EMV 3-D Secure

- Regulatorische Anforderungen
  - EBA Mandat
  - 3DS 2.0
  - Haftungsverschiebung
  - 3DS 2.0 und Compliance zur DSGVO
  - Ausnahmen und Ausklammerungen der PSD2 SCA
- Computop Paygate
  - Authentisierungs-Optionen
  - Message Version 2
  - Handhabung von Soft decline
    - WICHTIG:
      - Whitelisting von vertrauenswürdigen Begünstigten
      - Transaktionen mit geringem Wert
      - Transaktionsrisikoanalyse
      - One-Leg-Out-Transaktionen

Regulatorische Anforderungen

EBA Mandat

Die Europäische Bankenaufsichtsbehörde (EBA) hat angeordnet, dass alle Zahler, die online auf ihr Zahlungskonto zugreifen und elektronische Zahlungstransaktionen über einen Remote-Kanal auslösen, beginnend ab 14. September 2019 stark authentisiert werden müssen (alias Starke Kundenauthentisierung (SCA)). Die Kartenorganisationen haben diese Möglichkeit ergriffen, um das etablierte Protokoll 3D-Secure für die Karteninhaber-Authentisierung zu überarbeiten und mehrere Probleme anzugehen, welche die Annahme im Markt gebremst haben.

3DS 2.0

Bisher hatten Internethändler die Wahl, dem Karteninhaber eine Challenge (z.B. TAN / Passwort) zu präsentieren oder 3DS gänzlich zu übergehen. Einige haben einen dynamischen Ansatz basierend auf dem PSP oder der eigenen Risikobewertung gewählt, aber viele Händler schätzten einen reibungslosen Kassenvorgang und hohe Konversionsraten mehr als die möglichen Vorteile einer Haftungsverschiebung. Die Gesamtstrategie der Kartenorganisationen für 3DS 2.0 ist es, Reibereien durch eine verbesserte Erfahrung der Karteninhaber (Geräte-Bewusstsein) zu verringern und Ausnahmen von der SCA basierend auf einer robusten Transaktionsrisikoanalyse (TRA) auszunutzen mit dem obersten Ziel, optimale Autorisierungsleistung und Konversionsraten zu erreichen. Daher ist die TRA entscheidend für reibungslose Zahlungsabläufe für Remote-Transaktionen mit geringem Risiko. Deshalb hat das Protokoll 3DS 2.0 eine Unmenge zusätzlicher Datenpunkte eingeführt, die dem Kartenherausgeber zur Unterstützung der Transaktionsrisikoanalyse und für die Anwendung von Ausnahmen der SCA übermittelt werden können.

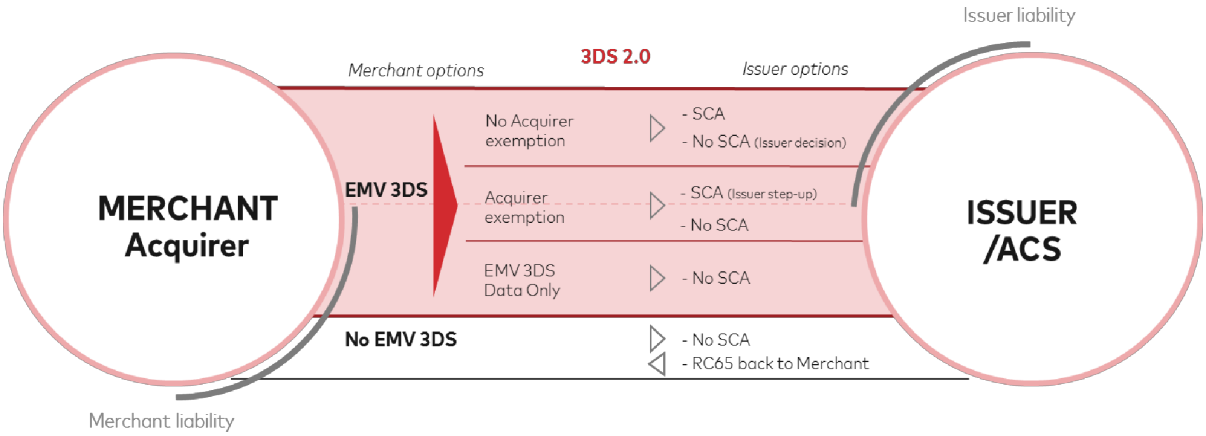
SCA wird erforderlich, wenn:

- die Transaktion nicht außerhalb vom Geltungsbereich der PSD2 RTS ist
- keine Ausnahme der PSD2 SCA für eine Zahlungstransaktion zutrifft
- eine Karte zu einer Händler-Datenbank hinzugefügt wird (hinterlegte Karte)
- eine Vereinbarung für wiederkehrende Zahlungen über feste oder variable Beträge beginnt, einschließlich der Festlegung des anfänglichen Mandats für vom Händler ausgelöste Transaktionen (MIT)
- eine Vereinbarung für wiederkehrende Zahlungen zu einem höheren Betrag geändert wird (beispielsweise ein Premium-Angebot)
- ein White-Listing eingerichtet wird (oder zum Ansehen/Ändern von White-Lists)
- ein Gerät mit einem Karteninhaber verknüpft wird

Haftungsverschiebung

Als Daumenregel gilt, wenn die Authentisierung des Karteninhabers über 3-D Secure erfolgt ist, sind Händler normalerweise vor Streitigkeiten bezüglich Betrug im E-Commerce geschützt und die Haftung verschiebt sich vom Händler / Acquirer zum Kartenherausgeber. Es gibt jedoch Ausnahmen vom Schutz des Händlers vor Streitigkeiten. Im Kontext von 3DS 2.0 sind Händler regelmäßig nicht geschützt, falls gewährte Ausnahmen gemäß PSD2 RTS aktiv vom Händler / Acquirer angefragt worden sind.

Das folgende Diagramm zeigt Optionen und Haftungen unter den Anforderungen von PSD2 RTS gemäß MasterCard.

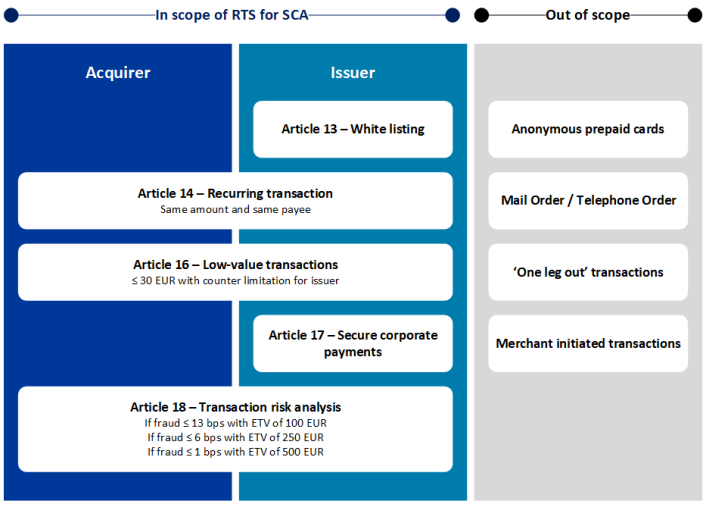


3DS 2.0 und Compliance zur DSGVO

Karteninhabern müssen ausführliche Informationen darüber gegeben werden, wie ihre Daten erfasst, verarbeitet und verwendet werden. Das kann über eine Datenschutzerklärung erreicht werden, die mindestens die Arten der verarbeiteten Daten, den Zeck ihrer Verarbeitung, die verwendeten Daten usw. enthält. Kartenorganisationen und Kartenherausgeber verwenden die EMV 3DS Daten für keinen anderen Zwecke als Betrugsprävention und Authentisierung. Das schließt die Verwendung persönlicher Daten für andere Zwecke wie Verkauf, Marketing und Data-Mining (außer zur Betrugsprävention) aus.

Ausnahmen und Ausklammerungen der PSD2 SCA

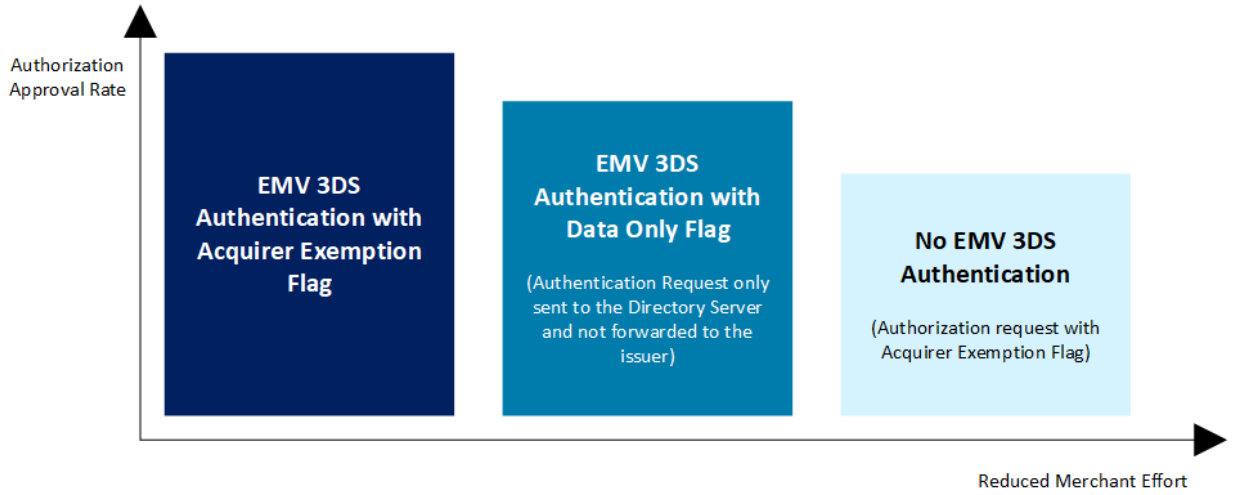
Gemäß den technischen Regulierungsstandards (RTS) gibt es einige wichtige Ausnahmen der SCA, die unter verschiedenen Bedingungen gelten können, welche im folgenden Diagramm dargestellt sind.



Computop Paygate

Authentisierungs-Optionen

Einem Acquirer kann erlaubt sein, infolge geringer Betrugsraten und TRA die SCA nicht anzuwenden. Für diese Ausnahmen gibt es verschiedene Optionen zur Verarbeitung, die im folgenden Diagramm dargestellt sind.



Standardmäßig schlägt Computop Paygate anwendbare Ausnahmen (sofern unterstützt) im EMV 3DS Authentisierungsablauf dem Kartenherausgeber vor, um die bestmöglichen Zustimmungsraten der Autorisierung zu erreichen.

EBA-Op-2018-04, Paragraph 47 - Klartstellung zu PSP (Acquirer-Betrugsraten)

Die Betrugsrate ist im Anhang A der RTS definiert und wird für alle Überweisungs-Transaktionen und alle Kartenzahlungen berechnet und kann nicht pro einzelnem Zahlungsempfänger (z.B. Händler) oder pro Kanal (entweder App oder Web-Schnittstelle) definiert werden. Die Betrugsrate, die bestimmt, ob sich ein PSP für die SCA-Ausnahme qualifiziert oder nicht, kann nicht nur für bestimmte Händler berechnet werden, d.h. wenn der Zahler eine Zahlung an einen bestimmten Händler leisten möchte und dieser bestimmte Händler eine Betrugsrate unter dem Grenzwert hat. Während der PSP (Acquirer) des Zahlungsempfängers vertraglich vereinbaren kann, die Überwachung seiner Transaktionsrisikoanalyse an einen gegebenen Händler 'outzusourcen' oder nur bestimmten vordefinierten Händlern erlauben kann, von den Vorteilen von dieser PSP-Ausnahme zu profitieren (basierend auf einer vertraglich vereinbarten geringen Betrugsrate), muss die Betrugsrate, welche einen bestimmten PSP für eine Ausnahme gemäß Artikel 18 geeignet macht, dennoch auf Basis der ausgeführten oder akquirierten Transaktionen vom PSP des Zahlungsempfängers berechnet werden und nicht ausgehend von den Transaktionen des Händlers.

Message Version 2

Um die Menge der zusätzlichen zahlungsfremden Daten zu handhaben und die Abwärtskompatibilität soweit wie möglich zu erhalten, hat sich Comput op dafür entschieden, seine Paygate-Kartenschnittstelle über den zusätzlichen Parameter **MsgVer** zu versionieren. Die aktualisierte API basiert weiterhin auf Schlüssel-Wert-Paaren, aber setzt stark auf Base64-codierte JSON-Objekte zur Unterstützung der Lesbarkeit und Skript-Nutzung auf der Client-Seite.

Händler können weiterhin unsere klassische Schnittstelle für Anfragen auch mit 3DS 2.0 verwenden, aber es gibt ein paar Einschränkungen:

- Viele zusätzliche Datenpunkte für die Risikoanalyse des Kartenherausgebers sind nicht verfügbar und daher kann die Quote der reibungslosen Transaktionen geringer sein
- Antworten und Benachrichtigungen der API enthalten neue JSON-Objekte, um für die Spezifikationen des Protokolls 3DS 2.0 zu sorgen und erfordern eine Modifikation vorhandener Händler-Integrationen

Aus diesen Gründen ist es sehr empfohlen, auf die Version 2 zu aktualisieren.

Handhabung von Soft decline

Falls eine Transaktion keine SCA hat, können Kartenherausgeber mit einem sogenannten Soft decline reagieren. Das bedeutet, die Autorisierung der Transaktion wird vom Kartenherausgeber angelehnt, dieselbe Transaktion kann jedoch erneut initialisiert werden. Der Hauptgrund für Soft declines im Kontext von 3D Secure ist, dass Kartenherausgeber die vom Händler angefragten SCA-Ausnahmen nicht akzeptieren, wenn diese direkt zur Autorisierung gesendet werden oder wenn der eine Zahlung ohne zuvor durchgeführte Authentisierung anfordert. Die beste Methode ist es dann, die Zahlung mit 3DS neu zu starten.

Mit der **Automatischen Handhabung von Soft Decline** reagiert das Computop Paygate je nach Konfiguration auf eine Soft decline Antwort mit einem automatischen Neustart der Zahlung mit erzwungener SCA. Das Computop Paygate erzeugt dann automatisch eine neue Zahlung im Namen des Händlers und integriert den 3DS-Ablauf.

WICHTIG:

- Aus Sicht des Kunden bemerkt dieser keinen Unterschied und muss seine Kreditkartendaten nicht erneut eingeben. Der gesamte Prozess wird vom Computop Paygate gesteuert.
- Beachten Sie bitte, dass diese Lösung für **Server-zu-Server** Verbindungen nicht verfügbar ist, weil das Computop Paygate den Client (Browser) nicht zum Start des 3DS-Ablaufes steuern kann. Für Server-zu-Server-Verbindungen muss der Händler die Zahlung mit 3DS-Ablauf neu auslösen und vor allem die SCA-Challenge über den angegebenen Parameter JSON threeDSPolicy (*challengePreference* = *mandateChallenge*) erzwingen.

Whitelisting von vertrauenswürdigen Begünstigten

Ein Karteninhaber dafür optieren, einen Händler zu einer Liste vertrauenswürdiger Begünstigter hinzuzufügen, die beim Kartenherausgeber geführt wird, um diesen speziellen Händler bei zukünftigen Zahlungen von der SCA auszunehmen. Das passiert normalerweise während einer Challenge des Karteninhabers, aber Karteninhaber können beispielsweise auch über ihre Banking-App eine Liste vertrauenswürdiger Begünstigter verwalten.

Händler können von einer Whitelist-Ausnahme profitieren, wenn diese angefragt ist und wenn nicht anderweitig eine Challenge des Karteninhabers gefordert ist.

> Beachten Sie bitte, dass die Whitelist-Funktion ab 3DS Version 2.2 und höher verfügbar ist. Derzeit unterstützten die Kartenherausgeber meistens 3DS 2.1.

Transaktionen mit geringem Wert

Kartenherausgeber können Transaktionen von der SCA ausnehmen, sofern die folgenden Bedingungen erfüllt sind:

- der Zahlungsbetrag übersteigt nicht 30 Euro,
- der kumulierte Betrag vorheriger Zahlungstransaktionen ohne SCA übersteigt nicht 100 Euro,
- die Anzahl der vorherigen Zahlungstransaktionen ohne SCA übersteigt nicht fünf aufeinanderfolgende Zahlungstransaktionen.

Beachten Sie bitte, dass die Ausnahmen für geringen Wert angefragt werden müssen, um für einen reibungslosen Authentisierungs-Ablauf berücksichtigt zu werden.

Transaktionsrisikoanalyse

Acquirer und Kartenherausgeber dürfen auf die SCA verzichten, sofern die gesamte Betrugsrate nicht höher als die Referenz-Betrugsrate für den Ausnahmengrenzwert (ETV) ist, der in folgender Tabelle angegeben ist und wobei die risikobasierte Beurteilung jeder einzelnen Transaktion als geringes Risiko angesehen werden kann.

ETV	Kartenbasierte Zahlungen
EUR 500	1 bps
EUR 250	6 bps
EUR 100	13 bps

One-Leg-Out-Transaktionen

One-Leg-Out-Transaktionen sind solche Transaktionen, wo sich entweder der Zahlungsdienstleister des Zahlers oder der Zahlungsdienstleister des Empfängers außerhalb der Europäischen Union befindet.

Zahlungsdienstleister im Kontext kartenbasierter Transaktionen und im Geiste der PSD2 sind regelmäßig **Acquirer** und **Issuer**.

Daher sind weder die Nationalität des Karteninhabers noch der Geschäftsort des Händlers für die Beurteilung relevant, ob eine Transaktionen infolge der Regel 'one-leg out' außerhalb des Geltungsbereiches liegt.