

# Die EBA hat die **Chance** zur offenen Regulierung **verpasst**

Von Ulrich Binneböbel



Mit dem überarbeiteten Entwurf der RTS zur Umsetzung der PSD2 hat die europäische Bankenaufsicht zwar die ungewöhnlich heftige Kritik im Rahmen der Konsultation aufgegriffen. Doch die im neuen Entwurf eingearbeiteten Änderungen greifen immer noch zu kurz, so Ulrich Binneböbel. So bremsen auch die höheren Betragsobergrenzen für den Verzicht auf Zwei-Faktor-Authentifizierung die weitere Entwicklung zu „Seamless Payments“, Whitelists und Ausnahmeregelungen im Automatenbereich schaffen ungleiche Wettbewerbsbedingungen. Das Kernproblem liegt allerdings an anderer Stelle, so der Autor: Mit dem Vorschreiben einer Technologie wurde die Chance zu einer offenen Regulierung verpasst. Red.

Bereits in der Vorbereitung zur Erstellung der zweiten Zahlungsdiensterichtlinie hatte der HDE darauf hingewiesen, dass mit der Festschreibung einer technischen Vorgabe die Chance einer offenen Regulierung verpasst werde. Anstelle der generellen Definition eines Schutzziels, wie zum Beispiel Verbraucher vor Verlust durch Missbrauch zu schützen, wurde ein Prozess definiert, der die

Möglichkeiten der Beteiligten weitgehend einengt.

Nachdem dieser Einwurf nicht beachtet und die Richtlinie verabschiedet wurde, drängte der HDE in der Umsetzung durch technische Standards darauf, entsprechende Ausnahmereiche zu definieren, die sicherstellen, dass „Alltagszahlungen“ nicht durch überhöhte Anforderungen an die Authentifizierung zu komplex und damit unattraktiv werden und schließlich zu Ausweichreaktionen der Kunden führen können.

## Anspruch einer technologieoffenen Regulierung nicht erfüllt

Diese Befürchtung hat sich mit der Vorlage des Entwurfes durch die europäische Bankenaufsicht EBA inzwischen bestätigt. Denn die EBA hat die möglichen Spielräume der Richtlinie zur Gestaltung von Ausnahmereichen nicht genutzt und nun regulatorische technische Standards (RTS) vorgelegt, die dem Anspruch einer technologieoffenen Regulierung nicht entspricht.

### Zum Autor

**Ulrich Binneböbel**, Referat Zahlungsverkehr, Handelsverband Deutschland e.V. (HDE), Berlin

Nachdem ein erster Entwurf der sogenannten Regulatory Technical Standards (RTS) im Konsultationsverfahren zu ungewöhnlich vielen und kritischen Äußerungen aus der Wirtschaft geführt hatte, wurde nun ein finaler Entwurf veröffentlicht und der Kommission zugeleitet, der sich fundamental vom ersten Entwurf unterscheidet. Den Verbänden sollte aufgrund der Änderungen allerdings erneut Gelegenheit zur Kommentierung gegeben werden, was leider bislang nicht geschah.

In dem jetzt übermittelten Entwurf\* sind zwar tatsächlich einige Änderungen enthalten. Aber reicht das und ergeben sich nicht neue Fragen?

## 30-Euro-Obergrenze greift zu kurz

Entscheidende und selbstbewusst von der EBA nach außen getragene Änderung ist die Erweiterung der Betragsgrenze auf 30 Euro für den Verzicht auf eine Zwei-Faktor-Authentifizierung für bestimmte Online-Zahlungen. Diese Grenze lag bislang bei nur zehn Euro. Diese Erweiterung ist zwar willkommen, ob sie aber künftigen Anforderungen gerecht wird, muss hinterfragt werden.

Künftige Weiterentwicklungen der Zahlungssysteme in Richtung eines Seamless Payments am Point of Sale, also der Bezahlung im Hintergrund eines Ein-

kaufsprozesses – werden sicher gebremst. Immerhin: Kontaktlose Zahlungen im stationären Handel – das sogenannte Tap & Go – sind weiterhin bis zu 50 Euro auch ohne PIN-Eingabe möglich, maximal jedoch 150 Euro kumuliert.

### Risikoanalyse mit Umsetzungsproblemen in der Praxis

Die RTS sehen weiter vor, dass bei Betragsgrößen bis 500 Euro künftig eine Risikoanalyse die Zwei-Faktor-Authentifizierung ersetzen kann. Die Regulierung liefert die Risikofaktoren für bestimmte Betragsklassen mit und setzt enge Grenzen, die hinterfragt werden dürfen. So darf die Betragsrate bei Online-Zahlungen für Beträge bis 100 Euro maximal 0,13 Prozent betragen, damit auf die Zwei-Faktor-Authentifizierung verzichtet werden kann; bis 250 Euro sind es 0,06 Prozent, bis 500 Euro 0,01 Prozent. Für Überweisungen gelten ähnliche Grenzen. Hierbei stellen sich zwei Fragen:

- Auf welcher Basis wurden diese Betragsobergrenzen festgelegt?
- Und wie kann eine Umsetzung in der Praxis erfolgen?

Letztlich gilt es, die Vorgaben transparent zu machen. Kunde und Akzeptant müssen wissen, was auf sie zukommt, wann eine

PIN-Eingabe erfolgen muss und wann nicht. Ein Rätselraten über die PIN- oder TAN-Eingabe dient nicht gerade dazu, einen reibungslosen Einkauf zu organisieren.

### Willkürliche Ausnahmeregelungen bei unbedienten Terminals auflösen

Interessant in diesem Zusammenhang ist die Ausnahme für Park- und Ticketautomaten. Die RTS sehen vor, dass bei Park- und Ticketautomaten eine starke Authentifizierung nicht erforderlich ist. Hier kann also auch künftig betragsunabhängig auf die PIN-Eingabe verzichtet werden. Diese Freigabe erscheint recht willkürlich. Welcher Anlass führte zur Ausnahme für derartige Geräte? Warum sind zum Beispiel Verkaufsautomaten nicht ebenfalls ausgenommen? Können weitere „unattended terminals“ nicht auch freigestellt werden?

Es sollte mindestens eine Freigabe für alle unbedienten Terminals gelten, also auch zum Beispiel für Verkaufsautomaten oder Self-Checkout-Kassen. Zumindest aber sollte eine stichhaltige Begründung erfolgen, warum nur die Park- und Ticketautomaten von der 30-Euro-Obergrenze für Transaktionen ohne Zwei-Faktor-Authentifizierung ausgenommen werden.

### Whitelists schaffen ungleiche Wettbewerbsbedingungen

Ein zweischneidiges Schwert ist auch die Ausgestaltung der sogenannten Whitelists. Sie sollen dafür sorgen, dass Verbraucher vertrauenswürdige Zahlungsempfänger angeben können, bei denen sie auf eine starke Authentifizierung verzichten wollen.

Allerdings ergibt sich hier eine Benachteiligung kleinerer Händler. Denn grundsätzlich wird wohl kein Verbraucher einen Händler auf eine Whitelist bringen, bei dem er nur einmalig etwas kauft. Große Marktplätze oder regelmäßige Einkaufsstellen werden dagegen eher auf eine Aus-

nahmeliste gesetzt, um einfach bezahlen zu können. Die Regelung sorgt also tendenziell für einen weiteren Konzentrationsprozess hin zu großen Händlern.

Weiterhin können nach der Neuformulierung die kontoführenden Institute eine „vordefinierte“ Liste mit vertrauenswürdigen Zahlungsempfängern anbieten, die der Kontoinhaber auf einfachen Wege akzeptieren und für sich nutzen kann. Auch hier ergeben sich Fragen, die an dem ursprünglichen Ziel der PSD2 gemessen werden sollten.

- Wer entscheidet über die Vertrauenswürdigkeit? Durch vorausgefüllte Listen ist es am Ende wohl nicht mehr der Kontoinhaber. Sondern er überlässt die Entscheidung in aller Regel seiner Bank. Diese erhält damit tendenziell eine Entscheidungsgewalt über die Händler beziehungsweise Zahlungsempfänger, die einen erleichterten Zugang zum Kunden haben.
- Weiterhin stellt sich die Frage: Können Zahlungsplattformen ihren Kunden eine Liste anbieten, die grundsätzlich alle beteiligten Plattformhändler freistellt?
- In diesem Kontext muss auch geklärt werden, wie Händler sich für den Eintrag in eine solche Liste empfehlen können. Setzt die Bank Kriterien fest oder lässt sie sich den Eintrag etwa bezahlen?

Ergänzend sei festgestellt, dass die RTS weitere Punkte regeln, über die andere Parteien eine Meinung finden müssen. Zuvorderst betreffen sie die dritten Dienstleister, jene neu geschaffenen Institutionen also, die künftig für Wettbewerb bei Zahlungsbeziehungsweise Kontoprozessen sorgen sollen. Ihnen muss ein akzeptabler und nachhaltiger Zugang zum Konto geschaffen werden.

So ist beispielsweise der Zugriff auf Kontoprozesse für Zahlungsinformationsdienstleister nur viermal täglich möglich und muss für alle Dritten Dienstleister über

### Bleiben Sie immer auf dem neuesten Stand:

Ihre Kreditwesen-Redaktion informiert nun auch täglich in der Rubrik „Meldungen“.

Folgen Sie uns auf



oder besuchen Sie uns unter

[www.kreditwesen.de](http://www.kreditwesen.de)

eine dedizierte Schnittstelle erfolgen. Welche Auswirkungen diese Einschränkungen haben, kann aus Handelssicht nicht eingeschätzt werden.

Vorläufiges Fazit: Das ursprüngliche Ziel der PSD2 war es, Verbraucher besser zu schützen. Dabei wurde leider in der endgültigen Fassung bereits die Art und Weise eingeschränkt, wie dieses Ziel zu erreichen ist. Durch den Einsatz von Technologie in Form der starken Authentifizierung soll sichergestellt werden, dass Transaktionen stets nur mit dem Willen des Kontoinhabers ausgelöst werden.

### **Regulierung setzt der Ausgestaltung einen Riegel vor**

Das Ziel, den Verbraucher vor Verlust zu schützen ist aber auch auf andere Weise möglich als Technologien vorzuschreiben, die selbst in Gefahr stehen, über kurz oder lang geknackt werden zu können. Eine Garantie beispielsweise, Verluste bedingungslos ersetzt zu bekommen, oder die Möglichkeit, den Beteiligten die Wahl der Mittel zu überlassen, wurde nicht berücksichtigt. Statt im Sinne einer solchen offenen Regulierung ein Schutzziel zu definieren, wie etwa Verbraucher vor Verlust durch Missbrauch zu schützen, wurde ein Prozess definiert, der die Möglichkeiten der Beteiligten weitgehend einengt.

Jetzt ist es wohl zu spät, um noch einen anderen Weg einzuschlagen. Schließlich sind politische Prozesse oft unumkehrbar. Künftig liegt es damit nicht mehr in den Händen des Zahlungsempfängers, seines Dienstleisters oder des Dienstleisters des Kunden, den Weg der Bezahlung für den Verbraucher möglichst einfach zu gestalten. Allzu häufig setzt die Regulierung der Ausgestaltung einen Riegel vor und wird künftig für komplexere Abläufe sorgen. Die Verantwortung hierfür liegt beim Gesetzgeber.

#### **Quelle:**

\* <https://www.eba.europa.eu/-/eba-paves-the-way-for-open-and-secure-electronic-payments-for-consumers-under-the-psd2>