EBA-Kommentar zur PSD2-RTS

Auflösen von Unklarheiten wirft neue Fragen auf

Dominik Siebert
Dr. Waldemar Grudzien
Benedikt von Hake

Juli 2019
Blogpost

Key Facts

- EBA veröffentlicht abschließendes Positionspapier zur starken Kundenauthentifizierung (SCA) im Kontext der finalen RTS der PSD2
- Vielzahl der Rückfragen offenbaren Unsicherheit der Betroffenen zur Auslegung der RTS und Möglichkeit einer Übergangsfrist für die Umsetzung der SCA-Anforderungen bei Issuern und Merchants erstmals offiziell eingeräumt
- Verhaltensbasierte Biometriemerkmale zur Authentifizierung zugelassen bei Umsetzung erforderlicher Qualität – Modalitäten für Nachweis jedoch nicht konkretisiert
- Mögliche Interpretation: Biometrieeinsatz bei 3-D Secure 2.0 nach heutiger Umsetzung incompliant mit RTS
- Kurzfristige Klärung mit der EBA herbeizuführen; mittelfristig Entwicklung eines PSD2 complianten Industriestandards anzustreben

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 von der EBA ausgearbeiteten „Regulatory Technical Standards (RTS) zu starker Kundenauthentifizierung und sicherer Kommunikation im bargeldlosen Zahlungsverkehr“ spezifiziert sind.

Schon während des iterativen Prozesses der RTS-Entstehung gab es immer wieder Rückfragen und Anmerkungen von Marktteilnehmern, welche im Zuge des Abschlussreports zur finalen RTS vom Februar 2017 durch die EBA reflektiert wurden. Doch bis heute scheinen für die Betroffenen nicht alle Fragen abschließend geklärt zu sein; dies zeigt sich z.B. im Anfang Juni veröffentlichten Brief des Handelsverbands EuroCommerce an die EBA.

Als Reaktion auf diese Unklarheiten hat die EBA am 21. Juni 2019 – also nicht einmal 3 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).

Das Papier richtet sich primär an die national zuständigen Behörden (CAs), soll aber angesichts der damit verbundenen aufsichtsrechtlichen Erwartungen auch für Zahlungsdienstleister (PSPs), Zahlungssysteme und Zahlungsdienstnutzer (PSUs) einschließlich Händlern als Orientierung dienen.

Die EBA unterteilt ihre Kommentare in „generische“ und „spezifische“ Anmerkungen. Ein Großteil der Anmerkungen beantwortet entweder sehr spezielle an die EBA gerichtete Rückfragen, oder dient eher einer ergänzenden Konkretisierung einzelner Vorgaben, welche die allgemein im Markt wahrnehmbare Auslegung der RTS jedoch nicht tangieren.

Einige der EBA-Kommentare dürften jedoch die bisher vorherrschende Interpretation der Marktteilnehmer mindestens in Teilbereichen korrigieren und sollen daher nachfolgend kurz ausgeführt werden.

Unerwartete EBA Auslegungen und deren Bedeutung für den Markt

Absatz 13 und 14: EBA eröffnet Möglichkeit von Übergangsfristen

Während auch nach Veröffentlichung der finalen RTS einige inhaltliche Punkte marktseitig noch immer in Diskussion waren, war bisher recht unstrittig, dass ab dem 14. September 2019 alle betroffenen Marktteilnehmer die RTS mandatorisch umzusetzen haben, wobei eine Nicht-Erfüllung die Sanktionierung durch national zuständige Behörden (CAs) potenziell zur Folge hat. Laut Vorgaben der PSD2 waren dabei keine Spielräume für individuelle Beurteilungen vorgesehen.

In Absatz 12 und 14 des EBA-Papiers wird nun eingeräumt, dass die CAs in Ausnahmefällen „zur Vermeidung unbeabsichtigter negativer Folgen für Zahlungsdienstenutzer“ entscheiden können, limitiert zusätzliche Zeit zur Umsetzung der SCA Anforderungen einzuräumen. Diese Flexibilität der Aufsichtsbehörden verlangt jedoch explizit, dass die betroffenen PSPs[1] einen Migrationsplan erstellen, diesen mit den CAs abgestimmt haben und nach den Vorgaben der CAs umsetzen. Die CAs wiederum sind angehalten, die Umsetzung dieser Pläne zu überwachen, um eine rasche Einhaltung der technischen Standards der PSD2 und der EBA zu gewährleisten. Darunter fiele auch, dass eine adäquate Kommunikation ggü. den PSUs vorliegen muss.

Gleichwohl merkt die EBA in Absatz 15 an, dass sie die adäquate Nutzung dieser Spielräume beobachten und wenn nötig bei Nichteinhaltung aktiv werden wird.

Zusammenfassend kann diese EBA Ausführung jedoch ambivalent gewertet werden: Das Statement selbst kann als mögliche Entlastung für PSPs gewertet werden, welche die initial forcierte Timeline zur RTS-Umsetzung aller Wahrscheinlichkeit nach nicht einhalten können, respektive gibt sie den Aufsichtsbehörden die Möglichkeit, situativ über das weitere Vorgehen zu entscheiden. Da die EBA jedoch explizit auf „zahlreiche Rückfragen“ in diesem Kontext verweist, wäre eine mögliche Interpretation, dass dies wohl auf mehr PSPs zutrifft als derzeit im Markt kommuniziert. Dass der europäische Handelsverband EuroCommerce noch Anfang Juni per Brandbrief EBA Excecutive Director Adam Farkas warnte, dass der Handel mit der Umsetzung der SCA-Anforderungen noch nicht weit genug vorangeschritten sei und fatale Folgen für Handel- und Verbrauchervertrauen zu Befürchten seien, passt ins Bild. Explizit fordert der Verband eben jene nun gewährte Übergangszeit für die Umsetzung der Anforderungen. Inwieweit die neuen Spielräume dann tatsächlich ausgeschöpft werden, bleibt abzuwarten.

Absatz 18 – 20: Nutzung von Inhärenz-Authentifizierungsfaktoren

Laut Artikel 4 (30) der PSD2 bedingt starke Kundenauthentifizierung (SCA) mindestens zwei Elemente aus den drei Kategorien: Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das der Nutzer ist), die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt.

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

In Absatz 18 – 20 des Positionspapiers konkretisiert die EBA nun die Anwendbarkeit von Inhärenz-Authentifizierungsfaktoren: Zum einen konstatiert die EBA, dass neben physiologischen auch verhaltensbasierte Biometriemerkmale wie die Anschlagdynamik auf der Tastatur als Authentifizierungsfaktor genutzt werden kann, was vielen bisher vorherrschenden Auslegungen der RTS widerspricht. Weiterhin wird jedoch unter Verweis auf Artikel 8 der RTS relativiert, dass nicht der Faktor an sich, sondern die (Qualität der) Umsetzung die Anwendbarkeit für die starke Kundenauthentifizierung determiniert, d.h. aus Perspektive der EBA ist prinzipiell kein biometrisches Merkmal per se ausgeschlossen, solange die Implementierung eine „*sehr geringe Wahrscheinlichkeit, dass eine unbefugte Partei als Zahler authentifiziert wird*" sicherstellt. Inwieweit eine solche Qualität jedoch validiert werden kann und muss, wird nicht näher konkretisiert. Somit eröffnen die Ausführungen der EBA eine Folgediskussion, da bspw. im Gegensatz zu PIN Pads für Biometrische Authentifizierungssysteme im Finanzsektor keine geregelten Zulassungsverfahren bestehen. Gleichwohl sind die Einlassungen der EBA zu begrüßen, eröffnen sie doch der Biometrie das große Feld der Fachaufsicht, das sie benötigt, um Marktstandards zu erzwingen und die Biometrie auch für Transaktionen zu etablieren. Diese Marktstandards sollte die betroffene Industrie erarbeiten und einer schnellen Akkreditierung in Kooperation mit der EBA zuführen.

Die Einordnung der EBA zur Nutzbarkeit von Inhärenz-Faktoren kann als technisch liberal und wettbewerbsfördernd interpretiert werden, nicht zuletzt, da die EBA selbst in Absatz 18 anmerkt, dass Biometrie in Hinblick auf das technische Potenzial zur sicheren Kundenauthentifizierung das „*innovativste*" und „*dynamischste*" Marktumfeld aufweist. Da die meisten Issuer bisher, bedingt durch die Breite der RTS-Anforderungen, lediglich auf eine minimal invasive Umsetzung fokussiert haben, dürften jedoch innovative Lösungen, welche diese Potenziale ausschöpfen, erst mittelfristig im Masseneinsatz zu finden sein.

Absatz 21 – 23: Inhärenz bei 3-D Secure 2.0

Getrieben durch Visa, Mastercard und weitere Kreditkartenanbieter avanciert im kartenbasierten Zahlungsverkehr im Distanzgeschäft die Karteninhaber-Authentifikation via 3-D Secure 2.0 zunehmend zum Marktstandard. In der aktuell vorherrschenden Marktwahrnehmung, deckt das Verfahren die SCA-Anforderungen der PSD2 vollumfänglich ab (https://core.se/de/techmonitor/sicherheit-im-kartenbasierten-zahlungsverkehr). Die EMVCo als Urheber des 3-D Secure Protokolls betont , dass die neue Version insbesondere die Integration von Biometrieverfahren zur Karteninhaberauthentifizierung vereinfachen solle.

Nicht vollständige Liste möglicher Inhärenz Elemente

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 Bewegungs-Pattern, 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 zur Zeit im Markt zu beobachten sind)
Eingeprägter Swiping Path	Nein

Abbildung 1: Übersicht möglicher Inhärenz Elemente gem. EBA Positionspapier

Entsprechend überraschend erscheint daher die Einordnung der EBA, dass zumindest die bisher im Markt ersichtlichen Umsetzungen zur Nutzung von Biometrie im Kontext 3-D Secure nicht den formulierten Ansprüchen eines Inhärenz-Faktors gerecht werden. Begründet wird dies damit, dass die für die biometrische Authentifizierung verwendeten Datenpunkte selbst (bspw. Fingerabruck) nicht Teil des Protokolls sind, wobei auf Artikel 8 der RTS verweisen wird. Dieser besagt, dass für die Nutzung eines Inhärenz-Authentifizierungsfaktors sichergestellt sein muss, dass das jeweilige Endgerät und die dazugehörige Software auch bei Zugriff auf ebendiese resistent gegen eine unauthorisierte Verwendung dieses Inhärenz-Faktors für die Authentifizierung sein müssen. Dies referenziert indirekt auf die in Fachkreisen seit längerer Zeit diskutierte Notwendigkeit der „Template-Protection“ (vgl. https://core.se/publications/blog-posts/default-title-1), eine weitere Ausführung dieses Punktes durch die EBA erfolgt jedoch nicht im Positionspapier.

Naheliegend ist jedoch, dass die EBA Artikel 8 der RTS potenziell verletzt sehen könnte, da bei den etablierten Biometriefunktionen von Smartphones und Tablets (TouchID, FaceID etc.) bei Zugriff auf den jeweiligen Device PIN der biometrische Faktor übersteuert, bzw. neu initialisiert werden kann.

Aktuell avancieren jedoch gerade diese Varianten zur Best Practice für die Umsetzung von 3-D Secure 2.0: Der Nutzer erhält im Transaktionsablauf eine Push-Notification auf eine zuvor an das Device gebundene App (Besitz-Faktor), öffnet diese via TouchID/FaceID (vermeintlicher Inhärenz-Faktor) und muss in der App selbst nur noch die Transaktion freigeben. Da letztgenannter Authentifizierungsfaktor gem. EBA-Kommentar nicht als solcher statthaft ist, müsste bspw. noch ein statisches Passwort (Wissens-Faktor) hinzugefügt werden, um die Mindestanforderungen an eine SCA einzuhalten.

Sollte diese Auslegung des EBA-Kommentars tatsächlich der regulatorischen Perspektive entsprechen, dürfte dies bei den Card Schemes wie Mastercard und Visa, 3-D Secure Providern und Karten-Issuern eine Neubewertung der Situation erfordern. Mehr noch wären auch diverse weitere Banken und Zahlungsverkehrsteilnehmer betroffen, da viele Umsetzungen von 2-Faktor-Authentifizierung (bspw. für den E-Banking Zugang) nach einem ähnlichen Schema aufgebaut sind.

Fazit

Die Ausführungen der EBA lassen in verschiedenen Dimensionen Schlüsse zur aktuellen Marktsituation und zukünftigen Entwicklung zu:

Zum einen machen die Tatsachen, dass es zahlreiche Rückfragen gab, Banken- und Handelsvertreter wiederholt um mehr Zeit bei der Umsetzung der Verpflichtungen gebeten haben, sowie dass die EBA nicht einmal 3 Monate vor Inkraftreten der RTS eine Interpretationshilfe veröffentlicht, deutlich, dass einige Verpflichtete der RTS an vielen Stellen noch nicht die notwendige Expertise aufgebaut haben, um die verlangten Anforderungen adäquat umzusetzen. Dass diese Rückfragen erst mehr als zwei Jahre nach Veröffentlichung der finalen RTS formuliert werden, suggeriert, dass der Markt die Herausforderungen aus der PSD2 partiell zu spät adressiert hat. Mehr noch scheint, dass das wettbewerbsdifferenzierende Potenzial der SCA-Umsetzungen bislang noch nicht vollumfänglich vom Markt antizipiert wird (vgl. https://core.se/de/techmonitor/sicherheit-im-kartenbasierten-zahlungsverkehr). Umso mehr sollten Issuer und PSPs nun angehalten sein, der Thematik SCA die notwendige Aufmerksamkeit zu widmen und nicht nur nach Minimalvorgaben des Regulators, sondern proaktiv und marktgestaltend konveniente Lösungen zu etablieren – z.B. durch den nun explizit von der EBA avisierten Einsatz von Biometrie.

Insbesondere die EBA-Einstufung zur Inhärenz bei 3-D Secure 2.0 lässt jedoch noch immer verschiedene Interpretationen zu und könnte somit noch zu einigen Spannungen im Markt führen. Trotz - oder gerade wegen – der teilweise nicht eindeutig interpretierbaren Ausführungen der EBA wird eine Diskussion zum Thema Biometrieeinsatz im Banking eröffnet, was grundsätzlich positiv zu bewerten ist und möglicherweise von der EBA sogar intendiert war.

Zwar bekräftigt die EBA in Absatz 11, über den bestehende Q&A-Prozess hinaus, keine weiteren Ausführungen dieser Art vor Inkrafttreten der RTS veröffentlichen zu wollen, doch insbesondere aufgrund der zeitnahen Wirksamkeit der RTS gilt es nun für alle Betroffenen, die Diskussion anzunehmen und kurzfristige Klarheit von der EBA einzufordern. Insbesondere im dynamischen Umfeld der Biometrie scheint mittelfristig notwendig, allgemeine Marktstandards und entsprechende Zulassungs- bzw. Prüfverfahren für biometrische Authentifizierungslösungen zu etablieren, um klare Rahmenbedingungen zu schaffen und so den großflächigen Einsatz und damit die Nutzung des Sicherheitspotenzials dieser Technologien zu ermöglichen.

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.bargeldlosblog.de/4773-2/
4. **Abbildung 1: Übersicht möglicher Inhärenz Elemente gem. EBA Positionspapier**
   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

Dr. Waldemar Grudzien setzt sich als Expert Director mit den aktuellen regulatorischen Anforderungen und deren technischer Realisierung auseinander. Als promovierter Elektrotechniker war er als Leiter in einem nationalen Bankenverband für die Bereiche Retailbanking und Banktechnologien zuständig.

Mail: waldemar.grudzien@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