

Quo vadis PSD2?

EBA-Kommentar hinterlässt weitere
Unklarheiten | Handel reagiert
zurückweisend | Erste Länder gewähren
Übergangsfristen

Key Facts

- › Die EBA hat am 21. Juni ein abschließendes Positionspapier zur starken Kundenauthentifizierung (SCA) mit Konkretisierung der Umsetzungscharakteristika veröffentlicht und gewährt Übergangsfristen als Reaktion auf Marktrückfragen
- › England, Österreich und Italien haben Übergangsfristen angekündigt, Regulatoren in Irland, Frankreich und Dänemark bewerten Verschiebungen
- › Prominent besetztes Konsortium rund um die „European Payment Institutions Federation“ (EPIF) richtet weiteren Brandbrief an die EBA und fordert einheitlichen Aufschub und Transparenz
- › EBA im Dilemma: Konsequenz oder Nachsicht?
- › Chance für nationale Regulatoren, europäisch zu handeln

Ausgangslage: EBA-Positionspapier vom 21. Juni 2019

Am 14. September 2019 werden die Pflichten zur starken Kundenauthentifizierung der PSD2 wirksam. Als Reaktion auf die fortwährende Diskussion und weiter bestehende Unklarheiten zur Auslegung der in der finalen „Regulatory Technical Standards (RTS)“ spezifizierten Umsetzungsvorgaben hatte die EBA am 21. Juni 2019 – weniger als drei Monate vor Inkrafttreten der RTS – ein weiteres und nach eigener Aussage abschließendes Positionspapier veröffentlicht (<https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf>).

Dabei haben insbesondere zwei Aspekte für Aufsehen im Markt gesorgt (siehe auch: <https://core.se/de/techmonitor/eba-kommentar-zur-psd2-rtS-aufloesen-von-unklarheiten-wirft-neue-fragen-auf>):

Aspekt 1 - EBA eröffnet Möglichkeit von Übergangsfristen

Bis zur Veröffentlichung des EBA-Kommentars war die im Markt vorherrschende Auslegung, dass ab dem 14. September 2019 alle betroffenen Marktteilnehmer die RTS mandatorisch umzusetzen haben.

Im EBA-Papier wurde nunmehr eingeräumt, dass die national zuständigen Behörden in Ausnahmefällen entscheiden können, die Umsetzungsfrist der SCA-Anforderungen zeitlich begrenzt zu verschieben. Ein derartiges Zugeständnis setzt voraus, dass betroffene PSPs¹ einen Migrationsplan erstellen und diesen mit den nationalen Behörden abstimmen. Nur eine Woche nach Veröffentlichung des EBA-Kommentars kündigte die britische Financial Conduct Authority (FCA) an, von der Möglichkeit der Verschiebung um bis zu 18 Monate Gebrauch zu machen. Weiterhin proklamiert die FCA, „in enger Abstimmung mit der Branche“ einen Migrationsplan erarbeiten zu wollen. Analog dazu reagierten die österreichische Finanzmarktaufsicht (FMA) sowie die Banca d'Italia Anfang August und gewährten Unternehmen einen zeitlichen Aufschub bei der Umsetzung

¹ PSPs im Sinne der RTS umfassen sowohl Payment Service Provider im klassischen Sinne sowie Issuer

der Anforderungen. Darüber hinaus sprachen sich in der Zwischenzeit Regulatoren aus Frankreich, Irland und Dänemark öffentlich für eine generelle zeitliche Verschiebung der Umsetzungsverpflichtung aus.

Aspekt 2 - Inhärenz bei 3-D Secure 2.x

Bis zum EBA-Kommentar war die vorherrschende Marktwahrnehmung, dass das 3-D Secure 2.x Protokoll für die Karteninhaber-Authentifizierung im Distanzgeschäft die SCA-Anforderungen der PSD2 vollumfänglich abdecke.

Liste möglicher Inhärenz-Elemente (Auswahl)		CORE®
Element	Zulässig für SCA*	
 Fingerprint Scanning	Ja	✓
 Stimmenerkennung	Ja	✓
 Venen Scanning	Ja	✓
 Hand- und Gesichtsgeometrie	Ja	✓
 Retina und Iris Scanning	Ja	✓
 Anschlagdynamik	Ja	✓
 Herzschlag oder andere physiologische Bewegungsmuster, die identifizieren, dass der PSU der PSU ist (z.B. für Wearables)	Ja	✓
 Der Winkel, mit dem ein Endgerät gehalten wird	Ja	✓
 Informationen übertragen über ein Kommunikationsprotokoll, so wie EMV® 3-D Secure	Nein (für Ansätze, die zurzeit im Markt zu beobachten sind)	✗
 Eingepprägter Swiping Path	Nein	✗

* Zulässigkeit für SCA ist abhängig von der jeweiligen Implementierung dieser Elemente

Abbildung 1: Übersicht möglicher Inhärenz-Elemente gemäß EBA-Positionspapier

Entsprechend sorgte die Einordnung der EBA für Unsicherheit, dass zumindest die bisher im Markt ersichtlichen Umsetzungen zur Nutzung von Biometrie im Kontext 3-D Secure nicht den formulierten Ansprüche an einen Inhärenz-Faktor gerecht würden (Abbildung 1; vgl. <https://core.se/de/techmonitor/sicherheit-im-kartenbasierten-zahlungsverkehr>), wenngleich der EBA-Kommentar Interpretationsspielräume offen ließ.

Marktreaktion: Forderungen von Handelsverbänden

Als Reaktion auf den EBA-Kommentar hat ein Konsortium aus *European Payment Institutions Federation* (EPIF), Visa, Mastercard, den Händlerverbänden *EuroCommerce* und *E-Commerce Europe*, der *European Association of Payment Service Providers for Merchants* (EPSM), des *European Hotel Forums* und der *European Tourism Association* am 2. August einen öffentlichen Brandbrief an die EBA und die EU-Kommission übersandt. Darin bestätigen die Unterzeichner ihre grundsätzlich positive Haltung gegenüber der Verbreitung der SCA, monieren jedoch energisch die von der EBA im Positionspapier avisierten Auslegungen zu oben genannten Punkten:

Marktkonsortium fordert einheitliche Regelung für Umsetzungsfrist

Die Unterzeichner thematisieren, dass trotz der 18-monatigen Umsetzungsfrist weite Teile des Marktes sowohl auf der Issuing- als auch auf der Merchant-Seite noch nicht vollumfänglich auf die am 14. September umzusetzenden Anforderungen vorbereitet seien. Verweisend auf eine Studie von Stripe wird konstatiert, dass allein im ersten Jahr der Umsetzung ein Verlust i.H.v. EUR 57 Mrd. im PSD2-Wirkungsraum durch Kaufabbrüche zu erwarten sei.

Die Öffnung der EBA für Übergangsfristen würde dementsprechend begrüßt, jedoch sei der Ansatz, die Nutzung und Ausgestaltung ebendieser in die Obhut der nationalen Regulatoren zu übergeben, kontraproduktiv und würde die Komplexität der Umsetzung sogar noch erhöhen: so würde beispielsweise im Szenario, dass die FCA einen Aufschub gewährt, die BaFin jedoch nicht, ein deutscher Issuer Transaktionen eines Acquirers aus UK ablehnen müssen, der im Rahmen seiner national geltenden Vorschriften die SCA-Anforderungen noch nicht umgesetzt habe. Viele Acquirer seien jedoch länderübergreifend aktiv und müssten entsprechend unterschiedliche Vorgaben in den jeweiligen Zielmärkten reflektieren. In der Konsequenz würde vor allem der Kunde ein inkonsistentes Einkaufserlebnis nicht nachvollziehen können, was unmittelbar zu erhöhten Kaufabbrüchen führen würde, weswegen die Annahmen der Stripe-Studie nachzuvollziehen seien.

Die Ankündigungen aus Österreich, Italien, Irland, Frankreich und Dänemark lassen vermuten, dass es sich bei dem aufgeführten Beispiel nicht um einen Ausnahmefall handelt, sondern dass Europa eine regulatorisch heterogene Gesamtsituation bezüglich der Umsetzungsfristen der RTS und einhergehender Implimentierungen droht.

Folglich fordern die Unterzeichner einen europaweit einheitlichen Fahrplan zur Umsetzung der SCA-Anforderungen und einen Aufschub von mindestens 18 Monaten sowie eine Bekanntgabe dieses Fahrplans noch vor dem 14. September. Dabei wird nicht nur die EBA selbst angesprochen, sondern es wird konstatiert, dass ebenso eine abgestimmte Auslegung der Übergangsfristen durch die nationalen Regulatoren dieses Zielbild erreichen könnte.

Marktkonsortium fordert klare Aussage der EBA zu 3-D Secure 2.x

Des Weiteren monieren die Unterzeichner, dass die im EBA-Kommentar vom 21. Juni ausgeführte Auflistung von Authentifizierungsansätzen (Abbildung 1) die Auslegung zulässt, dass aktuelle Umsetzungen von 3-D Secure 2.x, welche sich eines biometrischen Authentifizierungsfaktors bedienen, nicht compliant seien, da keine Datenpunkte des biometrischen Faktors über das Protokoll ausgetauscht werden. Sofern die EBA bei dieser Auslegung bliebe, müsste eine weitere Iteration des 3-D Secure-Protokolls vorgesehen werden, was jedoch entsprechende Vorlaufzeiten für Entwicklung, Testing und Deployment nach sich ziehen würde – demnach keinesfalls bis zum 14. September bereitstehen könnte.

Weiterhin sind die Unterzeichner der Meinung, dass die bestehenden Umsetzungen von 3-D Secure 2.x mit biometrischen Faktoren die derzeit höchstmöglichen Sicherheitsniveaus realisieren und der entsprechenden Alternative (statisches Passwort / Sicherheitsfrage) überlegen seien. Sie fordern daher, dass die EBA eine differenziertere Positionierung ggü. biometrischen Faktoren publiziere und, mehr noch, die Industrie zur Adaption ebendieser anhalte.

Fazit

Die Reaktion auf den EBA-Kommentar ist wenig überraschend, wenngleich die Deutlichkeit der Kritikpunkte und Forderungen sowie der große und namhafte Kreis der Unterzeichnenden bemerkenswert und in dieser Tragweite bisher noch nicht dagewesen ist: Allein in der EPIF sind u.a. First Data, PayPal, Elavon, Amazon Payments, SIX Payment Services, Klarna und Worldpay vertreten, womit bereits ein Großteil des E-Commerce Acquiring-Marktes abgedeckt wird.

Das von den Unterzeichnern aufgebaute dystopische Chaos-Szenario ab dem 14. September wird mit der Stripe-Studie plausibilisiert, kann jedoch hinterfragt werden: In den Medien formiert sich die Gegenposition, dass die 18-monatige Umsetzungsfrist von den Betroffenen schlicht „verschlafen“ wurde oder dass die aktuell vorliegende Marktunsicherheit ein von den Betroffenen bewusst herbeigeführter Zustand zur Durchsetzung einer Verschiebung sein könnte.

Dabei fällt auf, dass bisher keine Verlautbarung der Issuing-Seite zu vernehmen war, d.h. keine Bank oder Bank-Vereinigung sich den Kritikern offiziell angeschlossen hat.

Eine Begründung hierfür könnte sein, dass die möglichen negativen Auswirkungen (Kaufabbrüche) die Banken nicht direkt, zumindest nicht so hart wie die Händler und Schemes betreffen. Aufgrund ihrer Fokussierung auf den domestischen Markt werden die Banken zudem die unterschiedlichen Auslegungen in den verschiedenen Ländern bei weitem nicht in dem Maße tangieren, wie die Acquirer und Händler. Weiterhin kann interpretiert werden, dass Banken die PSD2-Anforderungen – wobei die SCA-Anforderungen der RTS nur einen Teil ausmachen – bereits früher antizipiert haben und daher weniger Probleme durch die anstehende Umsetzung erwarten. Zu guter Letzt werden Banken aufgrund ihrer stärkeren Abhängigkeit von einem guten Verhältnis zu Regulatoren eine Mitautorschaft an zuspitzenden Briefen vermeiden. Als Bank sich als nicht betroffen zu begreifen, könnte jedoch ein Trugschluss sein, denn sofern die im Brief avisierten Entwicklungen tatsächlich eintreten, würden Banken kurzfristig durch sinkende Transaktionserlöse tangiert werden; wobei langfristig rücklaufende Kundenkontaktpunkte auch das Cross Selling-Potential des Zahlungsverkehrs (z.B. für Konsumentenkredite, Ratenkauf etc.) limitieren.

Für die EBA tritt nun folgendes Dilemma ein: Den Forderungen des Brandbriefes nachzukommen und eine einheitliche Verschiebung der Fälligkeit zu initiieren, könnte als zu große Nachsicht in der seit nunmehr 18 Monaten geführten Diskussion gegenüber den Marktvertretern interpretiert werden. Dies so kurzfristig vor der Fälligkeit zuzubilligen, provoziert zudem den Vorwurf, die EBA hätte die marktgerechte SCA-Ausgestaltung und -Umsetzung bis zuletzt nicht unter Kontrolle. Sofern aber die EBA zuließe, dass die nationalen Regulatoren untereinander einen einheitlichen Umsetzungsplan abstimmen, könnte die EBA zwar offiziell an ihrer bisherigen Frist festhalten, jedoch würde diese durch nationale Regulatoren unterwandert werden können.

Die Forderungen des Konsortiums abzulehnen, d.h. an der bestehenden Umsetzungsfrist und Auslegung der RTS festzuhalten, würde unter Verweis auf 18 Monate Umsetzungshorizont als konsequent gelten. Sollten die vom Konsortium avisierten Probleme im Markt tatsächlich eintreten, würde der EBA der wesentliche Teil der Verantwortung zugeordnet.

Die EBA steckt in einem Dilemma; welchen Weg sie einschlägt, bleibt abzuwarten. Die Unterzeichner des Briefes haben ihre Position klar formuliert, sollten sich jedoch in der Umsetzung der RTS-Anforderungen nicht durch die Diskussion aufhalten lassen – denn auch eine Verschiebung wird die inhärenten Herausforderungen nicht lösen. Eine Verzögerung würde längere Umsetzungszeiten nach sich ziehen, welche wiederum ebenso oft mit höheren Umsetzungskosten einhergehen. Stattdessen könnte eine kurzfristige Umsetzung auch als Chance zur Wettbewerbsdifferenzierung verstanden werden.

Dies gilt ebenso für Banken, wenngleich diese durch ihre Zurückhaltung in der Diskussion suggerieren, die Umsetzung ihrerseits rechtzeitig bis zum 14. September abschließen zu können. Sofern Banken eine einheitliche Verschiebung der Umsetzungsfrist ebenfalls befürworten, wäre aktuell die wohl letzte Gelegenheit, intervenierend in die Diskussion einzugreifen und eine weitere Perspektive einzubringen.

Quellen

1. Positionspapier der EBA zur Starken Kundenauthentifizierung unter PSD2

<https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf>

2. Finaler Report zum RTS Draft

<https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf>

3. Brief des Handelsverbands EuroCommerce an die EBA <https://www.bargeldlos-blog.de/4773-2/>

4. FCA Ankündigung des Migrationsplans

<https://www.fca.org.uk/news/statements/fca-response-european-banking-authority%E2%80%99s-opinion-strong-customer-authentication>

5. Joint Industry Statement on SCA Implementation

<https://www.bargeldlosblog.de/wp-content/uploads/Join-industry-Statement-on-SCA-Implementation.pdf>

6. Stripe Studie zu erwarteten Verlusten durch Kaufabbrüche

<https://stripe.com/reports/451-research-sca>



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 Bezahlösungen.

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 Bezahlssysteme 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 | UAE Emirates
<https://core.se/>
Phone: +97 14 323 0633