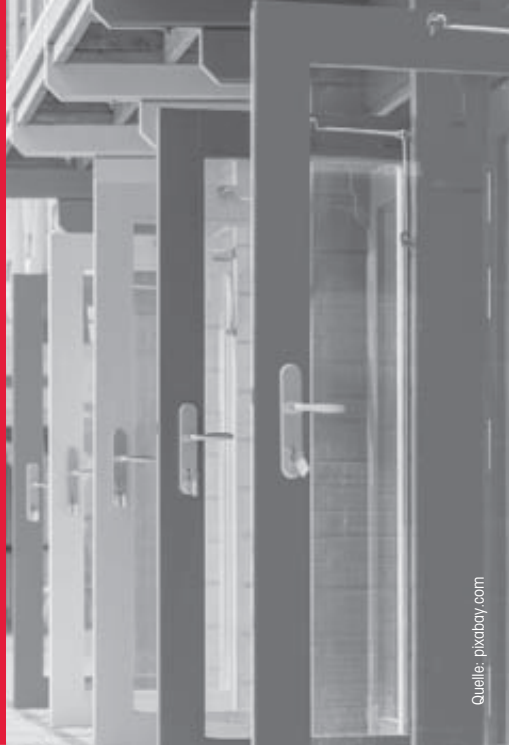
# PSD2: Neue Chancen für aktive Banken

Von Gerd Cimiotti und Matthias Hönisch



Quelle: pixabay.com

**Die PSD2 wird den Zahlungsverkehr noch stärker verändern als die Interchange-Regulierung, meinen Gerd Cimiotti und Matthias Hönisch. Denn die Rollen im Zahlungsverkehr verändern sich. Für Banken sehen die Autoren dabei neue Chancen, sich beispielsweise als Identitätsdienstleister auch für andere Bereiche als den Zahlungsverkehr zu positionieren. Die PSD2 bringt aber auch neue Kostenbelastungen für die Infrastruktur der Banken mit sich. Die Autoren plädieren deshalb für möglichst einheitliche Standards. Die Berlin Group hat bereits eine XS2A-Schnittstelle vorgestellt. Red.**

US-Präsident John F. Kennedy hat einmal gesagt, dass das chinesische Wort für Krise auch gleichzeitig Chance bedeuten kann. Diese Beobachtung charakterisiert ziemlich genau die Situation bei der bevorstehenden Inkraftsetzung der EU-Zahlungsdiensterichtlinie (PSD2) und der dazugehörigen „Regulatory Technical Standards" (RTS) und Leitlinien der EBA. Die PSD2 ist bereits am 8. Oktober 2015 vom Europäischen Parlament verabschiedet worden und wird im Januar 2018 in deutsches Recht umgesetzt werden. Sie wird wahrscheinlich einen deutlich größeren Einfluss auf den Zahlungsverkehr in Europa haben als die EU-Verordnung über die Begrenzung der Interchange bei Kartenzahlungen (MIF-Verordnung), denn hierbei geht es unter anderem auch darum, dass die von einer Bank bereitgestellte Infrastruktur des Online-Bankings anderen (dritten) Zahlungsdienstleistern preisfrei zugänglich gemacht werden muss. Damit wird die Kontoschnittstelle für Drittdienstleister geöffnet.

## Neu definierte Rollen im Zahlungsverkehr

Die PSD2 schafft neue Spielregeln im Zahlungsverkehr mit Auswirkungen für alle Teilnehmer: für die Kunden, neue Anbieter (zum Beispiel Fintechs), aber vor allem für die europäischen Banken. Die Banken werden mit der PSD2 verpflichtet, durch Schnittstellen, sogenannte Application Programming Interfaces (API), Zugänge für Drittdienstleister zu gewähren und damit den Kontozugriff („Access to Account", XS2A) zu schaffen, damit diese direkter am Zahlungsverkehr teilnehmen können.

**Zu den Autoren**

**Gerd Cimiotti**, Geschäftsführer, SRC Security Research & Consulting GmbH, Bonn, **Matthias Hönisch**, Head of Cards, Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. (BVR), Berlin

Drittdienstleister erhalten somit einen diskriminierungsfreien Zugang zu den Zahlungsverkehrskonten der Kunden. Die beiden folgenden Klassen der Drittdienstleister sind die wichtigsten.

**1. Zahlungsauslösedienst** (oder auch PISP Payment Initiation Service Provider): Ein Drittdienstleister, der vom Kunden beauftragt beziehungsweise berechtigt ist, Zahlungen (Überweisungen) in seinem Namen direkt von seinem Konto bei der kontoführenden Bank auszulösen. Diese Zahlungsauslösedienste müssen künftig von der nationalen Finanzaufsicht zugelassen und beaufsichtigt werden. Zudem brauchen die Zahlungsauslösedienste eine entsprechende Versicherung.

**2. Kontoinformationsdienste** (oder auch AISP Account Information Service Provider): Kontoinformationsdienste oder Aggregatoren, welche im Auftrag des Kunden und Kontoinhabers Kontoinformationen elektronisch direkt bei den kontoführenden Finanzinstituten abholen, mit dem Ziel, konsolidierte und benutzerfreundliche Informationen und Übersichten in elektronischer Form für den Kunden bereitzustellen. Diese Drittdienstleister müssen sich künftig lediglich registrieren.

Für die europäischen Regulatoren ist der Zahlungsverkehr ein wesentlicher Baustein des digitalen europäischen Binnenmarktes. Die Regulierung soll dazu dienen, den Wettbewerb im Zahlungsverkehr

zu intensivieren und die Entwicklung von Produktinnovationen im Zahlungsverkehr zu beschleunigen. Übergeordnete Zielsetzung des Regulierers ist die Unterstützung eines europäischen digitalen Binnenmarktes durch sehr wettbewerbsfähige und innovative Zahlungsverkehrsdienstleistungen.

### Warum wird der Zahlungsverkehr reguliert?

Die Regulierung des Kontozugangs geht einher mit weiteren regulatorischen Eingriffen, wie der EU-Datenschutzgrundverordnung oder der Etablierung von Instant-Payments-Infrastrukturen, um den Zahlungsverkehr in Zukunft auch in Echtzeit abwickeln zu können.

Dabei soll aber gleichzeitig gewährleistet werden, dass der Zahlungsverkehr – wie in der Vergangenheit – sicher und effizient abgewickelt wird. Nicht zuletzt dann, wenn der Zahlungsverkehr in Zukunft auch noch in Echtzeit abgewickelt wird, müssen mit der Öffnung des Zahlungsverkehrs für Drittdienstleister auch Regeln und Mindeststandards für die Absicherung der Zahlungsverkehrstransaktionen eingeführt und überwacht werden, die durch Drittdienstleister initiiert werden. Dies ist notwendig, um die gebotene Balance zwischen der Sicherheit des Zahlungsverkehrs und dem Komfort durch auf der Öffnung von Bankinfrastrukturen beruhenden innovativen Zahlungsdienstleistungen zu gewährleisten.

### Zwei wesentliche Änderungen

Aus Sicht des Zahlungsverkehrs sind mit der Umsetzung der PSD2 in nationales Recht vor allem zwei wesentliche Änderungen verbunden:

- Höhere Anforderungen an die Absicherung von Zahlungstransaktionen (umgesetzt über den EBA RTS on Strong Customer Authentication) und an den Nachweis der Angemessenheit von Sicherheitsmaßnahmen (Risikomanagement und -controlling);
- formale Trennung zwischen Produktion von Zahlungsverkehrsleistungen und deren Distribution durch Einführung des Kontoinformationsdienstes und des Zahlungsauslösedienstes als neue Rollen.

Die neuen Anforderungen an die Absicherung von Zahlungstransaktionen führen in Banken dazu, dass Authentifizierungsverfahren auf die neuen Anforderungen des EBA RTS ausgerichtet werden müssen und dass die interne Dokumentation zum Risikomanagement an die Anforderungen der PSD2 angepasst werden muss. Dies betrifft nicht nur die Risikoerfassung und die Bewertung der Effektivität der Maßnahmen zur Begrenzung der Risiken, sondern auch die Etablierung von Prozessen zur Bereitstellung der im Rahmen des EBA RTS geforderten statistischen Auswertungen zu Missbrauchsfällen.

### Auswirkungen auf den Nutzerkomfort noch nicht klar absehbar

Die neuen Rollen des Zahlungsauslösedienstes und des Kontoinformationsdienstes können langfristig große Auswirkungen auf die Geschäftsmodelle im Zahlungsverkehr haben. Die mehr oder weniger parallele Einführung von Instant Payments auf Basis einer vom Regulierer bereitgestellten Infrastruktur (TIPS) kann in diesem Zusammenhang auch als ergänzender Schritt zur Trennung der Produktion von zentralen Infrastrukturen verstanden werden. Damit kann die PSD2 im Zahlungsverkehrsmarkt langfristig ähnliche Wirkungen entfalten wie dies bei der regulatorischen Öffnung der Telekommunikations- oder der Energiemärkte erfolgt ist.

Es ist heute noch nicht klar absehbar, was sich aus Kundensicht im Einzelnen ändern wird und welche neuen Services durch die PSD2 entstehen werden. Kurzfristig dürfte vor allem die Umsetzung der Anforderung zur Nutzung der Strong Customer Authentication Auswirkungen haben. Abhängig davon, wie der noch in Abstimmung befindliche RTS letztlich genau aussehen wird, ist es nicht ausgeschlossen, dass im Vergleich zur heutigen Situation häufigere Authentifizierungen mittels eines starken Authentifizierungsmechanismus erforderlich werden, zum Beispiel beim Login in das Online-Banking oder etwa bei Kartenzahlungen im E-Commerce.

Ob dies so kommt und ob dies Auswirkungen auf den Komfort bei der Nutzung von Online-Zahlungsverkehrsangeboten hat, hängt wesentlich davon ab, welche Authentifizierungsverfahren künftig als ausreichend stark angesehen werden und in welcher Form Institute von den Ausnahmen des RTS zur Strong Customer Authentication Gebrauch machen können. Ein wesentliches Element wird hierbei – neben der Nutzung biometrischer Verfahren – wahrscheinlich auch die Nutzung sogenannter risikobasierter Verfahren sein, das heißt von Hintergrundsystemen, die dabei helfen sollen, risikoreichere von risikoarmen Transaktionen zu unterscheiden. Es wird in Zukunft aus Kundensicht möglicherweise weniger vorhersagbar sein, in welchen Fällen eine starke Kundenauthentifizierung von ihm verlangt wird.

### Technische Anpassungen für alle erforderlich

Mit der PSD2 wird unter anderem klargestellt, dass die Kunden Zahlungen über Zahlungsauslösedienste initiieren dürfen. Das heißt zum Beispiel auch, dass die Sicherheitsverfahren der Bank (PIN und TAN) gegebenenfalls auch aufseiten der Zahlungsauslösedienst eingegeben werden dürfen.

Für den Zugriff der Drittdienstleister auf das Konto sollen Banken den Drittdienstleistern künftig eine dedizierte Schnittstelle kostenlos anbieten (PSD2-Schnittstelle). Falls sie keine solche Schnittstelle anbieten, müs-

sen sie weiterhin das sogenannte Screen Scraping gegen sich gelten lassen, wobei hier noch nicht klar ist, wie dann die Anforderung der PSD2 zur Identifizierung des Drittdienstleisters durch den Kontoführer sinnvoll umgesetzt werden kann. Mit anderen Worten: Auch Zahlungsdienstleister, die keine dedizierte PSD2-Schnittstelle anbieten möchten, müssen technische Anpassungen vornehmen, damit sie zweifelsfrei feststellen können, ob der Zugriff auf das Konto tatsächlich über einen berechtigten Drittdienstleister erfolgt. Dies ist schon deshalb erforderlich, um im Falle von Fehlern in der Abwicklung Regressansprüche gegenüber Drittdienstleistern durchsetzen zu können.

### eIDAS-Verordnung regelt das Rechte-Management

Das Gelingen dieses Rechte-Managements kann europaweit durch die gerade in Kraft getretene eIDAS-Verordnung gewährleistet werden, die die Akzeptanz von Zertifikaten regelt. Damit kann zum Beispiel ein Zahlungsauslösedienst aus Portugal auf dem Konto eines Kunden einer Bank in Österreich eine Transaktion auslösen. Das Bundesamt für Sicherheit in der Informationstechnik hat hierzu einen Vorschlag für eine Ergänzung der eIDAS-Zertifikatspolicy vorgelegt, der zwischenzeitlich auch bereits Eingang in die internationale Normierung bei ETSI gefunden hat und auf breite Unterstützung zu stoßen scheint. Darüber hinaus müssen Banken, die für den Zugriff auf das Konto die Screen-Scraping-Schnittstelle nutzen möchten, sicherstellen, dass Drittdienstleister tatsächlich nur auf die für ihre Dienstleistung erforderlichen Kundendaten zugreifen dürfen, denn die Vorgaben der EU-Datenschutzgrundverordnung, die ab Mai 2018 gilt, sind natürlich ebenfalls einzuhalten.

Insgesamt erscheint die Umsetzung der PSD2-Anforderungen über eine dedizierte PSD2-Schnittstelle für viele Institute vorteilhafter als die Bereitstellung ein Screen-Scraping-Lösung, wenn Zahlungsdienstleister daran interessiert sind, einerseits die regulatorischen Vorgaben zu erfüllen, andererseits aber für die Schnittstelle zur Kommunikation mit den eigenen Kunden möglichst große Freiheitsgrade zu gewährleisten.

### PSD2-Vorbereitung via Berlin Group

Die PSD2 legt lediglich fest, dass Banken eine Schnittstelle zum Zugriff auf das Konto anbieten müssen, nicht, wie diese aussehen soll. Eine individuelle Festlegung einer technischen Schnittstelle durch jedes Institut wäre aber weder ökonomisch noch sachgerecht. Denn jedes Institut müsste seine Schnittstelle nicht nur gegenüber allen potenziell infrage kommenden Zahlungsauslösediensten und Kontoinformationsdiensten veröffentlichen, sondern es müsste auch Testmöglichkeiten zur Verfügung stellen und gewährleisten beziehungsweise nachweisen, dass die Schnittstelle tatsächlich den jeweiligen regulatorischen Anforderungen entspricht.

Es war daher naheliegend, hierfür eine Standardisierung auf europäischer Ebene zu initiieren. Hierfür bot sich die sogenannte Berlin Group an, die eine eigene Arbeitsgruppe zur Definition der PSD2-Schnittstelle eingerichtet hat. Die Berlin Group hat sich im Oktober 2004 in Berlin konstituiert und hat daher ihren Namen. Derzeit besteht sie aus 24 Hauptakteuren der Zahlungsbranche aus sieben verschiedenen Ländern der Eurozone und aus Großbritannien, Schweden, Dänemark, Norwegen, Island, Lettland, Estland, Litauen, Türkei, Bulgarien, Ungarn und Serbien. Die Teilnehmer an der Arbeitsgruppe kommen von Banken (wie etwa aus Deutschland die DZ Bank, die Deutsche Bank), Bankenverbänden, nationalen und internationalen Zahlungssystemen (zum Beispiel Visa) und Interbankprozessoren, die im Sepa-Raum arbeiten. Das Ziel der Berlin Group ist es, als Ergänzung zu den Arbeiten des EPCs offene Scheme- und Prozessor-unabhängige Standards im Interbanking-Bereich zu schaffen, als Ergänzung zu den Arbeiten des EPC. In enger Abstimmung wurde im Rahmen der Berlin Group ein erster Entwurf einer Spezifikation entwickelt, in dem alle gesetzlich vorgeschriebenen Rollen der Drittdienstleister im Regime der PSD2 beschrieben worden sind, sodass die Umsetzung der Spezifikation in einer kontoführenden Bank die Anforderungen vollumfänglich erfüllen kann. Der Entwurf der PSD2-konformen XS2A-Schnittstelle ist am 2. Oktober 2017 am Markt vorgestellt worden und wird bis zum 17. November 2017 konsultiert, sodass die Rechenzentren der Banken noch im Jahr 2018 mit den Arbeiten der Implementierung der PSD2-Schnittstelle beginnen können. Bereits jetzt haben viele Banken und Bankengruppen in Europa erklärt, auf die Berlin-Group-Schnittstelle als einheitliche und regelkonforme XS2A-Schnittstelle zurückgreifen zu wollen und diese zu implementieren.

### Chancen für Banken

Den Akteuren im Finanzmarkt stehen durch die PSD2 weitreichende Veränderungen bevor, von denen auch der Bereich der Kundenauthentifizierung betroffen sein wird. Bestehende Verfahren müssen unter Umständen abgelöst oder überarbeitet werden, um den Anforderungen des EBA RTS zu entsprechen. Hierbei ist es wichtig, ein gutes Verständnis der Kundenbedürfnisse und der rechtlichen sowie technologischen Gestaltungsspielräume zu verbinden.

Für Banken bieten sich aber möglicherweise auch neue Marktchancen, denn sie können sich zum Beispiel auch selbst als Drittanbieter positionieren. Durch die gleichzeitige Regulierung der Drittanbieter entsteht ein Level Playing Field, das Banken einen fairen Wettbewerb mit den neuen Wettbewerbern ermöglicht.

### Banken als Identity Provider

Die mit dem EBA RTS zur Strong Customer Authentication verschärften Anforderungen an die Authentifizierung von Kunden bei Zahlungen tragen dazu bei, dass der Be-

darf zur Ausrichtung der technischen Sicherheit am individuellen Risiko einer Transaktion zunimmt. Banken stehen dabei in ihrer Rolle als „Identity Provider" für Bankdienstleistungen künftig im Wettbewerb mit anderen Anbietern digitaler Identitäten. Die steigenden Anforderungen an die Kontrolle über die eigenen Daten, die wachsenden Datenschutzanforderungen und die häufige Nutzung der von Banken ausgegebenen digitalen Identitäten im Rahmen des Zahlungsverkehrs bieten Banken zunächst eine gute Ausgangsposition, um in dem sich abzeichnenden „Digitalisierungsmarkt" die Rolle des Identity Providers zu übernehmen. Beispiele aus Norwegen, Schweden und Finnland zeigen zumindest, dass dies grundsätzlich möglich ist.

In Verbindung mit den sich derzeit im Markt etablierenden Interoperabilitätsstandards für Authentifizierungsinstrumente (wie zum Beispiel Fido) wäre es dann auch möglich, ein bankbezogenes Authentifizierungsinstrument auch in anderen Online-Diensten zu nutzen. In Verbindung mit dem eIDAS-Framework ist es auch vorstellbar, einen entsprechenden Mechanismus zum Beispiel zur Generierung von eIDAS-Fernsignaturen zu nutzen und das kreditwirtschaftliche Authentifizierungsverfahren so auch zur rechtssicheren Absicherung von Willenserklärungen in anderen Online-Diensten zu nutzen.

## Neues digitales Ökosystem

Die Bereitstellung einer Smartphone-Applikation zur Authentifizierung von Bankkunden und die Integration dieser Applikation als Authentifizierungsinstrument in möglichst viele Online-Dienste können damit einen ersten Schritt bei der Entwicklung einer Digitalisierungsstrategie auf Grundlage von Zahlungsverkehrsinfrastrukturen darstellen. Ein Kunde mit hoher digitaler Affinität mag eine schnelle und reibungslose Authentifizierung über sein Smartphone bevorzugen, während ein Firmenkunde möglicherweise die Anforderung hat, einen besonders sicheren Zugang über seinen PC zur Verfügung gestellt zu bekommen. Wenn diese Aspekte beachtet werden, bietet neben dem Zugriff Dritter auch die starke Kundenauthentifizierung Zahlungsdienstleistern die Chance, notwendige Investments für die Umsetzung der PSD2 mit einer Stärkung der eigenen Position im Wettbewerb um die Kunden zu verknüpfen.

Noch konzentrieren sich Digitalisierungsinitiativen im Zahlungsverkehr vor allem auf die Entwicklung von Mobile-Payment-Lösungen. Seit 2017 stehen auch zunehmend Lösungen zur Authentifizierung im Mittelpunkt der Entwicklung im deutschen Markt. Ein nächster logischer Schritt könnte die Unterstützung der Digitalisierung von Prozessen Dritter mithilfe der dem Authentifizierungsmechanismus zugrunde liegenden Daten sein. Unter Voraussetzung einer standardisierten Schnittstelle zur Abfrage von Daten (nach vorhergehender Freigabe durch den Kunden) sind zum Beispiel Services zur elektronischen Bereitstellung von Attributen zu E-Identities vorstellbar.

Offene APIs sind Voraussetzung für die Umsetzung künftiger, eher datengetriebener Geschäftsmodelle. Mit der PSD2-konformen XS2A-Schnittstelle werden Banken künftig bereits für den Kontenzugriff einen Basisservice als API anbieten und könnten auf dieser Grundlage APIs für Mehrwertdienstleistungen konzipieren, wie zum Beispiel die Adressierung über Handynummern oder E-Mailadressen, die elektronische Rechnungsstellung, die Verifizierung von personenbezogenen Attributen im Rahmen von Onboarding beziehungsweise Know-Your-Customer-Services, die Bereitstellung von Bonitäts-/Risikoinformationen für Scoringsysteme oder – soweit datenschutzrechtlich umsetzbar – die Bereitstellung von Marketinginformationen. Prinzipiell wäre vorstellbar, dass Banken auf Grundlage entsprechend standardisierter Schnittstellen eigenständige digitale Ökosysteme – analog zu einem App-Store – anbieten, zu dem Drittapplikationen, die die von den Banken angebotenen APIs nutzen, zugelassen werden können.

Die Entwicklungen bei der Beschleunigung des Zahlungsverkehrs (Instant Payments) unterstützen diesen Prozess massiv. Für eine kundenorientierte Bank ist es positiv, dass sie den Kunden beziehungsweise das Bankkonto in den Mittelpunkt des Bank-Ökosystem stellen kann.

## Kostenbelastungen durch europaweite Schnittstellen begrenzen

Allerdings stellen die Umsetzungserfordernisse auch eine erhebliche Kostenbelastung für die Infrastruktur der Banken dar, da nicht mehr der (menschliche) Kunde die Schnittstelle bedienen muss, sondern häufig ein durch eine „Maschine" gesteuerter Mechanismus, der durch Datenabfragen der Bank erhebliche Kosten verursachen kann. Um der daraus erwachsenen Herausforderung des Kostenmanagements zu begegnen, tritt die Deutsche Kreditwirtschaft für möglichst europaweit standardisierte Schnittstellen ein. Mit der Umsetzung der Berlin-Group-XS2A-API werden einmal alle regulatorischen Anforderungen in möglichst effizienter Weise umgesetzt. Es kann aber gleichzeitig auch die Voraussetzung für ein neues Ökosystem von Zahlungsdienstleistern zur Digitalisierung von Prozessen Dritter geschaffen werden. Die Etablierung von Instant-Payments-Infrastrukturen führt dazu, dass die von Banken geschaffene technische Infrastruktur Echtzeit-Kommunikation theoretisch zwischen beliebigen Kontoinhabern in Europa anbieten kann.

Die Kreditwirtschaft hat damit die Möglichkeit, sozusagen das „WhatsApp" für werthaltige Informationen zu schaffen. Voraussetzung für die erfolgreiche Nutzung dieser Infrastruktur ist immer die Generierung kritischer Massen auf der Ebene der Nutzer. Dies kann immer nur dann funktionieren, wenn es gelingt, sich innerhalb der Kreditwirtschaft für solche Mehrwertfunktionen auf gemeinsame Standards zu verständigen, die es erlauben, die digitalen Ökosysteme der verschiedenen Banken miteinander zu verbinden.