV 3DS unterstützen

F: Welche Testanforderungen hat Mastercard?

A:
- **ACS-Anbieter** müssen Mastercard zufriedenstellende Testergebnisse eines externen EMVCo-Testlabors vorlegen, bevor sie zusammen mit Mastercard die ACS-Programmtests beginnen können, die auch spezifisch auf Programmvorschriften von Mastercard zugeschnittene Testfälle beinhalten.
- **Kartenherausgeber und Händler,** die mit externen Anbietern arbeiten, sollten von diesen zusätzliche Informationen zur Produktverfügbarkeit anfordern.
- Unabhängig davon, ob **Acquirer** einen oder mehrere Gateways/Prozessoren/Zahlungsdienstleister nutzen oder die Software eines Gateways/Zahlungsdienstleisters kaufen und verwenden, müssen Acquirer beide Nachrichtentypen (3DS 1.0 und EMV 3DS 2.0) unterstützen. Bitte berücksichtigen Sie, dass App-basierte Transaktionen nicht über den alten Standard abgewickelt werden können, da diese nur von den neuen EMV 3DS-Standards unterstützt werden.

F: Welche Kosten sind mit diesem Service verbunden?

A: Bitte entnehmen Sie diese Informationen Ihren regionalen Preislisten oder dem Mastercard Billing Services Guide für die Nutzungsgebühren des Mastercard Directory Servers.

Weitere Informationen zu EMV 3D-Secure oder Mastercard® Identity Check™ erhalten Sie von Ihrem Mastercard Ansprechpartner.

EMV 3D-Secure (EMV 3DS) und Mastercard® Identity Check™

Weitere häufige Fragen

F: Welches Regulierungsumfeld gilt in Europa – PSD2?

A: Die überarbeitete Zahlungsdiensterichtlinie der Europäischen Kommission (PSD2) ist am 13. Januar 2018 in Kraft getreten und wird den Bezahlvorgang für Verbraucher im digitalen Zeitalter transformieren. PSD2 ebnet den Weg für mehr Innovation, Wettbewerb und Effizienz. Sie führt höhere Sicherheitsstandards für Online-Zahlungen ein – Verbraucher fühlen sich dadurch künftig wohler beim Online-Kauf.

Die Sicherheitsvorschriften von PSD2, zu denen auch die Verwendung einer starken Kunden-authentifizierung (SCA) für elektronische Zahlungen zählt, beeinflussen den Kundenkomfort am stärksten und geben Finanzinstituten in Europa die Chance, das Einkaufserlebnis für Kunden attraktiv zu gestalten und entsprechend zu profitieren.

Besonders wichtig wird dabei der Nutzerkomfort auf mobilen Endgeräten sein. Bis 2021 existieren vermutlich 11,6 Mrd. internetfähige Geräte, fast drei Viertel davon sind „smarte" Geräte[1]. Auch das digitale und mobile Banking wird für Verbraucher zunehmend alltäglich: Bis 2020 dürften 2 Mrd. Menschen und damit über ein Drittel der Erwachsenen weltweit mobiles Banking nutzen[2]. In diesem neuen, dynamischen Umfeld müssen sowohl die Banken als auch die Einzelhändler schnell reagieren, um Kunden auf sich aufmerksam zu machen, zu gewinnen, an sich zu binden und den bestmöglichen Komfort zu bieten.

F: Wie soll PSD2 Online-Betrug verhindern?

A: PSD2 will über eine höhere Zahl von Transaktionen mit starker Kundenauthentifizierung gegen Online-Betrug vorgehen. Starke Kundenauthentifizierung (Strong Customer Authentication, SCA) ist ein verpflichtender Bestandteil der PSD2 und sorgt für hohen Kundenschutz und hohe Sicherheit von Zahlungen. Sie wird immer dann erforderlich, wenn ein Kunde (persönlich, mobil oder mit hinterlegten Kartendaten) einen elektronischen Zahlungsvorgang auslöst oder eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder eines anderen Missbrauchs birgt.

Sowohl Finanzinstitute als auch Händler benötigen neue Produkte und Lösungen, um starke Kundenauthentifizierung leisten zu können und während der Online-Zahlung eine Echtzeit-Karten-inhaberauthentifizierung zu ermöglichen. Bei guter Umsetzung kann SCA nicht nur die Sicherheit von Online-Zahlungen erhöhen, sondern den Bezahlvorgang für Verbraucher auch revolutionieren, ihn bequemer gestalten und zu mehr Kundenresonanz und -treue führen.

[1] CISCO VISUAL NETWORKING INDEX 2017: GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2016–2021 WHITE PAPER
[2] JUNIPER RESEARCH, PRESS-RELEASE/MOBILE-BANKING-USERS 2016

Über verbraucherfreundliche Authentifizierungstechnologien wie biometrische Identifizierung (z. B. Fingerabdruckscanner) eliminiert die SCA die Verwendung betrugsanfälliger statischer Passwörter und Sicherheitsfragen. Zudem sinkt auch die Wahrscheinlichkeit, dass Verbraucher Online-Käufe nicht abschließen, weil sie ihre Passwörter vergessen haben. Und SCA nutzt mobile Geräte, über die künftig das meiste E-Commerce-Geschäft abgeschlossen werden dürfte, als Authentifizierungsmedium. Sie legt die Authentifizierung damit sprichwörtlich in die Hand der Verbraucher.

F: Was ist starke Kundenauthentifizierung?

A: Die PSD2 verlangt eine Authentifizierung auf Grundlage zweier der folgenden Elemente:

- Wissen – „etwas, das nur der Nutzer weiß" (z. B. statisches Passwort, Code, PIN)
- Eigentum – „etwas, das nur der Nutzer besitzt" (z. B. Token, Smart Card, Mobiltelefon)
- Inhärenz – „etwas, das der Nutzer ist" (z. B. biometrische Daten)

Hier handelt es sich um einen Ansatz der „mehrstufigen Sicherheit": Die zwei Authentifizierungselemente müssen unabhängig voneinander sein. Auf diese Weise bleibt das jeweils andere unberührt, wenn ein Element missbräuchlich verwendet wird. Die SCA ist für Transaktionen zu verwenden, in denen sowohl der Kartenherausgeber als auch der Acquirer in einem EWR-Land ansässig sind (der Händler muss nicht in einem EWR-Land ansässig sein). Die technischen Regulierungsstandards (Regulatory Technical Standards, RTS) der PSD2 sehen auch diverse Ausnahmen vor, bei denen auf eine SCA für Transaktionen verzichtet werden kann, z. B. bei Kleinstbetragszahlungen oder Zahlungen an vertrauenswürdige Empfänger. Die Ausnahmen sind jedoch nicht verpflichtend anzuwenden, d. h. Zahlungsdienstleister (also Kartenherausgeber und Acquirer) können sich auch dazu entscheiden, grundsätzlich mit SCA zu arbeiten.

F: Was sind die wichtigsten Ausnahmen, die nach den EBA RTS erlaubt sind?

A: Ausnahmen für Online-Transaktionen beinhalten

- **Kleinstbetragszahlungen**
  - Unter 30 €
  - Der kumulierte Betrag beträgt weniger als 100 € oder überschreitet nicht 5 aufeinander folgende Transaktionen
  - Über 30 € gemäß Transaktionsrisikoanalyse (TRA)
- **Transaktionsrisikoanalyse (TRA)**
  - Betrugsraten- und risikobasierte Authentifizierung (RBA)
  - Der Transaktionsbetrag ist niedriger als oder gleich dem Ausnahmeschwellenwert
  - Maximaler Vorgangswert < 500 €
- **Wiederkehrende Transaktionen**
  - Nur für denselben Betrag, Transaktionen mit demselben Zahlungsempfänger
  - Die erste Transaktion und sämtliche Änderungen erfordern Authentifizierung
- **Positivliste vertrauenswürdiger Empfänger**
  - Der Karteninhaber verwaltet die Liste vertrauenswürdiger Empfänger
  - Der Kartenherausgeber hat das letzte Wort

Ausnahmen für Präsenztransaktionen beinhalten

- **Kontaktlose Kleinstbetragszahlungen**
  - Neue Regeln auf Basis des Einzel- und Kumulativ-Werts oder der Anzahl der aufeinander-folgenden Transaktionen
  - Transit/Parken
- **Zahlungskontoinformationen**
  - Maximal 90 Tage an Transaktionsinformationen
  - Kontosalden

Mastercard verbessert den 3D-Secure-Informationsfluss, damit SCA-Ausnahmen für Online-Transaktionen effizienter genutzt werden können.