PAYMENT SERVICE DIRECTIVE II

Herausforderungen und Chancen für Banken, Finanzdienstleister und Drittanbieter

WHITEPAPER

Version 07/17

Acando GmbH

Liebe Leserinnen und Leser,

Autoren

Imad Hassani (l.),
Senior Consultant

Shushant Kakkar,
Consultant

Acando GmbH

die EU Zahlungsdienstrichtlinie (Payment Service Directitve II) tritt im Januar 2018 in Kraft. Geldinstitute werden vom Europäischen Parlament und Rat verpflichtet, Drittanbietern Zugriff auf Zahlungskonten zu gewähren. Ziel ist es, den Markt für Innovationen zu öffnen und die Digitalisierung zu fördern. Die Implementierung der Richtlinie betrifft kleine wie große Bankinstitute und schafft Möglichkeiten, um neuartige Finanzdienstleistungen am Markt zu etablieren.

Welchen Herausforderungen müssen sich neue und bestehende Finanzdienstleister stellen, wie wird die Kundensicherheit gewährleistet und welche Chancen haben Banken, um Daten effizienter zu nutzen und die Kundenerfahrung zu verbessern?

Unser zusammenfassender Überblick dient der Orientierung im technologischen Anforderungskatalog und soll betroffenen Unternehmen dabei helfen, sich frühzeitig für das neue Marktumfeld fit zu machen.

INHALT

EINFÜHRUNG IN DIE PAYMENT SERVICE DIRECTIVE II

Die Direktive soll Innovationen fördern und gleichzeitig den Verbraucherschutz stärken.

Die PSD II ist eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt, die 2015 beschlossen wurde und bis 2018 umgesetzt sein muss. Aufbauend auf die bereits wirksame PSD I, die den Europäischen Zahlungsverkehrsraum (SEPA) vereinheitlicht hat, soll die zweite Direktive Innovationen im Zahlungsverkehrs- und Bankenumfeld fördern und gleichzeitig Verbraucherschutz und Sicherheit erhöhen.

Die Überarbeitung der PSD I war notwendig, um die technischen Entwicklungen der letzten Jahre auch in der Finanzbranche nutzen zu können und somit den Markt für Unternehmen mit innovativen Dienstleistungen und Produkten zu öffnen. In diesem Zusammenhang wurde auch eine rechtliche Grundlage zur Regulierung und Zertifizierung von sog. Third Party Providern (TPP) geschaffen.

Weitere Änderungen sind die Ausweitung des Geltungsraums der Richtlinie, die starke Haftungsbeschränkung zugunsten der Kunden und Anpassungen bei den Gebühren, z.B. für Auslandszahlungen.

Die Haftungsbeschränkungen sehen vor, dass Banken das Kundenkonto im (potenziellen) Betrugsfall innerhalb von 24 Stunden wieder bereinigen müssen. Erst dann kann mit der Ermittlung begonnen werden.

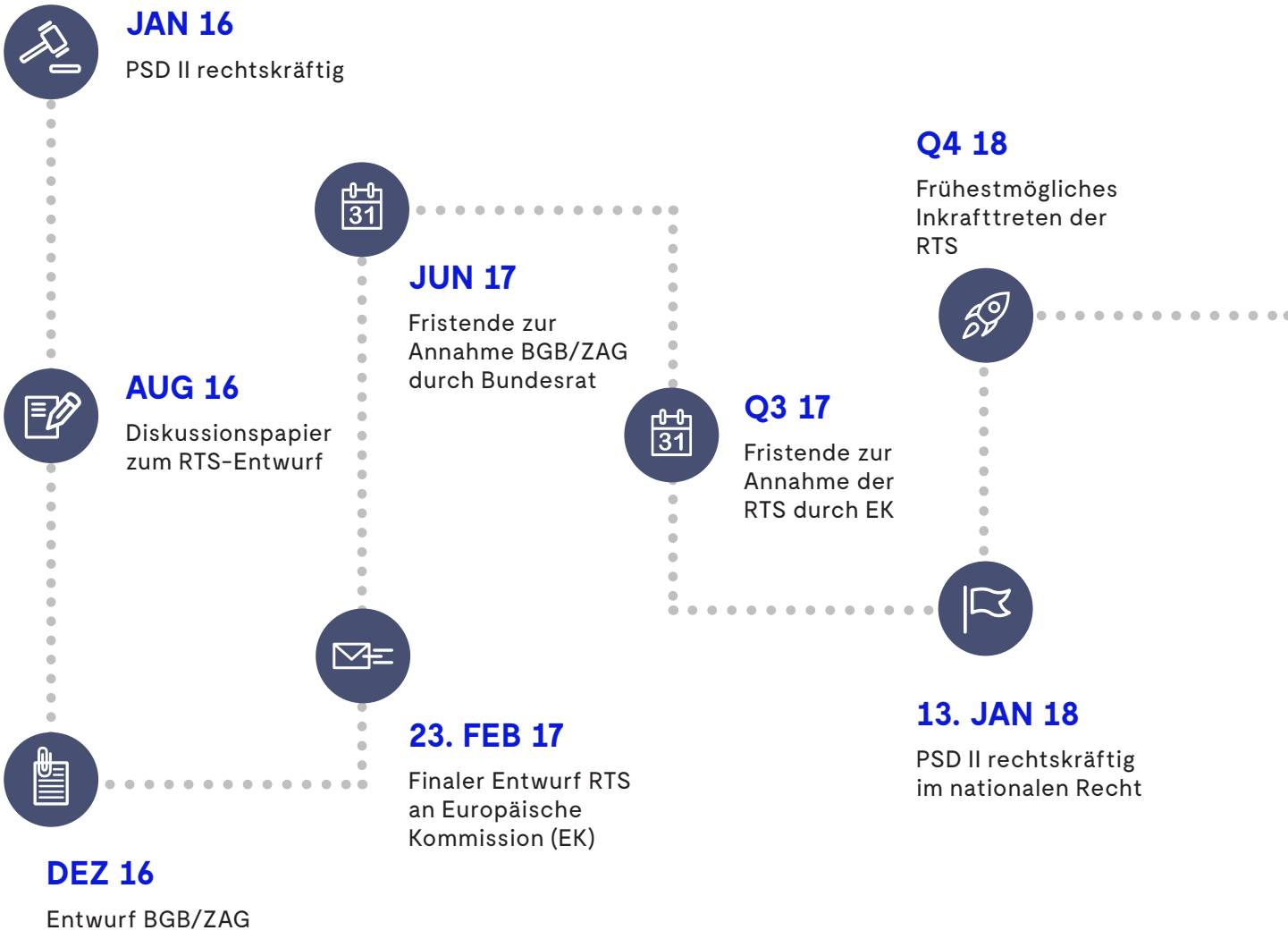
Die Themenfelder der PSD II

Die Entwicklung der neuen Schnittstellen soll bis zum Q4 2018 abgeschlossen sein.

Zur Umsetzung der verschiedenen Anforderungen muss die PSD II in das nationale Recht der jeweiligen Staaten überführt werden. Ausgenommen sind die Anforderungen zur Strong Customer Authentication und Secure Communication, die in einem Regulatory Technical Standard (RTS)-Dokument erfasst wurden und europaweit einheitlich gelten.

Mit dem Inkrafttreten der RTS sind die Banken verpflichtet, die neuen offenen Schnittstellen für TPPs innerhalb von 18 Monaten zur Verfügung zu stellen, d.h. die Entwicklung muss bis zum vierten Quartal 2018 abgeschlossen sein. Voraussetzung dafür ist, dass die Europäische Kommission die RTS innerhalb der festgelegten Fristen annimmt. Anderenfalls ist eine Verzögerung mit einzuplanen.

Ursprüngliche Fristen für die Umsetzung



REGULATORY TECHNICAL STANDARD – ÜBERBLICK

Die technischen Standards zur Umsetzung der Strong Customer Authentication sind im Regulatory Standard formuliert.

Neben der Regulierung und Öffnung des Bankenmarktes ist die Förderung der Sicherheitsstandards ein wesentlicher Bestandteil der PSD II. Artikel 97 und 98 der Direktive befassen sich hierzu insbesondere mit den Anforderungen zur Strong Customer Authentication, den technischen Standards zur Umsetzung dieser und zur Gewährleistung einer sicheren Kommunikation.

Eine Strong Customer Authentication ist notwendig, sobald

- online auf das Konto zugegriffen wird (vornehmlich über das Online-Banking-Portal)
- eine elektronische Zahlung ausgelöst wird
- Handlungen über einen Online-Kanal vorgenommen werden, die einen Betrug oder Missbrauch erleichtern

Die technischen Anforderungen zur Umsetzung der Strong Customer Authentication (SCA) und sicheren Kommunikation wurden im Regulatory Technical Standard erfasst. Im Gegensatz zur Direktive muss der RTS nicht in das nationale Recht überführt werden, sondern gilt europaweit nach Veröffentlichung durch das EU Parlament. Der finale Entwurf der RTS liegt der EU Kommission aktuell zur Prüfung vor. Die dafür vorgegebene Frist bis Ende Mai 2017 wurde allerdings nicht eingehalten.

Laut der Kommission sollen Änderungen an der RTS vorgenommen werden. Dazu veröffentlicht sie eine offizielle Stellungnahme und Änderungsvorschläge, die an die European Banking Authority (EBA) zur Prüfung und ggf. Aufnahme übergeben werden. Eine Einhaltung der ursprünglichen Zeitplanung zur Umsetzung der RTS ist folglich nicht mehr gegeben.

DIE WICHTIGSTEN ARTIKEL DER AKTUELLEN RTS

Zur Identifizierung von unautorisierten oder betrügerischen Zahlungsvorgängen müssen Payment Service Provider ein Transaction Monitoring System aufbauen.

Artikel 2: General Authentication Requirements

Zur Identifizierung von unautorisierten oder betrügerischen Zahlungsvorgängen müssen Payment Service Provider (PSP) – sowohl Banken als auch Drittanbieter – ein Transaction Monitoring System aufbauen, das alle Transaktionen in Echtzeit prüft und bewertet. Dazu werden die jeweiligen Zahlungsdetails (Höhe des Geldbetrags, Empfänger, etc.), bekannte Betrugsszenarien und die kundentypischen Gewohnheiten herangezogen. Außerdem sind die verwendeten Geräte und die Software auf Manipulation bzw. Infizierung durch Viren zu prüfen.

Artikel 4: Authentication Code

Im Zuge der Strong Customer Authentication ist ein zusätzlicher Authentication Code zu erzeugen, der nur einmalig für den Zugriff zum Online-Banking-Portal oder zur Auslösung einer Zahlung oder einer potenziell „gefährlichen“ Aktion genutzt werden darf. Bei der Erzeugung des Codes muss sichergestellt sein, dass er nicht kompromittiert werden kann und im Falle eines unerlaubten Zugriffs keinerlei Rückschlüsse über die verwendeten Verfahren zur Strong Customer Authentication gezogen werden können.

Eine Strong Customer Authentication ist vergleichbar mit der heute bekannten Zwei-Faktor-Authentifizierung. Jedoch werden in der RTS keinerlei Vorgaben gemacht, wie die Zwei-Faktor-Authentifizierung genau durchgeführt und welche Technologien verwendet werden sollen. Bedingung ist nur, dass zwei der folgenden drei Elemente genutzt werden sollen.

- Besitz (z.B. ChipTAN, Token, Smartphone)
- Wissen (z.B. Passwort, PIN, ID-Nummer)
- Inhärenz (z.B. Iris-Scan, Fingerabdruck, Gesichtserkennung)

Dabei muss der Payment Service Provider sicherstellen, dass die jeweiligen Elemente gegen einen unerlaubten Zugriff geschützt sind. Im Falle eines Passwortes wäre der Schutz etwa eine sichere und verschlüsselte Speicherung in den Bankensystemen. Oder im Fall einer App die Prüfung auf Viren oder einen Jail Break der Geräte.

Wenn Ausnahmen eingesetzt werden, steigen dafür die Anforderungen für die Transaction-Monitoring- und Fraud-Detection-Systeme.

Artikel 5: Dynamic Linking

Zahlungsinformationen müssen in die Generierung des Authentication Codes einfließen. Damit soll sichergestellt werden, dass eine Manipulation der Zahlungsdaten durch einen Dritten (bspw. bei einem Man-in-the-Middle-Angriff) zur Ablehnung der Zahlung führt. Bei Sammeltransaktionen wäre der Authentication Code mit allen einzelnen Zahlungen zu verknüpfen.

Artikel 10 - 16: Exemptions from Strong Customer Authentication

Gemäß der RTS ist es gestattet, in bestimmten Fällen auf die Strong Customer Authentication zu verzichten. Ob und welche der Ausnahmen den Kunden angeboten werden, ist den jeweiligen Banken überlassen. Auch dürfen die gegebenen Parameter, wie z.B. Schwellenwert für Low Value Transactions, angepasst werden – allerdings nur strenger als die vorgegebenen Werte der RTS. Wenn Ausnahmen eingesetzt werden, steigen dafür die Anforderungen für die Transaction-Monitoring- und Fraud-Detection-Systeme der Banken und die Anforderungen an die Meldung von Betrugsfällen an die EU Finanzaufsicht.

Ausnahmen	Strong Customer Authentication nicht notwendig für	Ausnahme gilt nicht
Payment Account	• Kontostand • Umsätze der letzten 90 Tage • Nichtsensitive Zahlungsdaten	• Kunde greift das erste Mal auf das Konto zu • Umsätze älter als 90 Tage
Trusted beneficiaries and recurring transactions	• Zahlungen an vertrauensvolle Empfänger • Serienzahlung an denselben Empfänger mit demselben Betrag (Dauerauftrag)	• Änderung der Liste „vertrauensvolle Empfänger“ • Änderungen/Erstellung des Dauerauftrags
Payments to self	Zahlungen, bei denen Sender und Empfänger dieselbe Person und die Konten bei derselben Bank sind	
Low Value Transaction	• Zahlungen unter 30 € • Kumulierte Zahlungen unter 100 € • oder max. 5 aufeinander folgende Zahlungen	
Transaction Risk	Je nach Schwellenwert der Betrugsrate für Zahlungen bis zu 500 €	
Transport and parking fares	Zahlungen am Automaten	
Contactless payments at POS	• Zahlungen unter 50 € • Kumulierte Zahlungen unter 150 € • oder max. 5 aufeinander folgende Zahlungen	

Banken müssen Drittanbietern eine gesonderte Kommunikations-schnittstelle zur Verfügung stellen.

Artikel 27: Communication Interface

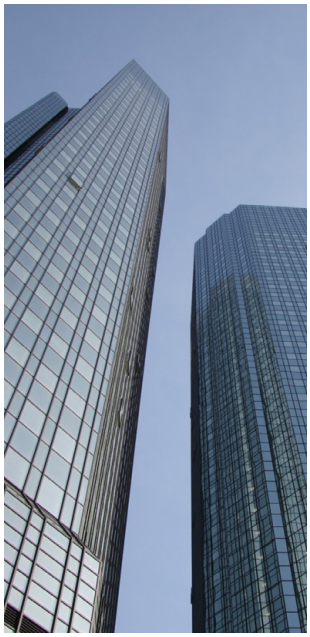
Account Serving Payment Service Provider (ASPSP), meistens Banken, müssen Payment Initiation Service Providern (PISP), Account Information Service Providern (AISP) und Payment Instrument Issuing Service Providern (PIISP) – in der Regel Drittanbieter - eine gesonderte Kommunikationsschnittstelle zur Verfügung stellen, um

- sich und den Kunden bei der Bank zu authentifizieren
- Kontoinformationen und Umsätze abzufragen
- eine Zahlung auszulösen und den Status der Zahlung abzufragen

Für die Verwendung der Schnittstelle dürfen keine Entgelte durch die Bank erhoben werden. Darüber hinaus erfordern Änderungen einen Vorlauf von drei Monaten (außer im Notfall).

Artikel 31: Data Exchanges

ASPSPs müssen sicherstellen, dass AISPs und PSPs für den Abruf der Umsätze und bei Auslösung einer Zahlung immer die gleichen Daten erhalten wie die Kunden im Online-Banking-Portal der jeweiligen Bank. Damit soll eine Diskriminierung der Drittanbieter verhindert werden. Des Weiteren soll über die Schnittstellen eine Abfrage der Kontodeckung mit einem „Ja“ oder „Nein“ als Antwort möglich sein.



BEDEUTUNG FÜR BANKEN UND DRITTANBIETER

Mit Veröffentlichung der PSD II versucht die EU den Bankenmarkt für Innovationen und Wettbewerb zu öffnen, aber auch gleichzeitig die neuen Drittanbieter zu regulieren. Damit bewegt sich die europäische Bankenwelt verstärkt in Richtung Digitalisierung. Banken und Finanzdienstleister sind angehalten, ihre Geschäftsmodelle an die Anforderungen der PSD II anzupassen und proaktiv Innovationen zu fördern, um die Gunst der Kunden mit neuartigen Produkten und Dienstleistungen zu gewinnen. Ziel sollte es sein, eine digitale Produktplattform als Dreh- und Angelpunkt für alle Finanzangelegenheiten der Kunden aufzubauen. Insbesondere Banken können von dem bereits bestehenden Kundenstamm und den dazugehörigen Daten profitieren.

Banken müssen kurzfristig Ihre digitale Strategie überdenken.

Strong Customer Authentication

Für die Banken wird es besonders wichtig, zumindest bankintern, eine einheitliche Spezifikation für die neu zu schaffenden Schnittstellen zu definieren. Dabei ist ein besonderes Augenmerk auf die Themen Strong Customer Authentication und die möglichen Ausnahmen zu legen. Insbesondere ist zu beachten, dass die Banken weiterhin die Hoheit über die Zugangsdaten der Nutzer haben und sie bereitstellen. Sie müssen sich daher neue Wege für eine Kundenauthentifizierung erarbeiten, die eine sichere Identifizierung über einen Drittanbieter ermöglicht.

Bei den Ausnahmen gilt es abzuwägen, wie man auf das Risiko von möglichen Betrugsfällen aufgrund fehlender Zwei-Faktor-Authentifizierung eingeht. Eine weitere Herausforderung besteht darin, den Kunden die Ausnahmen transparent zu machen, ohne sie zu verwirren.

Für die Banken ergibt sich aber auch ein neues Geschäftsfeld: Sie dürfen selbst als Drittanbieter auf dem Markt auftreten und Kunden eigene Lösungen anbieten. Zudem stellt die PSD II den Banken frei, über individuelle Vereinbarungen weitere entgeltliche Services für Drittanbieter anzubieten.

Schnittstellen

Für Drittanbieter ist die Öffnung des Marktes derzeit am lukrativsten, da sie den Zugang zu den bestehenden Bankensystemen erhalten und die Haftung zunächst auch bei den Banken liegt. Es wird eine Herausforderung sein, die eventuell vielen verschiedenen Schnittstellen anzubinden. Zudem unterliegen sie auch erhöhten Anforderungen für eine Lizenzierung durch die Finanzaufsichtsbehörden. Bereits heute agierende Drittanbieter sind insbesondere durch das Verbot der Nutzung von Screen Scrapping betroffen. Dadurch ist es ihnen nicht mehr möglich, über die Zahlung hinausgehende Kundendaten über das jeweilige Online-Banking-Portal der Banken abzugreifen. Andererseits erhöht die Beschränkung der neuen Schnittstellen auf bestimmte Geschäftszwecke die Kundensicherheit und damit das Vertrauen in die Drittanbieter.

Alexander Bingnet
Client Relationship Manager
+49 69 6696967-415
alexander.bingnet@acando.de

ACANDO GMBH – IHR PARTNER

Um die Anforderungen der PSD II vollständig und fristgerecht umsetzen zu können, müssen die bestehenden IT-Systeme angepasst und neue Schnittstellen und Plattformen geschaffen werden.

Acando hilft Ihnen mit technologieübergreifender Expertise und langjähriger Branchenerfahrung, Ihre PSD II-konforme digitale Strategie zu finden und innovative, zukunftssichere Lösungen zu implementieren.