CORE®

SCHWACHE KUNDEN-AUTHENTIFIZIERUNG

Warum die PSD2 SCA Anforderungen jetzt erst wirksam werden und warum dies eine Chance für Banken ist

Autoren
Benedikt von Hake
Dominik Siebert
Johannes Steinbrecher
Tim Gieske

Januar 2021
White Paper

Öffentlich

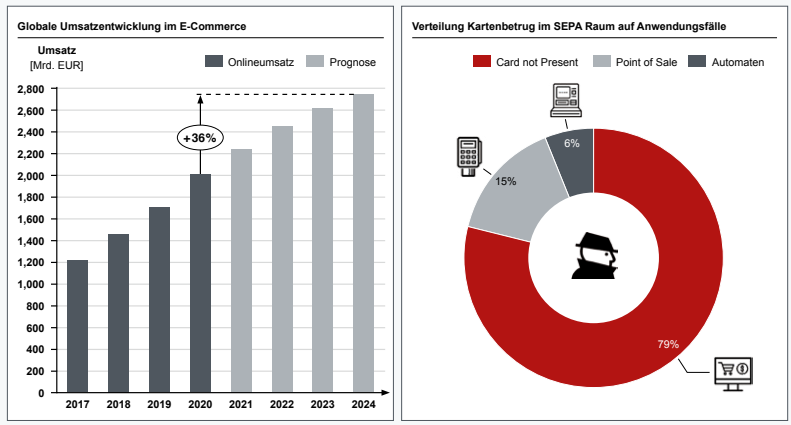
1 Einleitung

In den letzten Jahren – und abermals beschleunigt durch die Corona Krise sowie die einhergehenden Limitationen für den stationären Handel – steigt das E-Commerce Volumen weltweit stetig an. Die lokale Entkopplung des einkaufenden Endkunden vom Händler (Merchant) eröffnet dabei Möglichkeiten Convenience sowie Reichweite zu optimieren und bietet zudem Potenziale für gänzlich neue Geschäftsmodelle, wie bspw. Streaming Dienste. Gleichzeitig ist dieser Trend jedoch auch eine Gelegenheit für Betrüger, denn Kunden- sowie Zahlungsmitteldaten sind einfacher und mit größerer Skalierbarkeit zu entwenden. Sobald dies gelungen ist, steigt das Schadenspotenzial zusätzlich, da ein Betrüger binnen kürzester Zeit fast weltweit mit den gestohlenen Daten Schaden anrichten kann, wobei – im Gegensatz bspw. zum konventionellen Kreditkartenbetrug im stationären Handel – das Risiko der Strafverfolgung für den Betrüger vergleichsweise gering ist.

Wachsendes Distanzgeschäft bietet mehr Gelegenheiten und größere Skalierbarkeit des Schadens durch Betrüger

In logischer Konsequenz ist die Betrugsquote in Bezug auf Identitätsdiebstahl im E-Commerce im Vergleich etwa um Faktor 4 größer als beim stationären Handel oder am Automaten, sodass die s.g. Card-not-present-Transaktionen in Europa etwa 80% des Betrugsvolumens ausmachen[1]. Dies hat auch der Regulator erkannt und Maßnahmen ergriffen, um insbesondere die Konsumenten vor Betrug im Zahlungsverkehr allgemein, insbesondere jedoch im E-Commerce, zu schützen. In Europa ist der aktuelle und noch immer in der Umsetzung befindliche Standard die 2015 verabschiedete Zahlungsdienstrichtlinie 2 (PSD2).

Entwicklung der Onlineumsätze im E-Commerce und Verteilung Betrugsvolumen



Quelle: Statista, abgerufen am 19.12.2020 | https://www.merchantsavvy.co.uk/payment-fraud-statistics/, abgerufen am 12.01.2021

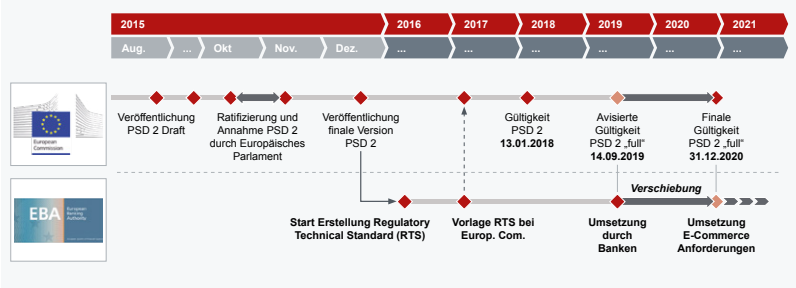
Abbildung 1: Entwicklung Onlineumsätze und Verteilung des Betrugsvolumens bei Kartenzahlungen im SEPA Raum

Am 8. Oktober 2015 ratifizierte das Europäische Parlament den Vorschlag der Europäischen Kommission zur Schaffung sichererer und innovativerer europäischer Zahlungen. Dadurch hatten die Mitgliedstaaten bis zum

[1] https://www.merchantsavvy.co.uk/payment-fraud-statistics

13. Januar 2018 Zeit, ihre nationalen Gesetze und Vorschriften der neuen Richtlinie entsprechend anzupassen und damit die seit 2007 geltende Zahlungsdiensterichtlinie 2007/64/EG (kurz PSD bzw. PSD1) abzulösen.

Zeitschiene der PSD2



Quelle: COREresearch 2021

Abbildung 2: Zeitschiene der PSD2

Die neuen Regeln zielten darauf ab, den digitalen europäischen Binnenmarkt zu stärken, die Verbraucher insbesondere im E-Commerce besser zu schützen, sowie die Entwicklung und Nutzung innovativer Online- und Mobilzahlungen zu fördern.

PSD2 umfasst weit mehr als die Schnittstellenöffnung, Anforderungen an Starke Authentifizierung haben deutlich mehr Auswirkungen im Kundenalltag

Der wohl prominenteste Bestandteil dieser in der Finanzindustrie breit diskutierten Direktive war die mandatorische Bereitstellung von externen Schnittstellen, über die Drittdienstleister kostenlos auf die Zahlungskonten der Bankkunden zugreifen können (Open Banking). Deutlich weniger prominent, aber nicht weniger bedeutend für Finanzinstitute, Zahlungsdienstleister und Handel waren die in Art. 97 der PSD2 formulierten Pflichten zur starken Kundenauthentifizierung. Diese wurden in den s.g. „Regulatory Technical Standards (RTS) zu starker Kundenauthentifizierung und sicherer Kommunikation im bargeldlosen Zahlungsverkehr" spezifiziert und sollten ursprünglich im Rahmen der PSD2 bis spätestens zum 14. September 2019 umgesetzt werden.

In den RTS werden unter anderem Vorgaben formuliert, in welchen Anwendungsfällen und Zahlungen, sowie innerhalb welcher Betragshöhen eine „starke Kundenauthentifizierung" (Strong Customer Authentication, SCA) durchzuführen ist.

Gemäß der Definition in der PSD2 ist eine „starke Kundenauthentifizierung" charakterisiert durch die Berücksichtigung von mindestens zwei Faktoren aus den unterschiedlichen Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das nur der Nutzer ist/ sein kann – bspw. biometrische Merkmale), die insofern voneinander unabhängig sind, als dass die Kompromittierung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt.

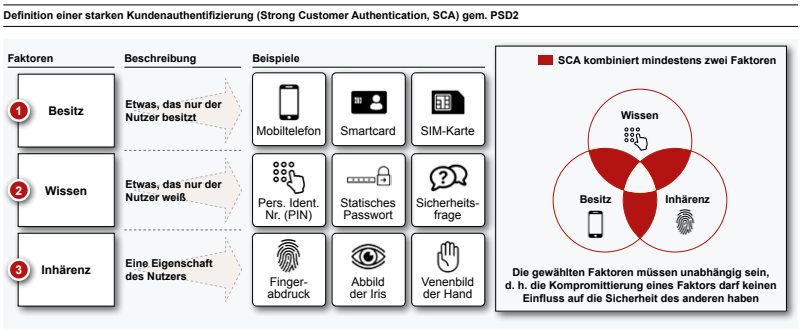


Abbildung 3: Definition starke Kundenauthentifizierung

Diese Multi-Faktor-Authentifizierung (MFA) wird schon lange angewandt: Am Point of Sale wird bspw. bei einer Kartenzahlung der Karteninhaber über den Besitz der Karte und das Wissen der PIN authentifiziert. Alternativ zur PIN kann auch eine Unterschrift erfolgen, welche rechtlich als Inhärenz-Faktor betrachtet wird.

2-Faktor Authentifizierungen in einem Zahlungsprozess stellen keine grundlegende Neuerung dar

Gleiches gilt für Überweisungen aus dem E- oder M-Banking: Das Wissen der Zugangsdaten allein (z.B. Nutzername und Passwort) wäre nur ein Faktor und reicht entsprechend nicht mehr aus. Folglich wird ein weiterer Faktor, i.d.R. ein Besitzfaktor abgefragt: Der Besitz der Bankkarte bei Chip-TAN, der Besitz einer bestimmten SIM-Karte bei SMS-TAN oder der Besitz einer an ein bestimmtes Device gebundenen Sicherheits-App (Push-TAN oder Foto-TAN).

Etwas komplizierter wird es, wenn eine Kartenzahlung im E-Commerce getätigt werden soll: Eine PIN kann hier mangels sicheren PIN-Eingabe-gerätes in den Händen der Nutzer nicht eingegeben werden und das Wissen über die Kartennummer (PAN), das Ablaufdatum und auch die Prüfziffer (CVV2/CVC2) zählen nicht als Wissens-Faktor, denn diese sind keine Information, die nur der Karteninhaber weiß – beispielsweise verfügt ein Merchant, bei dem diese Karte bereits eingesetzt wurde, über diese Informationen.

Folglich haben die Card Schemes schon vor einigen Jahren ein Verfahren entwickelt, um auch im Distanzgeschäft eine sichere Karteninhaber-authentifizierung zu ermöglichen: Das s.g. 3-D Secure Verfahren ermöglicht die 2-Faktor Authentifizierung bei Kartenzahlungen im Distanzgeschäft, indem der Karteninhaber seinen Besitz der Karte über einen separaten und zuvor aus einer sicheren Umgebung heraus registrierten Kanal nachweist. Ähnlich wie bei Online Überweisungen können hierbei ein per SMS, E-Mail oder in das Postfach des Kunden verschickte Einmalpasswort (OTP) oder eine gesicherte App zum Einsatz kommen. Dieses Verfahren ist bereits seit vielen Jahren im Einsatz, nur lag es i.d.R. in der Entscheidungshoheit von Merchants und Banken (Issuern), ob dieses Verfahren angewendet werden soll.

Die Verschärfung der SCA Anforderungen durch PSD2 führt nun – insbesondere im Distanzgeschäft – zu großen Herausforderungen für die involvierten Akteure:

- **Kunden / Karteninhaber** müssen Einschränkungen in der Convenience des Zahlungsprozesses hinnehmen und sich – je nach Umsetzung des Issuers – für weitere Authentifizierungslösungen registrieren.
- **Banken (Issuer)** müssen regulatorisch konforme Lösungen auf eigene Kosten bereitstellen und befinden sich im Dilemma zwischen Risikobereitschaft und Convenience für den Kunden.
- **Händler (Merchants)** müssen ihre Checkout-Prozesse anpassen, was nicht nur mit Aufwand und Investitionen einhergeht, sondern auch die Convenience für den Kunden durch einen weiteren Prozessschritt einschränkt und somit zu Kaufabbrüchen führen kann.

Signifikante Potenziale bleiben bisher sowohl bei Issuern als auch bei Merchants unerschlossen

Dabei hat eine Marktanalyse der Autoren mit mehr als 110 analysierten Issuern gezeigt, dass insbesondere auf der Bankenseite signifikante Potenziale unerschlossen bleiben und mitunter Implementierungsansätze im Markt ersichtlich sind, die nicht nur zu Lasten der Convenience gehen, sondern auch im Betrieb deutliche Mehrkosten bedeuten. Aus diesem Grund wurden die Marktsituation, ersichtliche Umsetzungsansätze sowie zukünftige Entwicklungspotenziale analysiert und auf dieser Basis Lösungsmuster konzipiert, welche gegeben der aktuellen Marktsituation als Best Practice formuliert werden können.

2 Ausgangslage

Um die resultierenden Herausforderungen für alle Akteure zu verstehen und eine Handlungsempfehlung für Issuer als primäre Adressaten dieses Whitepapers ableiten zu können, ist es notwendig die Entwicklungen hinsichtlich der PSD2 SCA Anforderungen und dem 3-D Secure Protokoll zu betrachten.

2.1 Der Weg bis zu 3-D Secure 2.x

Mit beginnender Ausbreitung des Internets im privaten Bereich entwickelte sich ein rasant wachsender Markt für Internetzahlungen. Bis dato reichte es für einen Merchant im Distanzgeschäft aus, die Kartendaten eines Kunden – also Name, PAN, Prüfziffer und Ablaufdatum – zu wissen, um die Karte belasten zu können. In den frühen Jahren des E-Commerce zeigte sich jedoch schnell, dass sich durch diese Loslösung der Kartendaten von der physischen Karte ein großes Betrugspotenzial ergibt: Einerseits wurde es im Distanzgeschäft bedeutend einfacher Kartendaten z.B. durch Phishing zu entwenden. Andererseits wirkte das Internet als Katalysator für den betrügerischen Einsatz einer entwendeten Karte bzw. entwendeter Kartendaten, denn ein Betrüger kann diese innerhalb kurzer Zeit und ohne räumliche Limitationen einsetzen und im Gegensatz zum POS-Geschäft besteht keine Notwendigkeit eine physische Karte zu fälschen. Zudem ist für den Betrüger das Risiko, bei einer unzulässigen Transaktion überführt zu werden, bedeutend geringer.

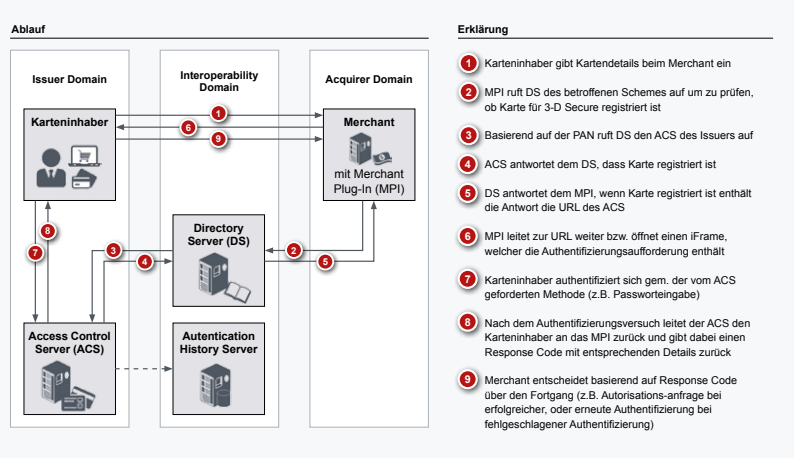
3-D Secure bietet 2-Faktor Authentifizierungen für Kartenzahlungen im Distanzgeschäft

Um diesem Sachverhalt entgegenzuwirken wurde 3-D Secure entwickelt; ein technisches Protokoll, welches die Anwendbarkeit einer 2-Faktor Authentifizierung im Distanzgeschäft ermöglicht und damit eine Erhöhung der Sicherheit intendiert. Der Name 3-D Secure spielt dabei auf die drei beteiligten Domänen Händler (Merchants) bzw. deren Acquirer, kartenausgebende Banken (Issuer) und die Netzwerkbetreiber (Card Schemes) als entsprechendes Bindeglied an.

Das Protokoll wurde im Jahr 2001 ursprünglich von Visa in Kooperation mit Arcot Systems[2] entwickelt und unter dem Namen „Verified by Visa“ vermarktet. Der Ablauf des ursprünglichen Protokolls ist in Abbildung 4 dargestellt: Nachdem der Käufer seine Kartendetails im Onlineshop des Merchants eingibt, wird eine Authentifizierungsanfrage an den s.g. Directory Server des jeweiligen Card Schemes geschickt. Dieser fungiert als eine Art globaler Router und leitet die Authentifizierungsanfrage an den s.g. Access Control Server (ACS) des Issuers weiter, welcher eine Kundenauthentifizierung anstößt. Die Authentifizierung selbst obliegt grundsätzlich dem Issuer und kann bspw. ein statisches und zuvor beim Issuer hinterlegtes Passwort, oder ein per SMS vom Issuer an den Kunden verschicktes Einmalpasswort (OTP) sein. Dabei kann der ACS, durch die in das Frontend des Merchants eingebetteten und vom Issuer erstellten s.g. CAP Screens, den Kunden durch den Authentifizierungsprozess steuern. Erst nach der erfolgreichen Authentifizierung wird die eigentliche Autorisierungsanfrage für die Zahlungsauslösung in einem zweiten Zyklus über das Card Scheme an den Issuer geschickt.

[2] 2010 durch CA Technologies aufgekauft

Ablauf einer Authentifizierung gem. ursprünglichem 3-D Secure Protokoll („3-D Secure 1.0“)



Quelle: COREresearch 2021

Abbildung 4: Ablauf 3-D Secure Transaktion gem. des ursprünglichen Protokolls („3-D Secure 1.0“)

Durch das beschriebene Vorgehen kann der missbräuchliche Einsatz abgegriffener Kartendaten im E-Commerce stark eingeschränkt werden, da ein zusätzlicher und nicht auf der Karte befindlicher Sicherheitsfaktor notwendig wird. Ein Vorteil für Merchants ist zudem, dass diese durch die erfolgreiche Authentifizierung einen Nachweis für einen autorisierten Einkauf haben und somit im Betrugsfall der Issuer haftet. Ohne den Einsatz von 3-D Secure haften i.d.R. die Merchants für missbräuchlich eingesetzte Karten, da es meist nicht möglich ist dem Kunden nachzuweisen, dass er selbst und nicht ein Dritter mit Kenntnis der Kartendaten die Transaktion initiiert hat. Das geringere Haftungsrisiko muss jedoch mit einer erhöhten Kaufabbruchquote aufgrund des zusätzlichen Interaktionsbedarfs durch den Kunden abgewogen werden.

3-D Secure Einsatz mindert das Risiko des Merchants durch Haftungsübergang auf den Issuer

Da zu Beginn der 2000er Jahre jedoch weder moderne Transport-verschlüsselung wie https/TLS, noch Alternativen in Form von performanten Fraud-Scoring Systemen im breiten Einsatz waren, und entsprechend der Kartenbetrug im Distanzgeschäft florierte, erfreute sich das 3-D Secure Protokoll einer großen Beliebtheit und wurde schnell im Markt akzeptiert. Folglich kam es auch binnen kurzer Zeit zur Adaption des Konzeptes durch andere Card Schemes.[3]

Doch schon bald zeigten sich Schwächen in der initialen Version des Protokolls wie bspw. die Zulässigkeit eines einfachen statischen Passworts, die dazu führte, dass bei der Ausspähung der Karteninformationen und dieses Passworts ein Betrüger auch bei anderen Merchants das 3-D Secure Verfahren erfolgreich durchlaufen konnte. Zudem war oft die Einbettung in die Merchantseite über Pop-Up Screens anstatt der damals wenig verbreiteten i-Frames gelöst, sodass der Kunde sein Passwort in einem Pop-Up eingeben musste, welches weder die URL des Merchants noch die seines Issuers hatte. Dies wirkte nicht nur auf den Kunden konsternierend, sondern bot auch Angriffsfläche für Man-in-the-Middle und

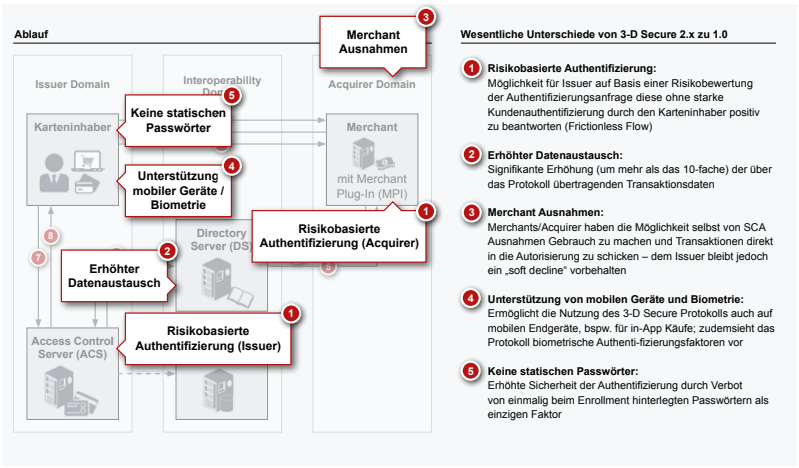
[3] Z.B. Mastercard mit „SecureCore“, JCB mit „J/Secure“ und American Express mit „SafeKey“.

Phishing Angriffe. Eine weitere Schwachstelle war, dass aufgrund einer proprietären Lösung pro Scheme der Merchant für jedes von ihm akzeptierte Card Scheme ein marginal abweichendes Verfahren implementieren musste.

Trotz dieser iterativen Weiterentwicklung des initialen Protokolls, baute sich daher zunehmend eine kritische Haltung seitens der Merchants ggü. dem 3-D Secure Verfahren auf, welche in verschiedenen Entwicklungen begründet war: Grundsätzlich führen zusätzliche Interaktionsschritte für den Kunden im Checkout-Prozess des Merchants zu höheren Kaufabbruchquoten. Solange die durch 3-D Secure vermiedenen Betrugsabschreibungen für den Merchant dies kompensieren, ist in Summe die Inanspruchnahme von 3-D Secure für den Merchant dennoch attraktiv. In der Zwischenzeit veränderte sich jedoch das Einkaufsverhalten im Internet, sodass einerseits immer mehr Onlineshops eigene und mit Passwörtern abgesicherte Kundenkonten führten, welche dann andererseits auch oft noch über einfache Fraud Systeme zusätzlich abgesichert wurden. Merchants, die ihre Kunden kennen, hatten daher immer öfter auf Anfrage einer 3-D Secure Authentifizierung verzichtet, da dies trotz der bestehenden Haftungssituation für sie attraktiver war. Hinzu kam, dass das durchschnittliche Transaktionsvolumen im E-Commerce abnahm, also immer mehr kleinvolumige Zahlungen aufkamen. Hier ist die schlanke Zahlungsabwicklung für den Merchant noch wichtiger, da die Risikoposition kleiner, die Abbruchquote durch zusätzliche Interaktionsschritte jedoch überproportional groß ist. Ferner zeichnete sich ab, dass zunehmend auch die Mobilgeräte also M-Commerce als wichtiger Verkaufskanal avancierte, worauf das damalige 3-D Secure Protokoll nicht ausgerichtet war.

3-D Secure Einsatz geht oft mit gesteigerten Kaufabbruchquoten einher

Wesentliche Unterschiede zwischen 3-D Secure Protokoll 1.0 und 2.x



Quelle: COREresearch 2021

Abbildung 5: Wesentliche Neuerungen beim 3-D Secure 2.x Protokoll

Folgerichtig wurde seitens der Card Schemes also die Notwendigkeit einer grundsätzlichen Überarbeitung des Protokolls erkannt, sodass Mastercard und Visa bereits im November 2014 (also noch vor der Veröffentlichung der PSD2) die gemeinsame Überarbeitung in eine Version „3-D Secure 2.0“

initiierten. Da schnell erkannt wurde, dass im Sinne der Händlerfreundlichkeit durch Standardisierung eine möglichst Scheme-übergreifende Lösung geschaffen werden sollte, wurde bereits im Januar 2015 die Entwicklungsverantwortung für 3-D Secure 2.x[4] an eine internationale Dachorganisation der Card Schemes delegiert: Der EMVCo, gegründet 1999 von Europay[5], Mastercard und Visa gehören heute zusätzlich American Express, UnionPay, Discover und JCB an und hatte bis dahin bspw. schon die internationalen Standards für chip-basierte Kartenzahlungen entwickelt.

Wesentlichen Änderungen zur Version 1.0 sollten sein:

Anpassungen in der neuen Protokollversion 3-D Secure 2.x adressiert bekannte Schwächen

- Besserer Betrugsschutz, (z.B. durch Vermeidung statischer Passwörter als alleinigen Authentifizierungsfaktor)
- Unterstützung mobiler Geräte
- Mehr Datenbereitstellung zur Authentifizierungsentscheidung durch den Issuer
- Mehr Kundenkomfort und weniger Kaufabbrüche durch risikobasierte Entscheidung (Risk Based Authentication – RBA) möglich
- Möglichkeit einer passiven Authentifizierung – dem so genannten „Frictionless Flow“ – bei dem keine Interaktion mit dem Kunden erforderlich ist
- Höhere Flexibilität für den Merchant hinsichtlich der Authentifizierungsanfragen und damit verbundener Haftung im Betrugsfall (siehe Abbildung 6)
- Grundsätzliche Möglichkeit zur Entkoppelung oder Delegation der starken Kundenauthentifizierung

Händleroptionen für Authentifizierungsanfragen gem. 3-D Secure 2.x Protokoll

<table>
<tr><th colspan="2">Händler Optionen</th><th>Issuer Optionen</th><th>Haftung</th></tr>
<tr><td rowspan="4">Verschickt eine 3DS2 Authentifizierungsanfrage und …</td><td>… fragt keine Acquirer Ausnahme an</td><td>Fordert SCA</td><td rowspan="2">Issuer</td></tr>
<tr><td rowspan="3">… fragt eine Acquirer Ausnahme an</td><td>Fordert keine SCA</td></tr>
<tr><td>Fordert SCA (issuer step-up)</td><td rowspan="2">Acquirer/Händler</td></tr>
<tr><td>… sendet aber nur Daten an Issuer, um Annahmequote der Autorisierung zu erhöhen; es kommt nicht zur Authentifizierung einer Transaktion (data only)</td><td>Fordert keine SCA</td></tr>
<tr><td colspan="2" rowspan="2">Verschickt keine 3DS2 Authentifizierungsanfrage</td><td>Fordert keine SCA</td></tr>
<tr><td>Antwortet mit einem Soft Decline, woraufhin die Transaktion nocheinmal mit einer 3-D Secure 2.x Authentifizierungsanfrage gesendet werden kann</td><td>Es kommt keine Transaktion zustande</td></tr>
</table>

Quelle: COREresearch 2021

Abbildung 6: 3-D Secure 2.x Protokoll gibt Merchants mehr Flexibilität für Authentifizierungsanfragen

Zusammenfassend war 3-D Secure ein wesentlicher Schritt für die Sicherheit kartenbasierter Zahlungen im E-Commerce und die Adjustierung des initialen Protokolls auf die weiterentwickelten Anforderungen im E- und M-Commerce von Kunden, Merchants und Issuern war mit 3-D Secure 2.x bereits ohne regulatorischen Eingriff initiiert.

[4] Mit 3-D Secure 2.x sind alle Iterationen des 3-D Secure Protokolls aufbauend auf der Version 2.0 gemeint

[5] 2002 mit Mastercard fusioniert

2.2 Verschärfung der Anforderungen durch PSD2 RTS

PSD2 RTS bringt deutliche Verschärfung der regulatorischen Anforderungen zur starken Kundenauthentifizierung

Gemäß der 2017 verabschiedeten PSD2 RTS ist grundsätzlich für vom Zahler initiierte Transaktionen eine SCA durchzuführen, sofern keine der in Abbildung 7 dargestellten Ausnahmen greift. Für Zahlungen im E-Commerce bedeutet dies also, dass alle Zahlungen über EUR 30, spätestens aber nach kumuliert EUR 100, oder bei der fünften Zahlung eine SCA (bei Kartenzahlungen also 3-D Secure) durchgeführt werden muss.

Ausnahmen von der Anforderungen zur starken Kundenauthentifizierung gem. PSD2 RTS

Ausnahme gem. RTS	Beschreibung
Kontaktlose Zahlung am POS [Art. 11]	▪ Einzelzahlung ≤ EUR 50 ▪ Kumulierter Betrag ≤ EUR 150 oder 5 aufeinander folgende Einzelzahlungen ohne SCA
Transport- und Parkgebühren [Art. 12]	▪ Unbeaufsichtige Zahlterminals, z.B. für Maut und Parken
Bekannte Empfänger und wiederkehrende Zahlungen [Art. 13]	▪ Empfänger Whitelist ▪ Nicht beim 1. Mal und bei Änderungen der Whitelist ▪ Zahlungsserie mit konst. Betrag an gleichen Empfänger
Zahlung an sich selbst [Art. 14]	▪ Zahlung an sich selbst und beide Konten bei gleicher Bank
Kleinbetragszahlung [Art. 15]	▪ ≤ EUR 30 ▪ Serie ≤ EUR 100 oder 5 aufeinander folgende Zahlungen ohne SCA
Transaction Risk Analysis (TRA) [Art. 16]	▪ Schwellenmaß ETV[1] abhängig von Referenz Verlustrate pro Zahlungsinstrument

Referenz Verlustrate (%) für:

Kartenzahlungen	Überweisungen	ETV[1]
0.01: 1€ von 10.000€	**0.005:** 1€ von 20.000€	**500€**
0.06: 1€ von 1.666€	**0.01:** 1€ von 10.000€	**250€**
0.13: 1€ von 770€	**0.015:** 1€ von 6.666€	**100€**

Lebenshilfe:
„Wenn bei betrachteter Bank nachweislich maximal 1€ von 10.000€ bei Kartenzahlungen auf eine betrügerische Transaktion fallen, darf bei Kartenzahlungen von bis zu 500 EUR / Transaktion auf SCA verzichtet werden"

1: Exemption Threshold Value

Quelle: Finale Version der PSD2 RTS (EBA 2017)

Abbildung 7: Ausnahmen zur starken Kundenauthentifizierung gem. PSD2 RTS

PSD2 RTS räumt Möglichkeiten für Ausnahmen ein, wobei die Umsetzung eines Risiko-Scorings eine wesentliche Basis darstellt

Ausgenommen hiervon sind Transaktionen welche die s.g. Transaction Risk Analysis (TRA) gem. Artikel 16 der RTS nutzen. Dabei können Issuer oder Merchants/Acquirer risikobasiert entscheiden, keine SCA durchzuführen, wofür jedoch ein Scoring System mit explizit einzubeziehenden und in Echtzeit zu bewertenden Risikofaktoren gefordert wird. Dabei sollen u.a. das historische Ausgabeverhalten des Nutzers, der Aufenthaltsort von Zahler und Zahlungsempfänger oder auch eine mögliche abnormale Nutzung eines Zugangsgerätes oder der verwendeten Software analysiert werden.

Zudem hängt die Anwendbarkeit der Ausnahme nach TRA dabei vom Schwellenmaß Exemption Threshold Value (ETV) ab: Abhängig einer zu ermittelnden und regelmäßig an die nationale Aufsicht[6] zu berichtenden Referenz Verlustrate des Zahlungssystemanbieters, kann der ETV EUR 100, EUR 250 oder EUR 500 betragen. Das heißt bis zu diesen Grenzen kann von der TRA Ausnahme Gebrauch gemacht werden, darüber hinaus muss immer eine starke Kundenauthentifizierung durchgeführt werden (siehe Abbildung 7).

Im Falle von Kartentransaktionen im E-Commerce ist die TRA Ausnahme der Risk Based Authentication (RBA) gem. 3-D Secure 2.x Protokoll gleichzusetzen, d.h. Merchant/Acquirer bzw. Issuer können anhand der zur Verfügung stehenden Daten risikobasiert entscheiden, ob eine SCA notwendig ist oder nicht. Sofern der Merchant auf die SCA verzichtet, würde

[6] In Deutschland die Bafin

er im Betrugsfall haften. Ferner kann der Issuer eine „non 3-D Secure“ Anfrage auch mit einem Soft-Decline ablehnen, d.h. er teilt dem Merchant mit, dass er 3-D Secure fordert. Ob er bei einer als 3-D Secure angefragten Transaktion auch tatsächlich eine SCA vom Kunden verlangt, kann bis zum jeweils geltenden ETV vom Issuer entschieden werden, wobei ein Verzicht der SCA immer die Haftungsübernahme im Betrugsfall bedeutet (vgl. Abbildung 6).

2.3 Card Schemes incentivieren diametral

Bis zum Inkrafttreten der PSD2 war die gelebte Praxis, dass der Merchant selbst entscheiden konnte, ob er die Transaktion mit oder ohne 3-D Secure anfragt. So konnten die Merchants, durch Abwägung von Risiko und Convenience je Transaktion, selbst die für ihr Geschäftsmodell zielführende Entscheidung treffen. Im Tagesgeschäft war dabei zu beobachten, dass zu Gunsten einer gesteigerten Convenience und geringeren Kaufabbrüchen nur bei hohen Transaktionsbeträgen und/oder wenn der Merchant den Kunden nicht kennt (z.B. Gastzugänge) 3-D Secure zur Anwendung kam. In diesem Sinne stellen die in den PSD2 RTS formulierten Anforderungen eine deutliche Verschärfung der SCA Pflichten für Merchants und Issuer dar. Dabei haben die Card Schemes, welche das 3-D Secure Verfahren im Rahmen der regulatorischen Vorgaben spezifizieren, selbst ein Interesse daran, eine wohlbalancierte Lösung für Karteninhaber, Merchants und Issuern zu finden – denn die Card Schemes verdienen ihr Geld primär in Abhängigkeit der über sie abgewickelten Transaktionen, sodass nachteilhafte Entwicklungen für eine der genannten Parteien sich auch nachteilhaft auf die Erträge der Card Schemes auswirken würde. So kam es auch, dass die Card Schemes die Merchants bis zum Inkrafttreten der PSD2 incentivierte, Transaktionen mit 3-D Secure anzufragen, indem neben dem Risikoübergangs auf den Issuer auch niedrigere Scheme Fees und teilweise eine niedrigere Interchange fällig wurden. Aufgrund der gem. PSD2 RTS klar definierten Anforderungen zur Anwendung der SCA und entsprechender Haftungen haben sich die Möglichkeiten zur Incentivierung der Card Schemes jedoch gewandelt. Die Card Schemes haben zwar weiterhin ein Interesse daran, möglichst wenig Kaufabbrüche bei einem möglichst hohem Sicherheitsniveau zu generieren, müssen die Incentivierung jedoch auf den durch die Regulatorik offen gelassenen Entscheidungsraum für Issuer und Merchants fokussieren.

Diametral zur PSD2 RTS incentivieren die Card Schemes eine risikoaffine Positionierung von Merchants und Issuern

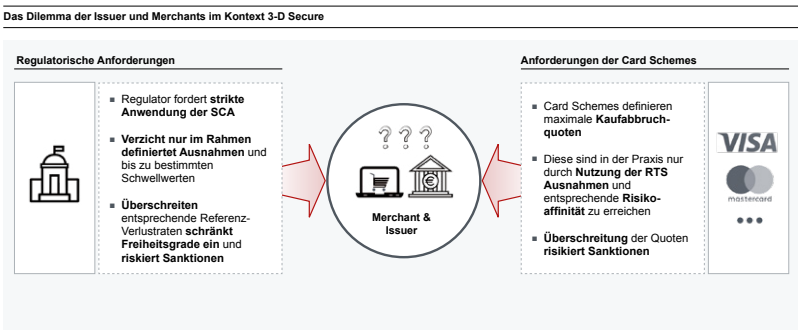


Abbildung 8: Merchants und Issuer im Spannungsfeld zwischen Regulator und Card Schemes

Daher haben die Card Schemes über die Zeit ansteigende Schwellwerte für maximal zulässige Kaufabbrüche definiert, welche Merchants und Issuer erreichen müssen, da andernfalls entsprechende Strafzahlungen appliziert werden können. Damit werden also Merchants und Issuer indirekt genötigt, die gem. RTS zulässigen Ausnahmen möglichst weit zu nutzen, wobei die Nutzung des RBA einen großen Hebel darstellt. Es wird daher ein Druck auf Merchants und Issuer ausgeübt, entsprechende Risiko-Scoring Systeme zu implementieren und diese wiederum entsprechend risikoaffin zu parametrieren, sodass die von den Card Schemes vorgeschriebenen Schwellwerte erreicht und damit Strafzahlungen vermieden werden können. Diese Incentivierung verhält sich jedoch diametral zu den TRA Schwellwerten der RTS, welche basierend auf den tatsächlich angefallenen Betrugsraten die Anwendbarkeit der Ausnahme limitieren und ihrerseits Sanktionen bei Nichteinhaltung antizipieren, entsprechend eine risikoaverse Parametrierung nahelegen.

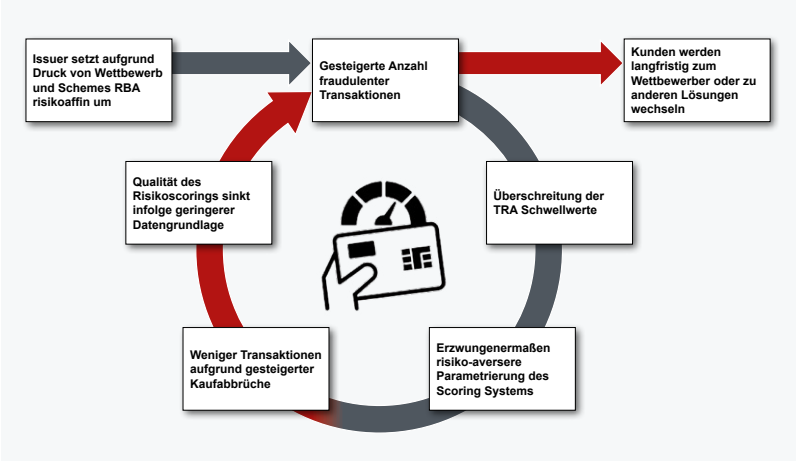
Da derzeit weder für die RTS, noch für die 3-D Secure 2.0 Umsetzungen breite Erfahrungswerte vorliegen, ist für Merchants und Issuer der Idealwert für den eigenen Risikoappetit schwierig zu antizipieren. Mehr noch fehlen die Datengrundlagen für entsprechende Parametrierungen der Risikosysteme, da bisher nur wenige Merchants das 3-D Secure 2.x Protokoll adaptiert haben bzw. auch falls das neue Protokoll umgesetzt ist, alle Daten vorliegen und übertragen werden.

Bei zu später oder unzureichender Umsetzung des Risiko-Scorings droht Abwärtsspirale

Im „Worst Case“ könnten daher Merchants und Issuer, welche das beschriebene Dilemma nicht hinreichend adressieren, durch die im Folgenden dargestellte Entwicklung in eine Abwärtsspirale geraten:

1. Merchants/Issuer muss RBA umsetzen und ist aufgrund von Wettbewerb und Card Scheme-Vorgaben tendenziell dazu angehalten, ihn risikoaffin zu parametrieren.
2. Merchants/Issuer überschreitet dadurch die TRA-Schwellwerte und muss gemäß RTS restriktiver SCA zur Anwendung bringen.
3. Kundenunzufriedenheit und Kaufabbrüche steigen durch eingeschränkte Convenience.
4. Kunden wechseln in Folge der schlechteren Convenience zum Wettbewerber.
5. Anzahl an Transaktionen sinkt und die geringere Datenbasis durch weniger Transaktionen limitiert Optimierungspotenzial für das Risiko-Scoring.

Abwärtspirale bei unzureichendem oder zu spätem Aufsetzen des Risikoscorings für RBA



Quelle: COREresearch 2021

Abbildung 9: Bei unzureichender oder zu später Umsetzung des RBA Risiko-Scorings droht Abwärtsspirale

2.4 Reaktionen des Marktes

Neben dem im Kapitel 2.3 beschriebenen Dilemma werden die verschärften SCA Pflichten oft als grundsätzlich finanzielle Bürde für Banken und Merchants verstanden, da diese neben den ohnehin schon vorhandenen Investitionen für die Implementierung der neuen Regeln auch eine deutliche Vergrößerung der Kaufabbrüche befürchten. Folglich kam es nach der ersten Veröffentlichung des RTS Drafts zu einer Vielzahl von Marktreaktionen durch Händler- und Bankenverbände, welche an diversen Stellen Lockerungen forderten. So sind bspw. die Betragsgrenzen für die SCA Pflicht in den Iterationen bis zur finalen RTS mehrfach angepasst worden und tatsächlich kam die TRA als Ausnahme mit dem größten Gestaltungspotenzial für Merchants und Issuer erst in der letzten Version der RTS hinzu. Obwohl die European Banking Authority (EBA) einige Reaktionen des Marktes in der finalen Version der RTS reflektierte, blieben die Stimmen zur RTS weiterhin kritisch. Eines der Hauptargumente der Kritiker ist, dass es eigentlich kein reales Problem im Markt gibt, welches die Umsetzung der RTS lösen würde: Der Schutz des Endkunden ist schwierig als Argument anzuführen, da schon vorher die Haftung gem. Scheme Regeln in fast allen Fällen entweder beim Merchant oder beim Issuer lag. Dass ein Kunde also die Kosten eines Betrugs selbst tragen muss, war auch vor der PSD2 i.d.R. nur dann der Fall, wenn dem Kunden entweder eine grobe Fahrlässigkeit nachgewiesen oder aber vertraglich explizit eine alternative Haftungsaufteilung zwischen Kunde und Issuer vereinbart wurde. Weiterhin war das 3-D Secure Protokoll mit der Version 2.x ohnehin schon ohne den regulatorischen Impuls in Überarbeitung und dass der E-Commerce Markt auch vor Lancierung der PSD2 ein starkes Wachstum zeigte, kann als Beleg für eine funktionierende Selbstregulierung des Marktes verstanden werden.

Insbesondere auf der Merchant Seite formiert sich Widerstand gegen die verschärften Anforderungen

Ein weiterer Kritikpunkt ist, dass aufgrund der öffentlich zugänglichen Regelungen der RTS Betrüger diese antizipieren können und bspw. nur betrügerische Transaktionen unter EUR 30 initiieren, da so die Wahrscheinlichkeit entsprechend groß ist, dass Merchant und Issuer diese als

Low Value Transaction ohne weitere Prüfung autorisieren. Der Gedanke einer höheren Sicherheit durch standardisierte Regeln wird damit umgekehrt in eine größere Angriffsfläche für Betrüger.

Folglich wundert es nicht, dass auch noch nach der finalen Verabschiedung der RTS besonders auf Seiten des Handels entsprechender Widerstand aufgebaut wurde: Eine Studie des Zahlungsdienstleisters Stripe konstatierte beispielsweise, dass allein im ersten Jahr der Umsetzung ein Verlust i.H.v. 57 Mrd. EUR im PSD2 Wirkungsraum durch Kaufabbrüche zu erwarten sei[7]. Ferner wurde vermehrt moniert, dass einige Aspekte der RTS – wie beispielsweise die Anwendbarkeit von Biometrie im Distanzgeschäft – nicht hinreichend präzise definiert seien.

Am 21. Juni 2019 – also nicht einmal 3 Monate vor Inkrafttreten der RTS – veröffentlichte daher die EBA ein weiteres und nach eigener Aussage abschließendes Positionspapier, wo auf die Unklarheiten eingegangen wurde und zudem ein Übergangszeitraum von bis zu 18 Monaten im Ermessen der nationalen Regulatoren zugestanden wurde.
Als Reaktion darauf richtete am 2. August 2019 ein Konsortium aus European Payment Institutions Federation (EPIF), Visa, Mastercard und diversen Handelsverbänden einen öffentlichen Brandbrief an die EBA und die EU-Kommission. Darin kritisierten die Unterzeichner die Auslegepräzisierungen zur RTS und forderten eine einheitliche Verschiebung der RTS Anforderungen, da weite Teile des Marktes sowohl auf der Issuing- als auch auf der Merchant-Seite noch nicht vollumfänglich auf die am 14. September 2019 umzusetzenden Anforderungen vorbereitet seien.

2.5 Aktueller Umsetzungsstand

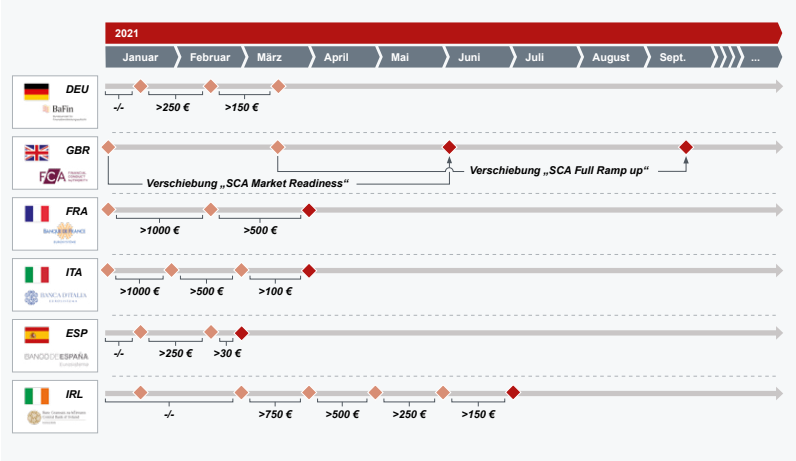
EBA lässt Verschiebung der SCA Anforderungen auf Ende 2020 zu

Die Pflicht zur Starken Kundenauthentifizierung besteht grundsätzlich seit dem 14. September 2019. Auf Basis eines Positionspapiers der Europäischen Bankenaufsichtsbehörde (European Banking Authority – EBA) vom 16. Oktober 2019 wurde den nationalen Aufsichtsbehörden allerdings ein nochmaliger Aufschub der Verpflichtung bis zum 31.12.2020 empfohlen. Resultat waren allerdings wiederum große Unterschiede zwischen den einzelnen Mitgliedsstaaten. So folgte Schweden der Empfehlung der EBA zum Beispiel nicht und verlangt die starke Kundenauthentifizierung seit dem 14. September 2019, die Deutsche BaFin kündigte an Kartenzahlungen im Internet bis zum 31. Dezember 2020 auch ohne eine erforderliche starke Kundenauthentifizierung nicht zu beanstanden, UK nahm sich auf Basis des nahenden Brexits komplett aus der Regulierung und Länder wie Frankreich formulierten Ausnahmen für unterschiedliche Branchen gemäß der Merchant Category Codes (MCC) und Beträge die bis zum 31. Dezember 2020 gelten sollten. Aber selbst nach Ablauf der neu eingeräumten Frist gibt es lokale Unterschiede und Ramp-up Perioden, weshalb viele Endkunden die neuen Anforderungen noch gar nicht aktiv zu spüren bekommen haben. So greift die Pflicht zur starken Kundenauthentifizierung in Deutschland erst seit dem 15. Januar 2021 und auch dann nur für Transaktionen über EUR 250. In einem Stufenmodell wird der Freibetrag dann zu Mitte Februar auf EUR 150 reduziert und erst ab 15. März 2021 gilt die Verpflichtung zur Starken Kundenauthentifizierung für sämtliche Transaktionen. In anderen Ländern gibt es ähnliche Regelungen. Weitere Fristen aufgrund der vom Handel proklamierten speziellen Situation der Corona-Pandemie scheinen darüber hinaus nicht ausgeschlossen.

Einführung der SCA Pflichten im Laufe des Jahres 2021 innerhalb Europas inkonsistent

[7] https://stripe.com/reports/451-research-sca, abgerufen am 29.12.2020

Stufenweise Einführung der SCA Anforderungen für Zahlungen im E-Commerce



Quelle: payment-universe.com

Abbildung 10: Stufenweise Einführung der SCA Anforderungen für Zahlungen im E-Commerce divergiert in Europa

2.6 Zwischenfazit

Der durch die unterschiedliche Handhabung der Umsetzung in den EU Mitgliedsstaaten entstandene Flickenteppich erschwert es insbesondere international agierenden Merchants und Zahlungsdienstleistern in allen lokalen Instanzen gesetzeskonform zu agieren und gleichzeitig möglichst niedrige Abbruchraten bei der Zahlungsabwicklung zu erreichen.

Dies gilt insbesondere für die Abwicklung komplexerer Zahlungsvorgänge wie der Realisierung von z.B. in der Reiseindustrie üblichen An- und Restzahlungen mit großem zeitlichem Abstand, die bei stringenter Auslegung der Regulierung teils eine mehrfache starke Kundenauthentifizierung benötigen würden. Ein weiteres Beispiel sind gemischte Warenkörbe bei Marktplatzmodellen, die Produkte und Dienstleistungen von verschiedenen Anbietern kombinieren, somit final unterschiedliche Zahlungsempfänger bedienen und theoretisch auch hier für jeden Begünstigten einzeln mit 3-D Secure authentifizieren müssten. Je nach lokaler Regulierung müssten sogar für einzelne Länder oder Branchen individuelle SCA Pflichten umgesetzt werden. In der Folge ergeben sich auch individuelle Umsetzungen bei Zahlungsdienstleistern und Banken, die auf Grund von divergierenden Interpretationen von Ausnahmen einerseits zu Unsicherheit für Merchants und Banken führen und andererseits hohe Abbruchraten bei Kartenzahlungen im Internet verursachen und somit das eigentliche Ziel der Regulierung, die einheitliche und konsequent sichere Abwicklungen von Zahlungen innerhalb der Europäischen Union verfehlen. Im schlechtesten Falle zeichnet sich gar ein Wettbewerb ab, inwiefern durch die kreative Anwendung von Ausnahmen und Anwendungsfällen, die nicht von der Pflicht zur Starken Kundenauthentifizierung betroffen sind (wie MOTO[8]-Transaktionen, merchant-initiierte Zahlungen oder anonyme

[8] Mail Order / Telephone Order, also Kartenzahlungen, bei denen die Kartendetails postalisch, per E-Mail oder telenfonisch vom Karteninhaber an den Merchant übergeben werden

Prepaidkarten) die Regulierung im Sinne der Customer-Experience umgangen werden kann. Weiter könnte perspektivisch auch die Entkoppelung oder Delegation der Starken Kundenauthentifizierung fernab des klassischen 3D-Secure Verfahrens eine Rolle spielen, wobei auch hier der Rechtsraum noch nicht vollständig abgesteckt ist und sich die Marktteilnehmer zudem erst auf gemeinsame Standards einigen müssten.

Trotz dieser für viele der involvierten Parteien nicht zufriedenstellenden Situation zeichnet sich bisher nicht ab, dass die verabschiedete PSD2 RTS in naher Zukunft in ihren Grundsätzen geändert würde, folglich obliegt es den Marktteilnehmern, sich bestmöglich auf die neue Situation anzupassen. Dabei gehen mit der Herausforderung einer optimalen Umsetzung gleichzeitig auch Chancen für eine positive Differenzierung im Wettbewerb einher, wobei insbesondere Banken als Hauptadressaten dieses Whitepapers eine Evaluierung der eigenen Ausgangslage und strategischen Potenziale nahegelegt wird.

Durchsetzung der Regulierung scheint besiegelt und Akteure sollten sich bestmöglich auf die neuen Umstän

3 Status Quo und Herausforderung für Banken

Auch wenn sich bisher der im Markt beobachtbare Widerstand und einhergehend auch die Verschiebungen der Umsetzungsfristen primär auf die Merchant-Seite fokussiert haben, bedeutet dies nicht, dass der Umsetzungsstand und die Situation für Issuer weniger kritisch sind. Vielmehr begründet die oft schlechte Umsetzung auf der Issuer Seite auch den Widerstand der Merchants, da inkonveniente Authentifizierungsverfahren, fehlende Single-Device Fähigkeit und teils auch vom Karteninhaber erhobene Gebühren Kaufabbrüche verstärken.

Umsetzung von 3-D Secure auf der Issuer Seite oft historisch gewachsen – Modernisierung mit Herausforderungen verbunden

Dabei sind die Issuer mit unterschiedlichen Herausforderungen konfrontiert: Die meisten Issuer haben historisch gewachsen eine 3-D Secure Lösung auf Basis eines SMS-OTP umgesetzt, da in den Anfängen des 3-D Secure Smartphones und damit Apps noch nicht im Markt etabliert waren und Authentifizierungslösungen mit zusätzlichem Hardware Device jedoch meist teuer und für den Karteninhaber unpraktikabel sind, da dieser ein weiteres Gerät mit sich führen muss. Gemäß PSD2 RTS und auch 3-D Secure 2.x Protokoll reicht ein SMS OTP allein jedoch nicht mehr aus, sondern muss durch einen statischen Sicherheitsfaktor (z.B. Passwort oder Sicherheitsfrage) ergänzt werden. Oftmals ist zudem das SMS OTP Verfahren nicht hausintern umgesetzt, sondern als Service von einem externe ACS Anbieter bezogen, welcher oft auch die dafür notwendige Mobilfunknummern verwaltet. Von dieser Lösung auf eine andere umzuschwenken gestaltet sich oft schwierig, da die über die Zeit gesammelten Mobilfunknummern und ggf. Passwörter meist nicht einfach migriert werden können und entsprechend vom Karteninhaber neu initialisiert werden müssten.

Im Zuge einer immer stärkeren Relevanz mobiler Anwendungen und unter der Annahme, dass der überwiegende Anteil der Kunden heute ein Smartphone hat, wäre ein App-basierte Lösung die naheliegende Alternative. Dabei ist jedoch zu bemerken, dass Stand heute nicht alle Banken eine hinreichend starke Mobile Banking Durchdringung haben, sodass davon ausgegangen werden kann, dass jeder Kunde auch über die App der Bank, in der diese Funktion integrierbar wäre, verfügt. Hinzu kommt, dass eine App kryptografisch an das jeweilige Device gebunden werden muss, um einen eindeutigen Besitz nachzuweisen, um somit als Sicherheitsfaktor nutzbar zu sein. Da die hierfür notwendige technische Expertise bei Banken oft nicht im eigenen Haus verfügbar ist, wird auch hier häufig auf extern eingekaufte Lösungen zurückgegriffen, wobei diese oft vom ACS Betreiber als eigenständige App oder SDK gesourced werden und damit nicht flexibel in die eigene Architektur integrierbar sind.

Sofern alle Kunden erreicht werden sollen, muss eine Lösung mit verschiedenen Authentifizierungsoptionen, z.B. App und SMS OTP offeriert werden. Da dieses Lösungsmuster meist jedoch nicht im Green Field Ansatz konzeptioniert, sondern historisch ausgebaut wurde, ist häufig zu beobachten, dass sich dabei kein synergetisches Architekturbild ergibt und somit zwei de Facto separate Systeme betrieben werden müssen. Das so limitierte Konvergenzpotenzial drückt sich mittelfristig nicht nur in höheren Betriebs- und Wartungskosten, sondern meist auch durch Kompromisse hinsichtlich der Nutzerfreundlichkeit aus.

Die Komplexität dieser Ausgangslage lässt den Schluss zu, dass viele Banken zwar die regulatorischen Vorgaben umgesetzt haben, die Um-

setzung selbst jedoch oft unwirtschaftlich, mit dem Aufbau von Legacy verbunden und aus Kundenperspektive ungenügend ist.

Um diese Hypothese zu untermauern haben die Autoren eine Analyse von über 100 Banken aus dem DACH Raum durchgeführt und das Angebot rund um das 3-D Secure Verfahren ausgewertet. Dabei wurden unter anderem folgende Fragestellungen untersucht:

- Welche Verfahren werden angeboten?
- Werden mehrere Verfahren parallel angeboten?
- Sind – falls vorhanden – die App Verfahren in die Banking App des Finanzinstituts integriert?
- Ist – falls vorhanden – das SMS OTP Verfahren PSD2-konform (also kombiniert mit einem zweiten statischen Faktor)?
- Ist – falls vorhanden – das SMS OTP Verfahren kostenpflichtig?

Mit 62 Finanzinstituten sind circa die Hälfte der untersuchten Institute aus Deutschland, die restlichen Institute teilen sich auf die Schweiz und Österreich, sowie einige globale Akteure auf[9].

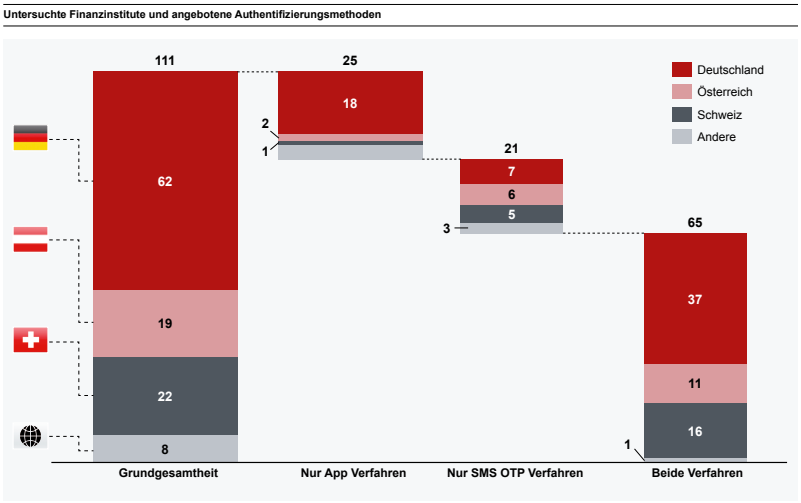


Abbildung 11: Auswertung zu Verfahren starker Kundenauthentifizierungen

Aus den Untersuchungsergebnissen lassen sich folgende 9 Kernaussagen ableiten:

1. **Alle 111 Finanzinstitute bieten ein Verfahren zur starken Kundenauthentifizierung von E-Commerce Transaktionen an:** 100% der untersuchten Finanzinstitute bieten mindestens entweder ein App oder ein SMS OTP Verfahren zur starken Kundenauthentifizierung per 3-D Secure Protokoll an.
2. **App und SMS OTP Verfahren sind die gängigsten angebotenen Verfahren zur Zwei-Faktor-Authentifizierung:** 81% der untersuchten Finanzinstitute haben ein App Verfahren, 77% ein SMS OTP Verfahren zur Authentifizierung angeboten.

Marktanalyse attestiert, dass Issuer im Regelfall nicht optimal auf die neuen Anforderungen vorbereitet sind

[9] Die PSD2 Anforderungen beziehen sich nur auf EU Mitgliedstaaten

3. **Die meisten Finanzinstitute haben ihr SMS OTP Verfahren bereits PSD2-konform (inkl. statischem Passwort oder Sicherheitsfrage als zweitem Faktor) umgesetzt:** 79% der untersuchten Finanzinstitute, welche ein SMS OTP Verfahren anbieten, haben dies zum Untersuchungszeitpunkt[10] mit einem zweiten Faktor versehen
4. **Noch immer bietet jedoch eine Minderheit der untersuchten Finanzinstitute kein PSD2-konformes Authentifizierungsverfahren an:** 5% der untersuchten Finanzinstitute bieten zum Untersuchungszeitpunkt[11] kein PSD2-konformes Authentifizierungsverfahren an, sondern lediglich ein SMS OTP Verfahren ohne zweiten Faktor (statisches Passwort oder Sicherheitsfrage).
5. **Finanzinstitute, welche ein App Verfahren anbieten, haben dies in der Regel nicht in die Banking App integriert:** 83% der untersuchten Finanzinstitute, welche ein App Verfahren anbieten, bieten dies als extra App an – lediglich 18% der untersuchten Finanzinstitute, welche ein App Verfahren anbieten, haben dieses in die Banking App integriert.
6. **Finanzinstitute, welche ein App Verfahren anbieten, bieten oft noch ein SMS-OTP Verfahren als alternatives Verfahren an:** 69% der untersuchten Finanzinstitute, welche ein App Verfahren anbieten, bieten auch ein SMS OTP Verfahren an.
7. **Finanzinstitute, welche SMS OTP Verfahren anbieten, bieten meist ein Alternativverfahren an:** 81% der untersuchten Finanzinstitute, welche ein SMS OTP Verfahren anbieten, bieten ein weiteres Verfahren zur Authentifizierung an.
8. **Finanzinstitute, welche SMS OTP Verfahren anbieten, machen dies für den Karteninhaber nur sehr selten kostenpflichtig:** 2% der untersuchten Finanzinstitute, welche ein SMS OTP Verfahren anbieten, berechnen dem Karteninhaber eine Gebühr für das Versenden des OTP per SMS.
9. **Nur sehr wenige Finanzinstitute bieten ein alternatives Verfahren zum App und SMS OTP Verfahren an:** 10% der untersuchten Finanzinstitute bieten ein Authentifizierungsverfahren an, welches nicht ein App oder SMS OTP Verfahren ist.

Issuer mehrheitlich regulatorisch konform, einige wenige Institute sind noch immer nicht compliant aufgestellt

Wenig überraschend bestätigt Kernaussage 1, dass alle Banken ein auf dem 3-D Secure basierendes Verfahren zur starken Kundenauthentifizierung anbieten. Trotz der in Kernaussage 4 festgehaltenen 5% der Finanzinstitute[12], welche zum Untersuchungszeitpunkt kein PSD2-konformes Authentifizierungsverfahren umgesetzt haben, lässt sich festhalten, dass die Banken zum Stichtag 1. Januar 2021 mit deutlicher Mehrheit PSD2-ready sind. Unabhängig von der regulatorischen Readiness der Banken, gilt es jedoch auszuwerten, welche Verbesserungspotenziale die Banken bei der Umsetzung bisher ungenutzt lassen.

[10] Dezember 2020

[11] Dezember 2020

[12] Von diesen gelten für 5 von 8 aufgrund ihrer Domizilierung in der EU die Regelungen der PSD2, die verbleibenden 3 Schweizer Issuer sind nicht Verpflichtete im Sinne der PSD2

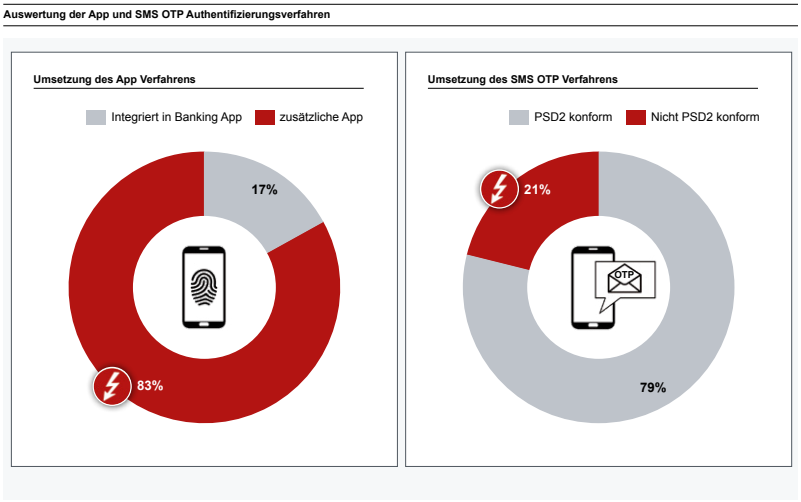


Abbildung 12: Auswertung zur Umsetzung der Authentifizierungsverfahren

Wenig überraschend bestätigt Kernaussage 1 in Kombination mit Kernaussage 2, dass die Finanzinstitute klar auf App und SMS OTP Verfahren zur Authentifizierung setzen. Das SMS OTP Verfahren ist historisch gewachsen und wird noch heute trotz annähernd vollkommender Smartphone-penetration von den Finanzinstituten gerne als Fallback genutzt, um auch nicht Smartphone-affinen Kundengruppen das Zahlen im E-Commerce zur ermöglichen. Diese Hypothese wird auch durch Kernaussage 7 nochmal insofern bestätigt, dass ca. 70% der untersuchten Finanzinstitute, welche ein App Verfahren anbieten, auch ein SMS OTP Verfahren als Alternative anbieten. Immerhin 19% der untersuchten Finanzinstitute bieten lediglich das SMS OTP Verfahren zur Authentifizierung an (siehe dazu Kernaussage 7). Neben der offensichtlichen und nicht zu vernachlässigenden Kostenkomponente für den meist durch die Bank zu tragenden Versand der SMS[13], ist dies auch eine Frage der Sicherheit: Es ist hinlänglich bekannt, dass der Versand von vertraulichen Informationen via SMS ungern von CISOs gesehen wird – so auch die Empfehlung vom Bundesamt für Sicherheit in der Informationstechnik (BSI).[14] Auch die EU Kommission hat sich in ihrer jüngst veröffentlichten „EU Strategie für den Massenzahlungsverkehr“ dafür ausgesprochen moderne Authentifizierungsverfahren zu etablieren, wobei ältere Technologien, wie der Versand von Einmal-Passwörtern per SMS, konsequent abgelöst werden sollen.

App basierte Authentifizierungsverfahren präferiert, SMS OTP aber immer noch deutlich präsent im Markt

Auch wenn SMS OTP noch immer weit verbreitet ist, scheinen App-basierte Verfahren von den Banken präferiert zu werden. Das zeigen zum einen die in Kernaussage 2 festgehaltenen 81% der untersuchten Finanzinstitute, welche ein App Verfahren anbieten, aber auch die prominente Platzierung der App Authentifizierungslösungen auf den Webseiten der Banken, welche im Rahmen der Recherche für diese Analyse untersucht wurde. Dies ist nachvollziehbar vor dem Hintergrund, dass die Nutzung der App für die Bank meist kostengünstiger ist und zudem dem Karteninhaber eine

[13] Lediglich 3% der untersuchten Finanzinstitute berechnen dem Karteninhaber eine Gebühr für das Versenden des OTP per SMS – siehe dazu Kernaussage 9

[14] Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/mTAN-Verfahren.html

höhere Convenience und Sicherheit bieten kann (z.B. durch den Einsatz von Biometrie zum App-Login). Es ist dabei jedoch bemerkenswert, dass die Banken diesen Weg nicht mit mehr Nachdruck verfolgen. So bedeutet die Integration der Authentifizierungslösung in die eigene Banking App nicht nur einen App-Download und Enrollment-Prozess weniger für den Kunden, sondern bietet auch einen wiederkehrenden Grund, die Kunden in die Banking App zu leiten und diese Kundenkontaktpunkte für Cross-Selling Opportunitäten zu nutzen. Dennoch bieten 83% der untersuchten Finanzinstitute, welche ein App Verfahren anbieten, dieses in einer gesonderten Authentifizierungsapp an. Dies kann nur bedingt dadurch erklärt werden, dass in den Anfangsjahren der Banking-Apps in der Auslegung des BSI zwei separate Apps noch als sicherer angesehen wurden, denn spätestens mit der PSD2, also ab 2015, waren auch Single-App Lösungen rechtssicher. Es erstaunt daher, dass neben den bekannten FinTech Playern (Revolut, N26, etc.) es lediglich eine Handvoll etablierter Banken gibt, welche den Schritt zu einer Single-App Strategie bereits gegangen sind.

Über den strategischen Ansatz und die Umsetzung der Authentifizierungsfrontends hinaus, offenbarten sich im Rahmen der Recherche weitere Optimierungspotenziale: Die sich aus den PSD2 RTS Ausnahmen ergebenden Möglichkeiten auf eine starke Kundenauthentifizierung zu verzichten, beispielsweise über ein Empfänger-Whitelisting oder den TRA bzw. RBA, bleiben oft ungenutzt. Stattdessen werden augenscheinlich starre Regeln eingesetzt, die darüber entscheiden, ob eine Authentifizierung abgefragt wird oder nicht. Folglich werden mehr Authentifizierungen durchgeführt, als regulatorisch notwendig wäre.

Nur wenige Issuer nutzen die in der RTS offerierten Ausnahmen durch Whitelisting und Risiko-Scoring

Da die Information über das bankeninterne Risiko-Scoring und entsprechende Regeln aus offensichtlichen Gründen nicht öffentlich transparent gemacht werden, ist eine Einbeziehung des Risiko-Scorings der einzelnen Finanzinstitute in die quantitative Analyse nicht möglich. Mittels einer großen Stichprobe an Testkäufen konnte dieser Eindruck jedoch plausibilisiert werden.

So schienen beispielsweise wiederholt authentifizierte Transaktionen mit ähnlichen Beträgen beim gleichen Merchant keinen Einfluss auf die Authentifizierungsentscheidung der Folgetransaktionen zu haben. Die regulatorischen Freiräume und damit die Potenziale für eine positive Wettbewerbsdifferenzierung bei gleichzeitiger Erhöhung des Sicherheitsniveaus bleiben also zu großen Teilen ungenutzt und die starren und damit antizipierbaren Regeln stellen eine Einladung für Betrüger dar. Die Idee einer Starken Kundenauthentifizierung wird also durch eine schwache Umsetzung korrumpiert.

Es muss daher festgehalten werden, dass ein Großteil der analysierten Banken in ihrem aktuellen Setup durch die im Laufe diesesJahres durchzusetzenden SCA Anforderungen mit großen Herausforderungen konfrontiert werden: Aufgrund der fehlenden Nutzung der in der RTS ermöglichten SCA Ausnahmen wird die Anzahl der notwendigen Authentifizierungen signifikant zunehmen. Damit wird die Nutzerfreundlichkeit im Kaufprozess eingeschränkt, was Kaufabbrüche und damit Umsatzrückgänge durch fehlende Interchange-Erträge zur Folge haben wird. Mittelfristig drohen

Bei einem Großteil der analysierten Issuer sind vermehrte Kaufabbrüche, Kundenabwanderung und steigende Authentifizierungskosten zu erwarten

zudem die Kunden zu Wettbewerbern abzuwandern, welche die SCA Anforderungen besser umgesetzt haben, indem sie ihre Authentifizierungslösungen auf die neuen Anforderungen und Möglichkeiten optimiert haben. Darüber hinaus werden auch die Authentifizierungskosten steigen, da bei vielen Issuern das immer noch präsente und mit hohen Kosten verbundene SMS OTP Verfahren häufiger zum Einsatz kommen wird.

4 Chancen für Banken

Mit den im vorherigen Kapitel aufgezeigten Herausforderungen gehen auch entsprechende Chancen für die Banken einher, welche sich diesen Herausforderungen stellen und ihre Lösungen entsprechend anpassen – sowohl Kostenersparnisse als auch Umsatztreiber können an dieser Stelle genannt werden.

Kostenersparnisse lassen sich durch die Abschaffung von Legacy (Abschaffung von historisch gewachsenen Authentifizierungsmethoden wie bspw. Chip TAN oder SMS OTP) oder aber durch die Schaffung von Synergien (bspw. durch den Umschwung auf eine Ein-App-Strategie und damit der Abschaltung der separaten Authentifizierungsapp) realisieren.

Substitution des SMS OTP Verfahrens bietet deutliche Vorteile in Hinblick auch Sicherheit, Convenience und Kosten

Am greifbarsten lässt sich eine mögliche Kostenersparnis bei der Authentifizierung per SMS OTP am Beispiel eines fiktiven Issuers erklären: Ausgehend von einem Portfolio von 1 Million Karten, welche alle für ein SMS-Authentifizierungsverfahren enrollt sind, kann mit 7 versendeten SMS pro Karte[15], also 7 Millionen SMS pro Jahr gerechnet werden. Bei EUR 0,07 pro SMS-Versand ergeben sich somit laufende Kosten von EUR 490.000 pro Jahr. Zu diesen laufenden Kosten von knapp einer halben Million lassen sich noch etwaige fixe Betriebskosten (Betrieb SMS Gateway, Enrollmentkosten, regelmäßiges Regressionstesting, etc.) addieren. Dabei basiert diese Beispielrechnung auf empirischen Zahlen in einer prä-PSD2 Beobachtung – insofern ist zukünftig mit tendenziell noch mehr notwendigen Authentifizierungen ergo zu versendenden SMS zu rechnen, wodurch die Einsparpotenziale ebenso wachsen.

Einsatz eines Risiko-Scorings steigert Convenience, hilft Kaufabbrüche zu vermeiden und ermöglicht positive Wettbewerbsdifferenzierung

Die Anzahl notwendiger Authentifizierungen ließe sich zudem durch die Nutzung vorhandener PSD2 Ausnahmen deutlich reduzieren: Zum einen könnte den Kunden die Möglichkeit offeriert werden, Merchants bei denen sie häufiger einkaufen auf eine Whitelist zu setzen. Dies würde den Issuern langfristig Authentifizierungskosten sparen und zudem die Convenience für den Karteninhaber erhöhen. Ferner könnte die TRA-Ausnahme (bzw. im 3-D Secure Kontext RBA) durch Integration eines intelligenten Risiko-Scoring Systems genutzt werden, sodass Transaktionen bis zu EUR 500 regelmäßig auch ohne Authentifizierung auskommen. Auch dadurch lassen sich nicht nur die Authentifizierungskosten entsprechend reduzieren, die Convenience erhöhen, sondern es resultieren auch umsatzseitig zusätzliche Chancen: Vor dem Hintergrund, dass 2010 in Deutschland noch rund 25,3 Millionen und 2019 bereits 44,2 Millionen Kreditkarten[16] im Umlauf waren, hat die durchschnittliche Zielkundschaft der hiesigen Issuer mehr als eine Kreditkarte im Portemonnaie. Hinzu kommt, dass die neue Generation Debitkarten, Debit Mastercard und Visa Debit, welche derzeit zunehmend im Markt ausgerollt werden, analog einer Kreditkarte auch im E-Commerce einsetzbar sind. Folglich hat der Kunde eine Auswahl, welche seiner Karten er für einen Onlinekauf nutzt. Durch eine effiziente Umsetzung des Risiko-Scorings und der Authentifizierungslösungen kann dabei ein möglichst reibungsloses Kundenerlebnis geschaffen werden, welches sich beim Karteninhaber als wettbewerbsdifferenzierend auswirken kann,

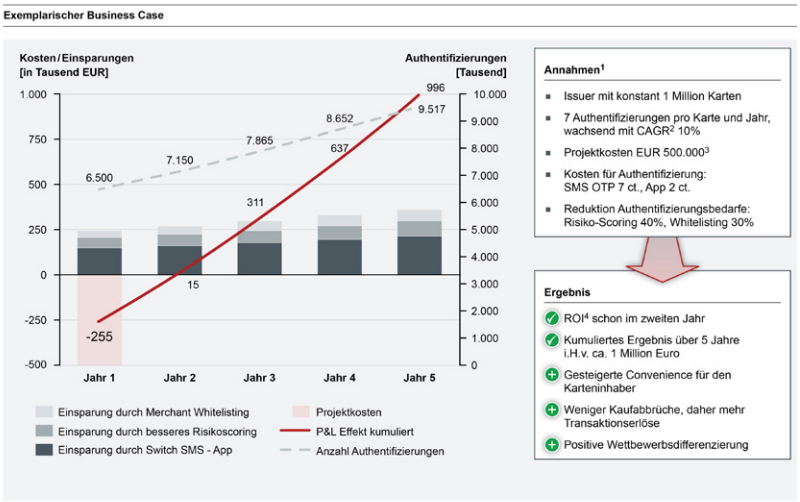
[15] Empirischer Durchschnitt einer Auswahl repräsentativer Issuer auf dem deutschen Markt

[16] https://de.statista.com/statistik/daten/studie/171485/umfrage/marken-der-persoenlichen-kreditkarten/#:~:text=Kreditkarten%20haben%20sich%20in%20Deutschland,bei%20etwa%2035%2C9%20Millionen.

denn 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 für Einkäufe im E-Commerce nur noch die Karte von Bank B nutzt.

Zudem lässt sich die im Kontext des Risiko-Scorings für die Authentifizierung gewonnene Datenbasis auch für das nachgelagerte Risiko-Scoring für die Autorisierungsentscheidung nutzen und durch diese holistische Sicht auf die Transaktion die Güte der Risikoprävention deutlich verbessern.

Insbesondere wenn die Authentifizierungslösung und die dahinterliegende Architektur nicht nur auf den Einsatz im 3-D Secure Kontext beschränkt ist, sondern noch weitere Authentifizierungs-Anwendungsfälle in der Bank, wie etwa die Freigabe von Überweisungen oder den Zugriff auf das Online Banking inkludiert, lässt sich nicht nur die Anwendungslandschaft für den Kunden vereinfachen, sondern es lassen sich auch signifikante finanzielle und operative Vorteile erschließen.



Quelle: COREresearch 2021 | ¹Gemittelt aus Projekterfahrungen bei europäischen Banken | ²Compound annual growth rate | ³Betriebskosten konstant | ⁴Return on Investment

Abbildung 13: Exemplarischer Business Case auf Basis gemittelter Projekterfahrungen

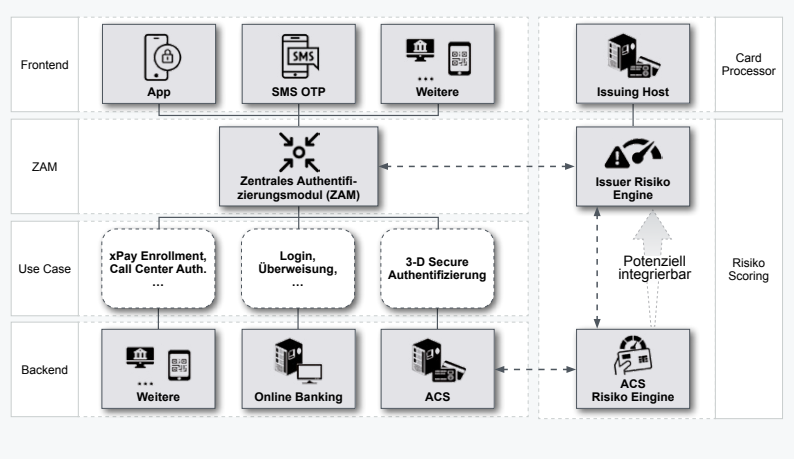
5 Lösungsmuster

Um die beschriebenen Chancen für Issuer unter Berücksichtigung der erörterten Herausforderungen zu adressieren, sollen nachfolgend konkrete Lösungsansätze und Handlungsempfehlungen für Issuer als primäre Adressaten dieses Whitepapers ausgeführt werden.

Aufbau eines Zentralen Authentifizierungsmoduls (ZAM) ist das Rückgrat einer modernen Authentifizierungs-Architektur

Der wesentliche Baustein der Ziellösung ist hierbei ein zentrales, primäres Authentifizierungsmodul über alle Portfolien und Produkte hinweg, d.h. es soll die gleiche Authentifizierungsmethodik im 3-D Secure Kontext verwendet werden, wie auch bspw. für die Autorisierung von Überweisungen oder den Zugang zum Online Banking. Dabei ist zu beachten, dass hiermit nicht das Authentifizierungs-Frontend für den Karteninhaber gemeint ist, sondern eine zentrale Authentifizierungsinstanz innerhalb der bankinternen Architektur, über die alle Authentifizierungen gesteuert werden. Dieses Zentrale Authentifizierungsmodul (ZAM – siehe Abbildung 14) sollte kundenzentriert aufgesetzt werden und die einzelnen Authentifizierungs-Frontends, sowie die Backends der einzelnen Produkte mit Authentifizierungsbedarf via API anbinden. Dafür muss das ZAM hinreichend stabil sowie skalierbar konzipiert und umgesetzt werden.

Exemplarisches Architekturschaubild als Lösungsmuster



Quelle: COREresearch 2021

Abbildung 14: Exemplarisches Architekturschaubild

Die Konvergenz der Anwendungsfälle und die verbundenen Skaleneffekte auf der System- und Infrastruktur-Ebene können dabei zu einer signifikanten Kostenreduktion gegenüber den aktuell im Markt beobachtbaren Legacy-Architekturen beitragen.

Um den Anwendungsfall einer 3-D Secure Authentifizierung abbilden zu können, muss das ZAM an einen ACS angebunden werden. Da Setup, Zertifizierung und Betrieb eines ACS vergleichsweise aufwändig sind und daher eine entsprechende Skalierung für den wirtschaftlichen Einsatz notwendig ist, bietet sich hier der Bezug als Service von einem externen ACS Provider an.

Im Falle einer notwendigen starken Kundenauthentifizierung übermittelt der ACS eine Authentifizierungsanfrage an das ZAM. Dieses ermittelt den entsprechenden Karteninhaber und die zur Verfügung stehenden (vom Karteninhaber aktivierten) Authentifizierungsverfahren und löst eine entsprechende Authentifizierungsanfrage im für den jeweiligen Anwendungsfall priorisierten Frontend aus. Zeitgleich wird dem ACS zwecks Anzeige des richtigen CAP Screens im Zahlungsprozess die gewählte Authentifizierungsmethode angezeigt. Abschließend muss dem ACS vom ZAM lediglich das Resultat der Authentifizierung mitgeteilt werden. Somit liegt die Hoheit des Authentifizierungsprozesses bei der Bank selbst, und nicht – wie heute üblich – ausgelagert bei dem ACS Provider. Dies erleichtert nicht nur etwaige nötige zukünftige Anpassungen, sondern ermöglicht auch eine holistische Datenerfassung über die Transaktion und den Karteninhaber. Zu Gunsten eines verbesserten Risiko-Scorings ist auch zu einer Kopplung bzw. Konsolidierung der Risiko-Scoringsysteme zu raten: Üblicherweise ist das Scoring für die Authentifizierung heute ein Service des ACS und damit für die Bank nicht direkt einsehbar. Eine Internalisierung verspricht höhere Freiheitsgrade, da die Bank selbst Regeln konfigurieren kann, die volle Hoheit über die Authentifizierungsdaten hat und diese ggf. noch mit etwaigen Risikodaten aus anderen Anwendungen anreichern kann – bspw. Provisionierungsinformationen aus dem Mobile Payment Enrollment oder Authentifizierungsdaten aus dem Online Banking. Wenn auch eine Konsolidierung der Risikosysteme auf Grund der erhöhten Komplexität nur langfristig eine valable Option ist, so ist doch zumindest eine technische Kopplung der Risikosysteme zum gegenseitigen Datenaustausch kurz- bis mittelfristig anzustreben. Darüber hinaus sollte sich der Einsatz des Risiko-Scorings nicht auf die Verwendung für die TRA-Ausnahmen gemäß PSD2 RTS beschränken, sondern auch Low-Value Transaktionen unter EUR 30 sollten berücksichtigt werden, um eine größere Datenbasis zu schaffen und die Antizipierbarkeit für Betrüger zu erschweren. Der Einsatz von Fuzzy-Logiken für die jeweiligen Regelgrenzwerte kann dies zusätzlich unterstützen.

Umfassendes und Use Case übergreifendes Risiko-Scoring ermöglicht Verbesserung der Convenience und Kostenoptimierung auch außerhalb des Zahlungsverkehrs

Auch bei der Umsetzung der Authentifizierungs-Frontends gibt es Synergiepotenziale: Zunächst kann aufgrund der höheren Sicherheit, Convenience und langfristig auch Wirtschaftlichkeit die klare Empfehlung für ein App-basiertes Authentifizierungsverfahren ausgesprochen werden. Dieses sollte dabei in die eigene Banking App integriert werden, was die Nutzung der Banking App stärkt, den Kunden einen App-Download und ein separates Enrollment erspart und oft auch mit geringeren Betriebskosten einhergeht. Die Authentifizierungsmethode zum Login in die Banking App ist dabei idealerweise dieselbe wie zur Authentifizierung der Transaktion oder für die Bestätigung des E-Banking Logins. Auch wenn zu einer Platzierung des App Verfahrens als primäre Authentifizierungsvariante zu raten ist, gilt es auch Alternativen anzubieten. Dies gilt vor allem für Banken, bei denen eine App für den Kunden nicht zwangsläufig vorausgesetzt ist. Dieses Angebot für non-Smartphone Zielgruppen sollte passiv positioniert sein, wobei auch hier eine zentrale Steuerung über das ZAM die nötige Flexibilität bietet.

Perspektivisch wäre zudem zu prüfen, welche alternativen Authentifizierungsverfahren für die non-App Zielgruppe umsetzbar sind. Hierbei bestehen verschiedene Initiativen wie etwa die FIDO Alliance[17] im Markt, welche die Schaffung eines globalen Authentifizierungsstandards intendiert, der auch entsprechend zertifizierte Hardware-Devices ermöglichen soll.

[17] Fast IDentity Online

Im Falle mehrerer parallel angebotener Authentifizierungsoptionen wäre auch der Switch zu einem alternativen Verfahren während des Authentifizierungsprozesses denkbar – entweder durch den Kunden selbst im CAP Screen, oder per Time-out getriggert. Hierdurch lässt sich die Kaufabbruchquote zusätzlich verringern, z.B. wenn der Kunde grade mit seinem Smartphone keinen Internetempfang hat, wohl aber eine SMS empfangen kann.

Unabhängig von der Umsetzung der Authentifizierungs-Frontends gilt grundsätzlich weiterhin, dass im idealen Ablauf eine starke Authentifizierung durch den Kunden gar nicht erst nötig wird. Zum einen ist dafür der Aufbau eines effektiven Risiko-Scorings unerlässlich, zum anderen gilt es aber auch die von der PSD2 gewährten Ausnahmen mit einer adäquaten Risikoaffinität einzusetzen. Hierbei kann das System durch eine über die Zeit anwachsende Datenbasis und unter Einsatz intelligenter Algorithmen (z.B. Deep Learning, Reinforcement Learning) das System weiter optimiert werden. Dies bedingt jedoch einen möglichst frühzeitigen Markteinsatz, da es andernfalls zunehmend schwieriger wird, die notwendige Datengrundlage und Expertise vor dem Wettbewerb aufzubauen. Zudem sollten sich Banken überlegen, ob die Kompetenzen im Bereich Analytics und Risiko-Scoring intern aufgebaut, oder extern gesourced werden sollen. Letzteres wird per Definition dazu führen, sich in diesem Bereich nicht vor dem Markt platzieren zu können. Jedoch ist der Aufbau von internen Kompetenzen schwierig sowie langwierig und die im Markt rekrutierbaren Experten in diesem Gebiet sind auch über die Finanzbranche hinaus stark umworben.

Whitelisting gibt Karteninhabern mehr Entscheidungsfreiheit und kann Issuern als zusätzliches Differenzierungsmerkmal dienen

Neben dem vglw. komplexen und zeitintensiven Aufbau des Risiko-Scorings kann zudem die Implementierung eines Merchant Whitelistings empfohlen werden, welches dem Karteninhaber ermöglicht bei vertrauten Merchants zukünftige Transaktionen i. d. R. nicht mehr stark authentifizieren zu müssen. Auch hierdurch lässt sich derzeit noch eine positive Wettbewerbsdifferenzierung realisieren.

6 Fazit

Die Anforderungen zur starken Kundenauthentifizierung der PSD2 RTS bedeuten eine deutliche Verschärfung der regulatorischen Vorgaben und sind für Issuer und Merchants gleichermaßen eine große Herausforderung. Ob dieser regulatorische Eingriff in einen bestehenden Wachstumsmarkt notwendig und verhältnismäßig ist, kann kritisch hinterfragt werden, jedoch scheint nach langer Zeit des öffentlichen Diskurses, welcher auch mehrfache Nachschärfungen und Verschiebungen von Anforderungen zur Folge hatte, die Durchsetzung in 2021 besiegelt. In Bezug auf Kartenzahlungen im immer wichtiger werdenden E-Commerce ist die starke Kundenauthentifizierung de Facto mit 3-D Secure gleichzusetzen, wobei die Protokollversionen 3-D Secure 2.x die Anforderung, aber auch die Ausnahmeregelungen der PSD2 abdecken.

Ein Blick in den Markt zeigt, dass die Durchdringung auf der Merchant-Seite noch immer weit hinter dem regulatorischen Ambitionsniveau zurückbleibt, doch auch auf Seiten der Issuer ist die Situation weiterhin angespannt: Die Marktanalyse hat gezeigt, dass zwar ein Großteil der 111 untersuchten Issuer grundsätzlich ggü. den PSD2 RTS Anforderungen compliant aufgestellt ist, jedoch sind die beobachtbaren Umsetzungen meist eher taktische Interimslösungen als strategisch platzierte Antworten auf eine elementare Herausforderung im modernen Zahlungsverkehr. Das ausgeführte Lösungsmuster zeigt dabei, dass eine umfassend durchdachte und mit hinreichend technologischem Know-how umgesetzte Lösung nicht nur die Convenience für den Kunden erhöht, sondern langfristig auch deutliche finanzielle Vorteile für den Issuer bietet. Der Umstand, dass trotz der langen Vorlaufzeit nur wenige Issuer die technologischen und regulatorischen Möglichkeiten nutzen, belegt, dass dem Thema bislang nicht hinreichend Aufmerksamkeit entgegengebracht wurde. Für betroffene Issuer wird dies mittelfristig zur Gefahr, denn die Umsetzung der Authentifizierungsarchitektur wird insbesondere unter Einsatz der RBA/TRA Ausnahmen zum wettbewerbsdifferenzierenden Faktor. Den Wettbewerb stellen dabei nicht nur andere Issuer dar, sondern auch andere Zahlungsanbieter wie etwa PayPal, die sich bereits seit geraumer Zeit durch hohe Convenience und überdurchschnittliches Risikohandling absetzen. Dabei lebt ein effektives Risiko-Scoring von der konstanten Datenzufuhr, was abermals postuliert: Je früher der Issuer ein Risiko-Scoring umsetzt, desto größer ist die Wahrscheinlichkeit, dass sich dieses qualitativ absetzen kann. Der in der durchgeführten Analyse offenbarte Entwicklungsstand des Marktes kann also auch als strategische Chance verstanden werden. Umgekehrt werden Issuer, die kurzfristig keine adäquate Lösung umsetzen, diesen Rückstand zunehmend schwerer aufholen können. Es empfiehlt sich daher das eigene Setup einem Review zu unterziehen, eine auf das eigene Institut abgestimmte Zielarchitektur abzuleiten und diese schnellstmöglich, mit der notwendigen Expertise und den richtigen Vendoren umzusetzen. Andernfalls droht nicht nur dieses Handlungsfeld, sondern der ganze Wettstreit um die Kundenschnittstelle im Retail-Zahlungsverkehr verloren zu gehen, denn eine mangelhafte Umsetzung der starken Kundenauthentifizierung bei Kartenzahlungen im Fernabsatz schadet Merchants und Issuern gleichermaßen und stärkt in der Konsequenz die alternativen Bezahlverfahren von Google, Apple oder PayPal, bei denen Banken nicht mehr direkt an der Kundenschnittstelle agieren. Ein Bedeutungsverlust, der sich auch finanziell auswirken wird und aus perspektive der Europäischen Finanzindustrie unbedingt vermieden werden sollte.

Erneuerung der Authentifizierungs-Architektur für die meisten der untersuchten Banken strategisch angeraten und zeitkritisch

7 Abkürzungsverzeichnis

Abkürzung	Ausgeschrieben
ACS	Access Control Server
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISO	Chief Information Security Officer
EBA	European Banking Authority
ETV	Exemption Threshold Value
MCC	Merchant Category Codes
OTP	One Time Passwort
PSD2	Payment Services Directive 2
RBA	Risk Based Authentication
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
TAN	Transaction Authentication Number
TRA	Transaction Risk Analysis
URL	Uniform Resource Locator
ZAM	Zentrales Authentifizierungsmodul

Autoren

Benedikt von Hake ist Transformation Manager bei CORE. Seine Schwerpunktthemen umfassen Zahlungsverkehr, digital & mobile Payment Solutions und 3-D Secure. Bei CORE blickt Benedikt auf umfassende Erfahrungen rund um die Entwicklung und Umsetzung von kartenbasierten Bezahllösungen zurück.

Benedikt von Hake
benedikt.hake@core.se

Dominik Siebert ist Managing Partner 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 Positionierung von Bezahllösungen mit Schwerpunkt Kartenzahlungen.

Dominik Siebert
dominik.siebert@core.se

Johannes Steinbrecher betreut als Senior Expert Manager bei CORE SE unterschiedlichste Projektvorhaben im Bereich Zahlungsverkehr von der Konzeption bis zur Umsetzung und fokussiert dabei Akzeptanzlösungen im E-Commerce und im stationären Handel.

Johannes Steinbrecher
johannes.steinbrecher@core.se

Tim Gieske ist Transformation Manager bei CORE. Seine Schwerpunkte umfassen digitale und mobile Payment Solutions, Zahlungsverkehr und Venture Investitionen. Bei CORE fokussiert sich Tim auf Projekte zur Entwicklung und Umsetzung von mobilen und kartenbasierten Bezahllösungen.

Tim Gieske
tim.gieske@core.se

Über COREresearch

Als unabhängiger Technologie Think Tank erforschen wir die Systematik technologisch getriebener Transformationen in Industrien mit einem hohen Anteil an IT im Wertschöpfungsprozess. Im Rahmen unserer Forschungsaktivitäten analysieren wir Märkte und Technologien, thematisieren Strukturen, Ursachen und Wirkmechanismen des technologischen Wandels und kuratieren Ergebnisse für Klienten und die Öffentlichkeit. Darüber hinaus stellen wir ausgewählte Resultate unserer interdisziplinären Forschungen im Rahmen von übergreifenden Publikationen, Einzelstudien sowie Vorträgen einer breiteren Öffentlichkeit zur Verfügung.

https://core.se

Disclaimer

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