# Sicherheit im kartenbasierten Zahlungsverkehr

## Konvergenz von TRA/RBA und 3-D Secure 2.0 als Herausforderung und Chance für Issuerbanken

Dominik Siebert
Benedikt von Hake

Juni 2019
Blogpost

## Key Facts

- Pflichten zur starken Kundenauthentifizierung (SCA) aus der finalen RTS der PSD2 ab 14. September 2019 geltendes Recht
- „3-D Secure 2.0“ reflektiert gestiegene Sicherheitsanforderungen bei Kartenzahlungen
- RTS bereits länger im Fokus der Finanzinstitute – 3-D Secure 2.0 bisher weniger beachtet
- Adäquates Risiko-Scoring-System zentraler Bestandteil sowohl von 3-D Secure 2.0 als auch der RTS der PSD2
- Erhöhung der Risikobereitschaft der Issuer zur Maximierung der User Convenience von Kartenschemes und Wettbewerb forciert – zur Vermeidung einer Abwärtsspirale qualitatives Risiko-Scoring frühzeitig aufzubauen

## Hintergrund

Am 14. September 2019 wird die PSD2 zu geltendem nationalem Recht. Damit werden auch die Pflichten zur starken Kundenauthentifizierung nach Art. 97 wirksam, welche in den „Regulatory Technical Standards (RTS) zu starker Kundenauthentifizierung und sicherer Kommunikation im bargeldlosen Zahlungsverkehr“ spezifiziert sind.

Grundsätzlich ist dabei für vom Zahler initiierte Transaktionen eine „Starke Kundenauthentifizierung“ (SCA) mittels zweier unabhängiger Faktoren durchzuführen, sofern keine der in Abbildung 1 dargestellten Ausnahmen greift. (https://core.se/de/publikationen/blog-posts/translate-to-deutsch-final-version-of-rts-under-psd-ii-eba-urges-technological-competition).

| Ausnahme | Regelt | Beschreibung |
|---|---|---|
| Informationen zum Zahlungskonto | Artikel 10 | ▪ Kontostand<br>▪ Transaktionen der letzten 90 Tage<br>▪ Keine Offenlegung geheimer Zahlungsdaten<br>▪ Nicht beim ersten Mal<br>▪ Nicht bei SCA vor länger als 90 Tagen |
| Kontaktlose Zahlung am POS | Artikel 11 | ▪ Einzelzahlung ≤ EUR 50<br>▪ Kumulierter Betrag ≤ EUR 150 oder 5 aufeinader folgende Einzelzahlungen ohne SCA |
| Transport- und Parkgebühren | Artikel 12 | ▪ Unbediente Zahlterminals, z.B. für Maut und Parken |
| Bekannte Empfänger und wiederkehrende Zahlungen | Artikel 13 | ▪ Empfänger Whitelist<br>▪ Zahlungsserie mit gleichem Betrag an gleichen Empfänger<br>▪ Nicht bei Änderungen der Whitelist<br>▪ Nicht beim ersten Mal |
| Zahlung an sich selbst | Artikel 14 | ▪ Zahlung an sich selbst und beide Konten bei gleicher Bank |
| Kleinbetragszahlung | Artikel 15 | ▪ ≤ EUR 30<br>▪ Serie ≤ EUR 100 oder 5 aufeinander folgende Zahlungen ohne SCA |
| Transaction Risk Analysis (TRA) | Artikel 16 | ▪ Schwellenmaß ETW abhängig von Verlustrate pro Zahlungsinstrument |

Abbildung 1: Ausnahmen von der Nutzung starker Kundenauthentifizierung

Im Falle der Ausnahme nach „Transaction Risk Analysis“ (TRA) gem. Artikel 16 werden explizit einzubeziehende und in Echtzeit zu bewertende Risikofaktoren gefordert, u.a. das historische Ausgabeverhalten des Nutzers, der Aufenthaltsort vom Zahler und Zahlungsempfänger oder auch eine mögliche abnormale Nutzung eines Zugangsgerätes oder der verwendeten Software.

Die Anwendbarkeit der Ausnahme nach TRA hängt dabei vom Schwellenmaß ETV „Exemption Threshold Value“ ab. Abhängig von der Verlusrate des Zahlungssystemanbieters kann das ETV 100, 250 oder 500 Euro betragen. Erst nach Überschreiten des ETV muss starke Kundenauthentifizierung eingeschaltet werden. Dabei unterscheidet die EBA zwischen kartenbasierten Zahlungen und Überweisungen. Die genauen Zahlenwerte gibt Abbildung 2 wieder.

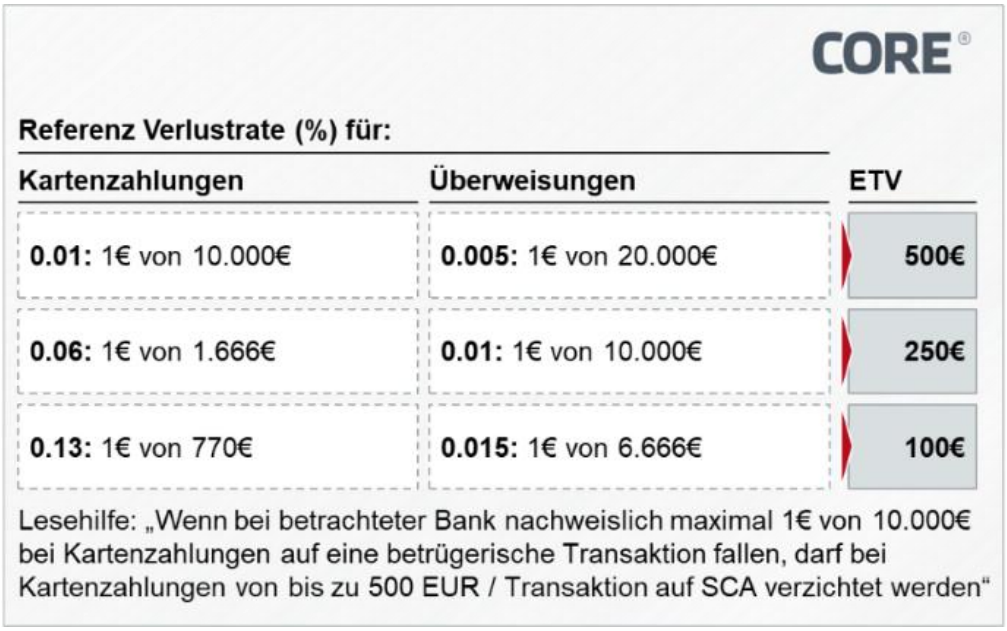


Abbildung 2: ETV in Abhängigkeit der Verlustrate und Zahlungsinstrument

Bei Kartenzahlungen im Distanzgeschäft ist die SCA durch das 3-D Secure Protokoll schon seit Jahren etabliert: Sofern ein Händler eine Transaktion über eine Kundenauthentifizierung per 3-D Secure abgesichert hat, geht das Betrugsrisiko auf die kartenausgebende Bank über. Eine über 3-D Secure abgesicherte Transaktion genügt prinzipiell den SCA-Anforderungen der RTS.

Da durch den zusätzlichen Schritt der Kundenauthentifizierung – beispielsweise ein per SMS versendetes Einmalpasswort – als zusätzlich notwendige Kundeninteraktion die Convenience des Checkout-Prozesses mindert, neigen Händler jedoch oft dazu, auf 3-D Secure Authentifizierungen zu verzichten, um Kaufabbrüche zu vermeiden und die Conversion Rate entsprechend zu erhöhen.

Diesem Umstand Rechnung tragend hat die Vereinigung der Kartenschemes EMVCo im Jahr 2015 eine neue Version des 3-D Secure Protokolls („3-D Secure 2.0“[1]) aufgelegt, welche u.a. den so genannten „Risk Based Approach“ (RBA) zulässt. Der RBA ermöglicht, dass die kartenherausgebende Bank auf Basis eines Risikoscorings auf die zusätzliche Kundeninteraktion im Authentifizierungsprozess verzichten kann. Dass Scoring fußt dabei primär auf neuen Datenelementen, welche im Zuge der 3-D Secure 2.0 Transaktionsanfrage an den Issuer, respektive dessen Service-Partner übertragen werden, bspw. Informationen zum Händler oder zum Warenkorb. Durch die somit gestiegene Convenience sollen Kaufabbrüche durch 3-D Secure vermieden werden und gleichzeitig die Händlernachfrage nach 3-D Secure steigen.

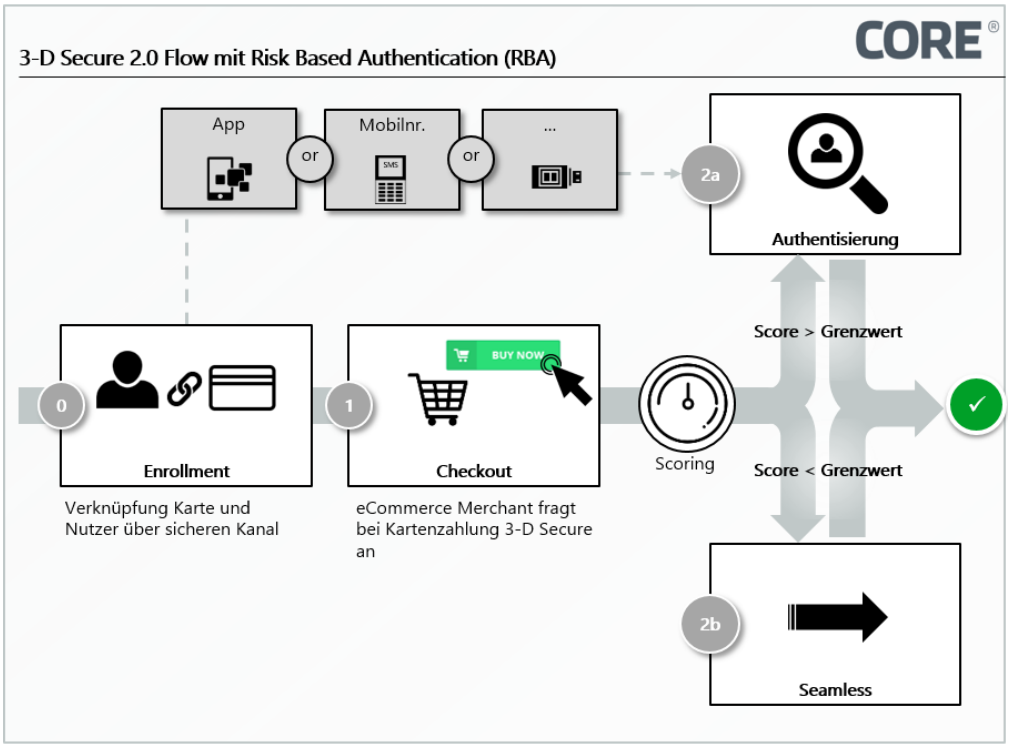


Abbildung 3: Vereinfachter User Flow nach 3-D Secure 2.0 Protokoll

Die TRA-Ausnahmeregelung der RTS und der RBA aus 3-D Secure 2.0 passen daher perfekt zusammen: Sofern die kartenherausgebende Bank ein hinreichendes Risiko-Scoring implementiert, kann sie dem Karteninhaber ein bequemes Einkaufen im E-Commerce ohne zusätzliche Schritte zur Kundenauthentifizierung ermöglichen und dabei dennoch im Einklang mit den strengen Anforderungen der SCA gem. PSD2 sein.

Mehr Sicherheit, höhere Convenience und damit potenziell mehr Transaktionen – das freut Kunden, Regulatoren, Händler, Banken und die Kartenschemes. Soweit zumindest die Theorie. Denn während die PSD2 RTS von Banken bereits antizipiert sind, ist die Aufmerksamkeit des

[1] Aktuelle Version des Protokolls ist 3-D Secure 2.2.0 (link zur Spezifikation unten), jedoch ist weiterhin der Wortlaut „3-D Secure 2.0“ geläufig

Marktes auf das Thema 3-D Secure 2.0 gering und steckt entsprechend auch dessen Adaption noch in den Anfängen.

## Implizierte Herausforderungen und resultierendes Dilemma

Zunächst ist zu berücksichtigen, dass sowohl Banken als auch Anbieter von 3-D Secure Lösungen das neue Protokoll 3-D Secure 2.0 und damit auch ein entsprechendes Risk-Scoring-System erst einmal implementieren sowie anschließend dem eigenen Risikoappetit passend parametrieren müssen, und das jeweils marktspezifisch. Bis die Convenience-Verbesserung und steigenden Abfragequoten sich in den Checkout-Prozessen der Händler bemerkbar machen, wird wohl noch einige Zeit vergehen.

Um diese Entwicklung zu beschleunigen, versuchen die Card Schemes Druck auf die Banken aufzubauen: Visa fordert die Umsetzung von RBA explizit für neu ausgegebene Karten, Mastercard indirekt über mandatorisch zu unterbietende Kaufabbruchquoten im E-Commerce, welche sich de facto nur mit Einsatz von RBA erreichen lassen.

Somit sind die Banken tendenziell angehalten, ihre Schwellwerte für den Verzicht auf die Kundenauthentifizierung eher risikofreudig zu parametrieren – nicht zuletzt, da die Convenience im E-Commerce durch die Regelungen der RTS nun wettbewerbsdifferenzierend wird: Wenn sich bspw. der Karteninhaber bei Bank A hochfrequent beim E-Commerce-Einkauf authentifizieren muss, bei Bank B aber ohne nachweislichen Sicherheitsnachteil i.d.R. auf diesen Schritt verzichtet werden kann, ist es sehr wahrscheinlich, dass der Kunde kurz- bis mittelfristig die Karte von Bank A nicht mehr einsetzen wird.

Demgegenüber bedeutet eine risikofreudige RBA-Parametrierung, dass eine Bank die Fraud-Schwellwerte gemäß RTS überschreiten könnte und damit seltener auf SCA, respektive die interaktionsbehaftete Authentifizierung bei 3-D Secure verzichten darf.

Da derzeit weder für die RTS- noch für die 3-D Secure 2.0 Umsetzungen breite Erfahrungswerte vorliegen, ist für Banken der Idealwert für den eigenen Risikoappetit schwierig zu antizipieren. Mehr noch fehlen die Datengrundlagen für entsprechende Parametrierungen, denn da die wenigsten Händler bisher das 3-D Secure 2.0 Protokoll adaptiert haben, gibt es fast keine historischen Daten für das Risikoscoring auf Basis der neuen Datenelemente – es stehen somit alle Issuer respektive 3-D Secure Service-Anbieter vor derselben Ausgangslage.

Im „Worst Case“ könnten daher Issuer, welche den Trend verpassen, durch die im Folgenden dargestellte potenzielle Entwicklung in eine Abwärtsspirale geraten:

1. Der Issuer muss RBA umsetzen und ist aufgrund von Wettbewerb und Card Scheme-Vorgaben tendenziell dazu angehalten, ihn risikoaffin zu parametrieren.
2. Der Issuer überschreitet dadurch die TRA-Schwellwerte und muss gemäß RTS restriktiver SCA zur Anwendung bringen.
3. Kundenunzufriedenheit und Kaufabrrüche steigen durch eingeschränkte Convenience.

4. Kunden nutzen stattdessen alternative Zahlmittel (ggf. auch vom Wettbewerber), wodurch die Anzahl an Transaktionen sinkt und die geringere Datenbasis durch weniger Transaktionen das Optimierungspotenzial für das Risikoscoring limitiert.
5. Mehr Fraud und/oder Kaufabbrüche führen im Resultat zu Umsatzrückgang, Reputationsverlusten und erhöhen letzlich sogar das Risiko von Sanktionen vom Regulator oder den Schemes.

## Fazit

Zunächst gilt festzuhalten, dass mit den Regelungen der PSD2 RTS bezüglich SCA der kartenbasierte Zahlungsverkehr im E-Commerce im Hinblick auf Sicherheit gestärkt wird, was im Sinne der Verbraucher und letztlich auch der kartenausgebenden Banken ist. Die in der finalen Version der RTS ergänzten SCA-Ausnahmeregelungen ermöglichen jedoch – unter der Prämisse der richtigen Implementierung seitens der Banken –, die Convenience auf einem moderaten Niveau zu halten, was ein wichtiger Faktor bei der Behauptung der Karte als Zahlungsmittel im Distanzgeschäft ist. Jedoch müssen die Issuer, wie in vielen anderen Situationen auch, eine Abwägung zwischen Sicherheit und Convenience treffen. Durch die beschriebene Gefahr einer „Abwärtsspirale“ werden die Issuer jedoch unter Druck gesetzt, was die kurzfristige Implementierung eines effizienten Risiko Scoring Tools für RBA/TRA unabdingbar macht: Die Marktentwicklung abzuwarten stellt keine Option dar und Issuer sollten entsprechend priorisieren und proaktiv agieren. Denn richtig ausgespielt kann eine überlegene Handhabung von RBA/TRA zum Wettbewerbsvorteil werden. Effektive Risiko Scoring Tools leben dabei von der konstanten Zufuhr an Daten, was abermals postuliert: Je früher der Issuer ein Risiko Scoring umsetzt, desto eher wird dieses sich qualitativ absetzen. Sich das Risiko Scoring als Service beim 3-D Secure Provider einzukaufen, kann die Herausforderung für Issuer potenziell auslagern, jedoch kann somit allenfalls das Niveau des Wettbewerbsumfelds, nicht aber eine positive Differenzierung erreicht werden. Zudem sollte idealerweise das Risiko Scoring für den RBA mit den heute im Kartengeschäft bereits fast flächendeckend und meist intern umgesetzten Risiko-Scorings für die Transaktions-Autorisierung verknüpft werden, da sich durch den erweiterten Datenumfang auch dieses weiter optimieren lässt. Je nach strategischer Stoßrichtung und in Abhängigkeit der eigenen Architektur sollten Issuer daher die interne Umsetzung des Risiko Scorings evaluieren.

Doch unabhängig davon, ob das Scoring extern gesourced oder intern umgesetzt wird: In den Anfängen der Umsetzungvon RTS und 3-D Secure 2.0 gilt es für Banken, die Umbruchphase zu nutzen und den Markt aktiv zu gestalten, bevor das Risiko Scoring vom Differenzierungspotenzial zum Hygienefaktor mutiert.

## Quellen


1. **EMV 3-D Secure**
   **Protocol and Core Functions Specification**
   https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf
2. **Apple Card Uncovered - Top 10 Q&A**
   https://medium.com/rivero-ag/top-10-questions-about-apple-card-9bf458649d03
3. **Commission Delegated Regulation (EU) 2018/389 of 27 November 2017**
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389
4. **Abbildung 1: Ausnahmen von der Nutzung starker Kundenauthentifizierung**
   CORE
5. **Abbildung 2: ETV in Abhängigkeit der Verlustrate und Zahlungsinstrument**
   CORE
6. **Abbildung 3: Vereinfachter User Flow nach 3-D Secure 2.0 Protokoll**
   CORE

**Dominik Siebert** ist Expert Director bei CORE und blickt in der Finanzindustrie auf fundierte Erfahrungen bei komplexen Transformationsvorhaben, von der strategischen Konzeptionierung bis zur Umsetzungssteuerung zurück. Bei CORE fokussiert sich Dominik auf Projekte zur Entwicklung und strategischer Positionierung digitaler Bezahllösungen.

**Mail: dominik.siebert@core.se**

**Benedikt von Hake** ist Transformation Manager bei CORE. Als studierter Volkswirt mit internationalem Abschluss sammelte er erste Berufserfahrung bei der Entwicklung einer digitalen Vertriebsplattform. Bei CORE setzt Benedikt sein Wissen ein, in der Banken- und Zahlungsindustrie bei komplexen IT-Transformationen vor allem in den Bereichen Plattform-IT und innovative Bezahlsysteme zu unterstützen.

**Mail: benedikt.hake@core.se**

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform MEA LLC
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633