EFP White Paper

Hintergrund

Noch gut fünf Monate und dann ist es soweit: die Payment Service Directive 2.0 geht live. Seit dem Inkrafttreten der ersten Zahlungsdiensterichtlinie 2008/64/EG in 2009 und der auf EU Ebene bereits im November 2015 verabschiedeten Novellierung unter 2015/2366, sind die Erwartungen aller Beteiligten groß. Neue Zahlungsdienste werden eingeführt, Authentifizierungsverfahren definiert und Öffnung von Schnittstellen kontrovers diskutiert - zum Wohle und der Sicherheit des Nutzers. Die vorhandene IT- und Prozesslandschaft sortiert sich neu und mittendrin die Banken, deren herkömmliches Modell ins Wanken gerät.

Eine Momentaufnahme.

Autoren
Christian Bley, Rolf Mathes

Stand
15.08.2017

PSD II – ein Update

Nach der Verabschiedung der Payment Service Directive II (PSD II) am 25. November 2015 im EU Parlament und der Ablösung der ersten Zahlungsdiensterichtlinie vom 13. November 2007 läuft nun unaufhaltsam die zweijährige Umsetzungsfrist. Bis zum 13. Januar 2018 gilt es, die Anforderungen der zweiten Zahlungsdiensterichtlinie umzusetzen.

Im Antritt, Innovation und Wettbewerb zu fördern, hat die EU Kommission neben der Schaffung und Vereinheitlichung eines vollharmonisierten Rechtsrahmens nun die Grundlage zur Öffnung des Marktes für Finanzdienstleistungen geschaffen. Die European Banking Authority (EBA) als unabhängige EU Behörde hat durch eine Vielzahl von *Regulatory Technical Standards (RTS)* und *Guidelines* weitere verbindliche Vorgaben erlassen, die die Anforderungen der PSD II spezifizieren. Diese Vorgaben erlangen - bis auf die Ausnahme der *RTS for strong authentication and secure communication* - ihre Gültigkeit zum 13. Januar 2018, wenngleich sie auch noch nicht alle in der jeweils finalen Fassung verabschiedet sind.

Einführung neuer Zahlungsdienste

Mit der PSD II ist es künftig neuen Zahlungsdiensten gestattet, über die in der Direktive geforderte offene Schnittstelle direkt auf das beim kontoführenden Zahlungsdienstleister geführte Konto des Zahlungsdienstnutzers zuzugreifen.

Der *Zahlungsauslösedienst* platziert im Auftrag des Zahlungsdienstnutzers unter Verwendung der für den Kontozugriff notwendigen Authentifizierungsparameter den Zahlungsauftrag bei dessen kontoführenden Zahlungsdienstleister, ohne dabei jemals selbst in Kontakt mit den Kundengeldern zu

kommen. Dem Zahlungsauslösedienst ist es somit möglich, über mobile Anwendungen oder Web-Lösungen Überweisungsaufträge bei der kontoführenden Bank des Kunden auszulösen.

Der *Kontoinformationsdienst* erhält ebenfalls - mit ausdrücklicher Zustimmung des Kontoinhabers - einen Kontozugang, der es ihm künftig erlaubt, die Informationen zu Buchungen, Kontoständen und weiteren Kontodetails auszulesen und für seine Dienstleistungszwecke zu verwenden.

Innerhalb der Startup Community erwachsen vielfältige kreative Ansätze von App-Anwendungen, die den Zahlungsdienstnutzern z.B. das Führen von Haushaltsbüchern erleichtern, das Ausgabeverhalten analysieren und graphisch aufbereiten und dabei Tipps für Einsparmöglichkeiten aufzeigen können.

Da der Kontoinformationsdienst weder in Berührung mit Kundengeldern kommt noch direkt Zahlungsaufträge erteilt, besteht für den Kontoinformationsdienst lediglich eine Registrierungspflicht bei der Bundesanstalt für Finanzen (BaFin). Für den Zahlungsauslösedienst wurden hingegen höhere Kriterien formuliert – insbesondere eine explizite Zulassungspflicht bei der BaFin und Auflagen hinsichtlich der Eigenmittelhinterlegung.

Access to Account

Die in der PSD II für den Zugriff der Drittdienstleistern geforderte offene Schnittstelle zum direkten Kontozugang („Access to Account“ oder „XS2A“) stellt einige Marktteilnehmer vor Herausforderungen. Der Kontozugriff setzt eine offene Schnittstelle voraus, die nach Meinung der EU Kommission und EBA dieselben Qualitätseigenschaften enthalten soll wie die vorhandene Kundenschnittstelle zum aktuell genutzten Online-Banking. Im Falle eines Ausfalls des Schnittstellenzugangs ist, nach Meinung der EBA, seitens der kontoführenden Zahlungsdienstleister ein Zugang über die originäre Kundenschnittstelle sicherzustellen. Wie das allerdings technisch aussehen soll, das gibt die derzeit vorliegende Spezifikation der RTS nicht vor.

Auch die Banken haben derzeit ihre Schwierigkeiten mit dem aktuell von einigen FinTechs angewandten technischen Zugang: besser bekannt unter dem Begriff „Screen Scrapping“ wird seitens der Drittdienstleister ein Verfahren angewandt, bei dem der Zugang über eine, der des kontoführenden Zahlungsdienstleisters nachgebaute Website imitiert wird. Nach Eingabe der Zugangsdaten des Nutzers, werden diese Daten für den direkten Zugriff über die offene Kundeschnittstelle des kontoführenden Zahlungsdienstleister verwandt.

Nicht nur die Weitergabe der Zugangsdaten an Dritte sehen die Banken kritisch, sondern mahnen sie auch hinsichtlich des Zugriffs auf die direkte Kundenschnittstelle zur Vorsicht: Ohne im Einzelfall bankseitig unterscheiden zu können, ob der tatsächliche Kontoinhaber oder ein von ihm beauftragter Dienst sich Zugang verschafft, könnten über diesen Kanal

vielfältigste Informationen abgegriffen werden. Dies könnten auch Daten sein, die weit über die für einen Zahlungsdienst erforderlichen hinausgehen und deren Ausmaß oftmals für die Kunden nicht sichtbar sein könnten.

Die Bereitstellung einer offenen Schnittstelle für den Kontozugriff erfolgt daher nicht ganz ohne Einwände der Banken: die technischen Anforderungen an extern zugänglicher Testumgebung und Hochverfügbarkeit der Schnittstelle liegen hoch und führen in der Umsetzung zu Mehrkosten auf Bankseite, denen vorerst auch keine Erträge gegenüberstehen. Zudem ist nicht ganz klar, wie sich die EBA die Anbindung genau vorgestellt hat. Wurden seinerzeit zur SEPA Einführung konkretere Spezifikationen vorgelegt, so überlässt die EBA es heute dem Markt selbst zu handeln. Die zur Klärung veröffentlichten *Regulatory Technical Standards for strong authentication and secure communication* lassen Spielraum für Interpretationen und konkrete Hinweise zur Umsetzung leider vermissen. Einerseits strengt die EU Kommission die Harmonisierung des EU Raumes an, andererseits überlässt sie es dem aufgerüttelten Markt, sich selbst zu finden und neu zu positionieren - ein Dilemma.

Was einst den traditionellen Banken in der Hoheit allen Zahlungsverkehrs vorbehalten war, bricht nun auf und zwingt sie zum raschen Umdenken. Neue Anbieter - sogenannte „Third Party Provider“ (TPP) - etablieren sich und bieten dem *mobil* gewordenen Kunden von heute neue intelligente Lösungen. Es ist nicht mehr DIE EINE BANK, die der Kunden als zentralen Anlaufpunkt nutzt. Es sind ANDERE und WEITERE, die mit Apps auf simple Art und Weise den sich über Generationen gewandelten Kunden dort abholen, wo er heute steht: immer *mobil* und *connected*, affin für smarte Lösungen mit einfachster Bedienung im „One-Klick“-Modus mitten im Wandel der Digitalisierung.

Starke Kundenauthentifizierung

Die PSD II fordert zwei Faktoren zur Sicherung einer starken Kundenauthentifizierung („2FA“). Die seit der Einführung der „Mindestanforderung zur Sicherheit im Internet“ (MaSI) hier in Deutschland geltende Multifaktorenauthentifizierung wird mit der PSD II und den *RTS for strong authentication and secure communication* somit ergänzt und differenziert.

Die künftig für eine Authentifizierung notwendigen zwei voneinander unabhängigen Faktoren entstammen dabei den folgenden Bereichen.

- Wissen (z.B. Benutzername, Alias, Passwort)
- Besitz (z.B. mTAN, Chip-TAN, App-TAN, Token)
- Inhärenz (z.B. Fingerprint, Iris, Gesicht, Stimme, Unterschrift)

Auch hier belässt es die EBA bei interpretationsfähigen Anforderungen an die Authentifizierungsverfahren und überlässt die Findung konkreter Lösungen den Marktteilnehmern bzw. die Bewertung letztendlich den Regulierungsbehörden.

Waren von der Regelung zur MaSI bisher nur Internetzahlungen betroffen, so geht die PSD II weit darüber hinaus und schließt nun auch alle Zahlungen am Point of Sale (POS) ein. Dennoch erlaubt der aktuelle Draft zur *RTS for strong authentication and secure communication* einige Ausnahmen zur starken Kundenauthentifizierung (Auszug):

- Allgemein alle Transaktionsbeträge < 30 EUR
- Kontaktlose Transaktionen < 50 EUR
- Transaktionen basierend einer White List
- „Risk-based Authentication" (Festlegung des Authentifizierungsverfahrens nach einer Risikoanalyse auf Basis aller gesamtheitlich, verarbeiteten Transaktionen durch den Zahlungsdienstleister)

Verbraucherschutz

Neben einer technischen Absicherung des Kunden durch die „starke Kundenauthentifizierung" hat die EU Kommission weitere Regelungen zum Schutze der Verbraucher erlassen. Beispielsweise ist die Haftungshöchstgrenze für unautorisierte Transaktionen gesenkt worden. Abseits von Vorsatz haftet der Zahlungsdienstnutzer bei Verlust oder Missbrauch künftig bis maximal 50 EUR (ursprünglich 150 EUR). Die Erstattung einer unautorisierten Transaktion ist unverzüglich, jedoch spätestens innerhalb eines Geschäftstages dem Kontoinhaber gutzuschreiben. Diese Vorgabe scheint zunächst trivial, jedoch sind bei der Operationalisierung insbesondere auch nachgelagerte Prozesse zu betrachten, die z.B. bei kreditkartengestützten Zahlungsdiensten größere Prozessanpassungen verursachen dürften.

Auch hat die Kommission grundlegende Vorgaben zu den Entgelten erlassen. Grundsätzlich ist ein Entgelt für den Einsatz eines kartenbasierten Zahlungsmittels („surcharging") nicht mehr zulässig, sofern die Zahlung durch die EU Interchange Regulierung (MIF-VO) reguliert ist (Consumer Cards innerhalb des EWR, am physischen oder virtuellen POS) und erlaubt dies aber explizit für die anderen Einsatzgebiete (Corporate Cards, Karteneinsatz außerhalb des EWR oder an Geldautomaten). Dennoch schafft die PSD II Rahmenbedingungen, in denen die Zahlungsdienstleister künftig kostenorientiert Entgelte erheben können.

Ebenso stellt die Direktive weitergehende Anforderungen an Kundeninformationen, insbesondere zur Entgelttransparenz.

Meldewesen

Nachdem ein zentrales Meldewesen von Störungen im Zahlungssystem an die Regulierungsbehörden (in Deutschland die BaFin und die Bundesbank) bereits mit der MaSI eingeführt wurde, hat die EBA die Anforderungen hieran deutlich erweitert (z.B. explizite Initial-, Zwischen- und Abschlussmeldungen) und auch im Rahmen der *Guidelines on major incidents reporting under Payment Service Directive 2* detaillierte Vorgaben über die involvierten Parteien, Prozesse und Informationen – inklusive eines standardisierten Formulars – vorgestellt.

Business Transformation

Die Zeit ist knapp: trotz der teilweise unvollständigen Vorgaben und des Interpretationsspielraums gilt für alle Beteiligten, sich proaktiv mit der PSD II auseinander zu setzen und die Auswirkung zu bewerten. Konkret bedeutet dies im Kern:

- Einführung und Umstellung auf eine einheitliche, offene Schnittstelle für den Kontozugang
- Ermittlung der Auswirkung auf die eigenen Geschäftsprozesse und Abläufe
- Anpassung der Verbraucher-relevanten Dokumente

Die Öffnung der Kontozugangsschnittstellen, dass die bisher etablierte, auf Ausschließlichkeit beruhende Kunde-Bank-Beziehung ausgedient hat. Auch wenn Drittanbieter auf die hauseigenen, dem Kunden gehörenden Daten zugreifen können, so ist es am Ende der gemeinsame Kunde aller. Es bedarf einer neuen Kundenfokussierung, die sich nicht in der Verdrängung des Mitbewerbers, sondern in der gemeinschaftlichen Erfüllung seiner Bedürfnisse ausdrückt. Dabei gilt es, den Kopf „frei zu haben“ für neue Ideen, zur Neuausrichtung und Findung der eigenen, neuen Identität. Ein nicht einfacher Spagat zwischen zeitgerechter Compliance und strategischer Neuausrichtung.

All diese Themen und Fragestellungen sollen zum 13. Januar 2018 abgeschlossen und umgesetzt worden sein – so will es das Gesetz. Einzig die *RTS for strong authentication and secure communication* wird erst 18 Monate nach Veröffentlichung in Kraft treten, was in keinster Weise als Schonfrist fehlinterpretiert werden sollte.

Profitieren Sie von unserer Expertise. Wir unterstützen Sie gern.