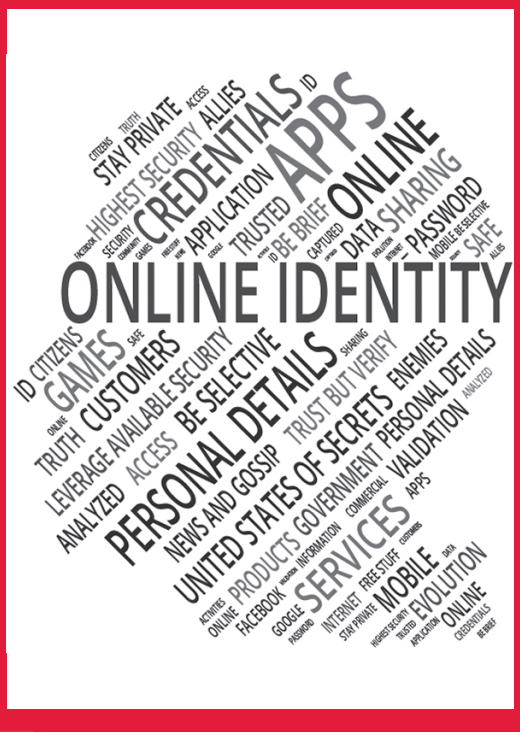
PSD2 und die Zukunft der Kundenauthentifizierung



Von Mirko Hüllemann

Die PSD2 und die technischen Regulierungsstandards der EBA bieten für alle Beteiligten vor allem Chancen, meint Mirko Hüllemann. Banken können von der Schnittstellenöffnung für Drittanbieter profitieren, indem sie neue, komfortable Services für ihre Kunden ermöglichen. Selbst der starken Kundenauthentifizierung kann der Autor Positives abgewinnen: Sie werde nicht nur die Sicherheit erhöhen, sondern die Verfahren zugleich für den Kunden komfortabler machen. Red.

Die erste Zahlungsdienste-Richtlinie der EU stammte aus dem Jahr 2007: die PSD 2007/64/EC. Ein wichtiger Grund für die zweite, grundlegend überarbeitete Payment Services Directive war es, dass die EU mit der Richtlinie nun auch die onlinebasierten Zahlungsdienste abdecken wollte. Die neue PSD2, die Richtlinie (EU) 2015/2366, hat die Europäische Kommission im Oktober 2015 beschlossen. Sie soll im Januar 2018 in Kraft treten. Bis dahin müssen die Mitgliedsstaaten die verbindlichen Anforderungen der PSD2 in nationales Recht umsetzen.

Auch wenn die regulatorisch-technischen Spezifikationen (RTS), die die European Banking Authority (EBA) Anfang 2017 in ihrer endgültigen Ausarbeitung liefern will, noch viel Freiraum bei der Umsetzung zu lassen scheinen, hat die Zahlungsdiensterichtlinie in ihrer zweiten Auflage doch unabweisbare Konsequenzen für den Bereich der Kundenauthentifizierung bei Zahlungen im Online-Handel. Im Idealfall steigen für den Endkunden der Komfort und die Sicherheit, während sich Anbietern und Dienstleistern die Chance eröffnet, sich durch neue Services Wettbewerbsvorteile zu verschaffen.

Vier konkrete Ziele von PSD2

Das generelle Ziel von PSD2 ist es, elektronische Zahlungen in Europa für die Verbraucher sicherer und bequemer zu machen. Aus Sicht der EU-Kommission bedeutet die Direktive auch einen Schritt hin zu einem digitalen Binnenmarkt, der Verbrauchern und Unternehmen zugutekommen und zum Wirtschaftswachstum beitragen soll.

Die EU-Kommission hebt vier Änderungen hervor, die sich durch PSD2 ergeben:

- Es wird strengere Sicherheitsanforderungen für die Auslösung und Verarbeitung elektronischer Zahlungen und den Schutz der Finanzdaten der Verbraucher geben.

- Der EU-Zahlungsverkehrsmarkt wird für sogenannte Zahlungsauslösedienstleister und Kontoinformationsdienstleister geöffnet.

- Die Verbraucherrechte werden in verschiedenen Bereichen gestärkt, etwa durch die Verringerung der Haftung für nicht autorisierte Zahlungsvorgänge und die Einführung eines bedingungslosen Erstattungsrechts bei Lastschriften in Euro.

- Die Berechnung von Aufschlägen (etwa für das Recht, mit einer Karte zu zahlen) wird untersagt – unabhängig davon, ob Verbraucher das jeweilige Zahlungsinstrument in einem Geschäft oder online nutzen.

Drittanbieter und die Bankenwelt

Einer der interessantesten Aspekte der neuen Richtlinie ist aus Sicht eines Payment Service Providers (PSP) die Öffnung der bislang für Drittanbieter verschlossenen Bankenwelt. Aber nicht nur die Zahlungsdienstleiter profitieren von solch einer Öffnung, auch die Banken selbst können sich mit neuen, komfortablen Services für ihre Kunden neu positionieren.

Zum Autor

Mirko Hüllemann, Geschäftsführer, Heidelberger Payment GmbH, Heidelberg

Gemäß Artikel 98 PSD2 obliegt es der Europäischen Bankenaufsichtsbehörde (EBA) in enger Zusammenarbeit mit der Europäischen Zentralbank (EZB), sogenannte technische Regulierungsstandards für die Authentifizierung und die Kommunikation zu definieren. Die EBA will diese Regulatory Technical Standards (RTS) an die EU-Kommission übermitteln, die sie dann als verbindlich erlassen kann.

Technische Regulierungsstandards der EBA

Wie die Kommunikationsschnittstelle im Detail beschaffen sein soll, regelt auch der vorliegende Final Draft der RTS der EBA zwar nicht – denn die Richtlinie selbst verlangt technische Neutralität gegenüber möglichen Internet-Kommunikationsstandards. Einige formale Anforderungen sind dennoch beschrieben, etwa der Einsatz einer geeigneten Verschlüsselung beim Datenaustausch, möglichst kurze Kommunikationsvorgänge und eindeutige Referenzen für die ausgetauschten Daten.

Auch den dritten Zahlungsdienstleistern, die nun erstmals auf Konto- beziehungsweise Kundendaten der Bank zugreifen dürfen, obliegen dabei besondere Pflichten. So müssen sie die Integrität und Vertraulichkeit der persönlichen Sicherheitsmerkmale und Authentifizierungscodes der Kunden gewährleisten, etwa indem sie sie ausschließlich in einer sicheren Umgebung gemäß ISO 27001 Standard für Informationsmanagement-Sicherheitssysteme verarbeiten.

Mehr Komfort und neue Services

Für Zahlungsdienstleister eröffnet diese begrenzte, aber direkte Kommunikation mit der Bankenwelt die Möglichkeit, Verbrauchern bei Kundenauthentifizierungsvorgängen im Online-Handel andere Services bieten zu können als bisher. Ein mögliches Beispiel: Wenn sich der Kunde im Online-Bezahlvorgang etwa mit seiner Girocard und per Chip-TAN authentifizieren möchte, kann ein Zahlungsinstitut diese Authentifizierung in Zukunft sofort prüfen. So werden auch ganz neue Instant-Payments-Optionen möglich.

Von einem derart engen Zusammenspiel von PSPs und Finanzinstituten profitieren am Ende alle Beteiligten: der Online-Händler, sein Kunde, das Zahlungsinstitut und die Bank. Denn eine Bank, die gute, sichere Schnittstellen für Dritte Zahlungsdienstleister schafft – etwa in Gestalt einer Anwendungsprogrammierschnittstelle (API) –, positioniert sich damit näher am Bedarf des Kunden. Sie schafft die Voraussetzungen dafür, dass für ihren Kunden die Zahlung im Internet einfacher und komfortabler wird.

Neue Authentifizierungsverfahren: sicher und komfortabel

Der andere hochinteressante Aspekt der PSD2 sind ihre Auswirkungen auf die Kundenauthentifizierung. Bei gewissen Zahlungsverfahren werden durch die überarbeitete Direktive neue Kundenauthentifizierungsmethoden notwendig. So könnte etwa beim Mobile Payment eine SMS-TAN auf das Smartphone nicht mehr zulässig sein.

In Artikel 97 schreibt die PSD2 zwingend eine sogenannte starke Kundenauthentifizierung vor, wenn der Zahlende beispielsweise online auf sein Zahlungskonto zugreift oder einen elektronischen Zahlungsvorgang auslöst.

Stark wird die Authentifizierung, wenn dabei wenigstens zwei von drei möglichen Kategorien herangezogen werden. Diese drei Authentifizierungskategorien sind:

- Wissen: etwas, das nur der Nutzer weiß (etwa ein Passwort).
- Besitz: etwas, das nur der Nutzer besitzt (etwa eine Chip-Karte).
- Inhärenz: etwas, das dem Nutzer persönlich beziehungsweise körperlich zu eigen ist (etwa ein Fingerabdruck).

Die Forderung der PSD2 nach einer starken Kundenauthentifizierung ist dann erfüllt, wenn das Authentifizierungsverfahren zwei dieser drei voneinander unabhängigen Elemente kombiniert.

Umständliches 3-D-Secure

Schon die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) legte in ihren „Mindestanforderungen an die Sicherheit von Internetzahlungen" (MaSI), die sie im November 2015 veröffentlichte, einen Schwerpunkt auf eine starke Authentifizierung.

Auch die einschlägigen Verfahren der Kreditkartenfirmen – wie der 3-D-Secure-Code bei Visa oder der Secure Code bei Mastercard – sollen das Sicherheitsniveau erhöhen. Wobei manche Institute diese Verfahren noch um Elemente wie Push-TANs, Smartphone-Apps oder Kartenlesegeräte ergänzen, um die Sicherheit bei der Kartenzahlung im Internet weiter zu erhöhen.

Verfahren wie das bisherige 3-D-Secure haben allerdings einen gravierenden Nachteil: Für den Kunden sind sie vergleichsweise umständlich anzuwenden. Entsprechend ungern bieten Online-Händler sie an. Denn fast immer ziehen diese Verfahren deutlich niedrigere Konversionsraten nach sich – die Gefahr von Abbrüchen steigt.

Selbst die starke Authentifizierung wird komfortabel

Der Nachteil für einen Händler, der sich solch einem starken Kundenauthentifizierungsverfahren verweigert, ist allerdings schon jetzt, dass er dann selbst das komplette finanzielle Risiko etwaiger Chargebacks trägt. In Zukunft wird in Europa durch die PSD2 eine Online-Kartenzah-

lung ohne starke Authentifizierung ganz unmöglich werden.

Insgesamt sollte durch PSD2 und die zwingend vorgeschriebene starke Kundenauthentifizierung das Sicherheitsniveau steigen. Der Betrug mit gestohlenen Daten wird in Zukunft schwieriger, wenn neue Verfahren sich der Kategorien Wissen, Besitz und Inhärenz bedienen, um eine starke Zwei-Faktoren-Authentifizierung zu realisieren. Vorstellbar sind etwa schnelle Methoden wie ein Iris-Scan oder eine Videoauthentifizierung einfach per Smartphone des Kunden. Den Kombinationsmöglichkeiten setzt die PSD2 keine Grenzen.

Es ist ebenso die Hoffnung der Zahlungsdienstleister wie der Händler, dass sich durch neue Verfahren die Zahl der Betrugsversuche und anschließender Rückbuchungen minimieren wird. Und aus Kundensicht sollte durch die neuen Verfahren der Komfort gegenüber tendenziell umständlichen Verfahren wie 3-D-Secure deutlich steigen.

Wer setzt PSD2 um?

Bleibt die Frage, wer die Umsetzung von PSD2 vorantreiben wird und in wessen Verantwortung sie letztlich liegt. Sicherlich sind durch die Direktive die Banken aufgerufen, entsprechend sichere und verfügbare Kommunikationsschnittstellen zu schaffen, aber auch viele Dritte Zahlungsanbieter werden in ihre Infrastruktur zu investieren haben, um auch auf ihrer Seite das geforderte Sicherheitsniveau zu realisieren.

Der aktuelle RTS-Entwurf sieht darum vor, dass zur Schnittstelle eine Testfunktion anzubieten ist, damit Drittanbieter das Zusammenspiel mit ihren eigenen Applikationen erproben können. Nur schweigen sich die regulatorisch-technischen Spezifikationen der EBA zu den Details der technischen Ausgestaltung weitgehend aus.

Und selbst wenn die EU-Kommission den RTS-Draft noch im Frühjahr 2017 annehmen sollte, wird er der PSD2-Richtlinie entsprechend erst 18 Monate später anwendbar. Da der RTS zur PSD2 allerdings als sogenannte Verordnung der EU erlassen werden soll, wäre er in sämtlichen Mitgliedsstaaten dann unmittelbar anzuwenden, ohne eine weitere nationale Umsetzung.

Nicht nur aus Sicht der Zahlungsdienstleister eröffnet PSD2 neue Chancen. Das Versprechen der neuen europäischen Richtlinie ist eine starke Kundenauthentifizierung, die die Sicherheit vor Betrug erhöht und E-Commerce-Transaktionen vereinfacht. Marktteilnehmer werden neue Verfahren der starken Authentifizierung dazu nutzen können, dem Endkunden Zahlungsoptionen beim Online-Kauf zu bieten, die ebenso sicher wie komfortabel sind.

Allen Beteiligten können dadurch Wettbewerbsvorteile entstehen. Es ist also an der Zeit, sich mit PSD2 auseinanderzusetzen, sich den neuen Anforderungen anzupassen und die Chancen zu nutzen, die sich jetzt eröffnen.