PSD2 AND OPEN BANKING
THE EUROPEAN REVOLUTION IN BANKING

Why Latest Banking Regulation Matters – For Banks, For Merchants, For You

Stefan Weiß, Head of Banking and Insurance – jambit GmbH
OFFICES IN MUNICH, STUTTGART, LEIPZIG. TECHNOLOGY-INDEPENDENT. ACROSS ALL INDUSTRIES.

KEY FACTS

- Customized software solutions
- Equity-financed company since its foundation in 1999 by Markus Hartinger and Peter F. Fellinger
- 300 top employees
GREAT PLACE TO WORK 2019
3. PLACE IN GERMANY
(251-500 EMPLOYEES)
100% ENTHUSIASM OF RENOWNED CUSTOMERS
CROSS-FUNCTIONAL TEAM

- Software Developers
- Software Architects
- System Architects
- Scrum Master
- Project Manager
- UI/UX Designer
- DevOps
- Tester

BUSINESS MODEL

- Contract for work
- Contract for services
- Agile fixed price
- Teams in jambit offices (Munich, Stuttgart, Leipzig) or on-site on the customer’s premises

RELIABLE PARTNER FOR DIGITIZATION

WE ACCELERATE INNOVATION.
OUR EXPERTISE AND SERVICES

- App & Mobile
- Front-End Development
- Back-End Development
- Internet of Things
- AI & Data Science
- Big Data & Fast Data
- User Centered Design
- Augmented & Virtual Reality
- Platforms & Cloud
INDUSTRY EXPERTISE & COMPETENCE CENTERS

AUTOMOTIVE

MEDIA

BANKING & INSURANCE

NEW BUSINESS

PLATFORMS & OPERATIONS
Planning, rollout, testing and operation of demanding IT platforms, IT security, cloud hosting

USER CENTERED DESIGN
Full-service graphics department, multi-platform design, best user experiences
REVOLUTION?
## WHAT HAPPENED BEFORE ...

<table>
<thead>
<tr>
<th>First, let's introduce the Payment Services Directive (PSD)</th>
<th>New players and services needed to be regulated</th>
<th>Towards an increasingly integrated EU single market</th>
</tr>
</thead>
<tbody>
<tr>
<td>The PSD was adopted in 2007. It created a single market for payments (essentially credit transfers, direct debits, cards) in the European Union. It provided the legal foundation for a Single Euro Payments Area (SEPA).</td>
<td>Since the PSD, the digitalisation of the European economy has steadily progressed. <strong>New services</strong>, provided by <strong>new players</strong>, have appeared for online payments. <strong>Problem</strong>: they were outside the scope of PSD, and therefore not regulated at EU level. An update of PSD was needed.</td>
<td>The objectives of PSD2 are to make payments safer, increase the consumers’ protection, foster innovation and competition while ensuring a level playing field for all players, including new ones.</td>
</tr>
</tbody>
</table>

15. September 2019
PSD2 INTRODUCES NEW RULES FOR PARTIES INVOLVED IN PAYMENTS (AND A LOT OF TLAS)

- PSD2 contains 117 articles that were turned into national law and there are more rules and details in RTSs and EBA Guidelines.
- A key novelty is XS2A

New players will now be registered, licensed, and regulated at EU level. Barriers will be removed for these companies, therefore increasing competition, which should translate into lower costs for customers. These new players will access the customers' payment account (that's the 'XS2A' - access to account) to make payments on their behalf (via credit transfers) and to provide them an overview of their various payment accounts. Obviously only with the prior consent of the customers!
WHO ARE THE INVOLVED PARTIES?

**Account Servicing Payment Service Providers (ASPSP)**
They provide and maintain payment accounts for customers.

**Payment Service Users (PSU)**
They make and/or receive payments. Can be either natural or legal persons. They interact as customers with all these organisations.
WHO ARE THE INVOLVED PARTIES?

**Account Servicing Payment Service Providers (ASPSP)**
- They provide and maintain payment accounts for customers.

**Third Party Payment Service Providers (TPP)**
- Introduced in PSD2. They are Payment institutions which don’t hold payment accounts for their customers, and have therefore a more limited scope of activities.

**Payment Service Users (PSU)**
- They make and/or receive payments. Can be either natural or legal persons. They interact as customers with all these organisations.
WHO ARE THE INVOLVED PARTIES?

**Account Servicing Payment Service Providers (ASPSP)**
They provide and maintain payment accounts for customers.

**Account Information Service Providers (AISP)**
They aggregate online information for multiple payment accounts and offer customers a global view of their daily finances, in a single place, in order to help them better manage them.

**Payment Initiation Service Providers (PISP)**
They facilitate the use of online banking to make a payment (which offers an alternative to the use of cards).

**Payment Service Users (PSU)**
They make and/or receive payments. Can be either natural or legal persons. They interact as customers with all these organisations.
USE CASE ACCOUNT AGGREGATION

Useful for personal financial planning, tax declaration, loan application ...
USE CASE PSD2 PAYMENT

Cheaper and more secure than card payment or direct debit ...

WHERE INNOVATION WORKS | 18
EUROPE IS LEADER IN A GLOBAL OPEN BANKING MOVEMENT

**Canada:** Public Consultation on metrics of open banking following the PSD2 regulation in EU

**US:** data sharing deals with partners. First Open Banking suggestions by industry bodys with alternatives to screen scraping emerge

**EU / UK:** PSD2 and UK Open Banking Initiative forces banks to open up their data with the aim to create an industry standard

**China:** new digital financial ecosystems emerge without any regulatory mandates

**South-east Asia:** Wide use of Open APIs and data sharing within the ecosystem

**Australia:** First regulatory framework for open banking leaned on UK Open Banking Standard

**Africa:** first API banking use cases and persecution of European PSD2 progress
OPEN BANKING? MY ACCOUNT, OPEN FOR EVERYBODY?
PSD2 IS ABOUT CUSTOMER EMPOWERMENT, SECURITY AND INNOVATION

- My account
- My data
- My money
- My choice

PSD2 creates more *options*, more competition, more innovation in a more secure way.
ALL INVOLVED PARTIES NEED LICENSES + AUDITS NOW

**Account Servicing Payment Service Providers (ASPSP)**
They provide and maintain payment accounts for customers.

**Account Information Service Providers (AISP)**
They aggregate online information for multiple payment accounts and offer customers a global view of their daily finances, in a single place, in order to help them better manage them.

**Payment Initiation Service Providers (PISP)**
They facilitate the use of online banking to make a payment (which offers an alternative to the use of cards).

**Payment Service Users (PSU)**
They make and/or receive payments. Can be either natural or legal persons. They interact as customers with all these organisations.
STRONG CUSTOMER AUTHENTICATION (SCA)

Increased security of Internet payments using SCA, reducing fraud by using $\geq 2$ authentication factors out of 3 categories (2FA)

- **Knowledge**: Something only the user knows (password, PIN...).
- **Possession**: Something only the user possesses (key material...).
- **Inherence**: Something the user is (fingerprint, voice recognition...).
EXAMPLES OF ...

### Knowledge

<table>
<thead>
<tr>
<th>Element</th>
<th>Compliant with SCA?*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Yes</td>
</tr>
<tr>
<td>PIN</td>
<td>Yes</td>
</tr>
<tr>
<td>Knowledge-based challenge questions</td>
<td>Yes</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Yes</td>
</tr>
<tr>
<td>Memorised swiping path</td>
<td>Yes</td>
</tr>
<tr>
<td>Email address or user name</td>
<td>No</td>
</tr>
<tr>
<td>Card details (printed on the card)</td>
<td>No</td>
</tr>
<tr>
<td>OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)</td>
<td>No (for approaches currently observed in the market)</td>
</tr>
<tr>
<td>Printed matrix card or OTP list</td>
<td>No</td>
</tr>
</tbody>
</table>

*Compliance with SCA requirements is dependent on the specific approach used in the implementation of the element.

### Possession

<table>
<thead>
<tr>
<th>Element</th>
<th>Compliant with SCA?*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)</td>
<td>Yes</td>
</tr>
<tr>
<td>Possession of a device evidenced by a signature generated by a device (hardware or software token)</td>
<td>Yes</td>
</tr>
<tr>
<td>Card or device evidenced through a QR code (or photo TAN) scanned from an external device</td>
<td>Yes</td>
</tr>
<tr>
<td>App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device</td>
<td>Yes</td>
</tr>
<tr>
<td>Card evidenced by a card reader</td>
<td>Yes</td>
</tr>
<tr>
<td>Card with possession evidenced by a dynamic card security code</td>
<td>Yes</td>
</tr>
<tr>
<td>App installed on the device</td>
<td>No</td>
</tr>
<tr>
<td>Card with possession evidenced by card details (printed on the card)</td>
<td>No (for approaches currently observed in the market)</td>
</tr>
</tbody>
</table>

*Compliance with SCA requirements is dependent on the specific approaches used in the implementation of the elements.

### Inheritance

<table>
<thead>
<tr>
<th>Element</th>
<th>Compliant with SCA?*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint scanning</td>
<td>Yes</td>
</tr>
<tr>
<td>Voice recognition</td>
<td>Yes</td>
</tr>
<tr>
<td>Vain recognition</td>
<td>Yes</td>
</tr>
<tr>
<td>Hand and face geometry</td>
<td>Yes</td>
</tr>
<tr>
<td>Retina and iris scanning</td>
<td>Yes</td>
</tr>
<tr>
<td>Keystroke dynamics</td>
<td>Yes</td>
</tr>
<tr>
<td>Heart rate or other bodily movement pattern identifying that the PSU is the PSU (e.g, for wearable devices)</td>
<td>Yes</td>
</tr>
<tr>
<td>The angle at which the device is held</td>
<td>Yes</td>
</tr>
<tr>
<td>Information transmitted using a communication protocol, such as EMV® 3-D Secure</td>
<td>No (for approaches currently observed in the market)</td>
</tr>
<tr>
<td>Memorised swiping path</td>
<td>No</td>
</tr>
</tbody>
</table>

*Compliance with SCA requirements is dependent on the specific approaches used in the implementation of the elements.
WHEN IS SCA REQUIRED?

- **When users consult their payment account, or an aggregated view of their payment accounts, using an additional service.**
  - The 1st time the account (or aggregated view) is consulted.
  - At least every 90 days.

- **Each time the user makes a payment, except in certain situations (exemptions), such as:**
  - Below a certain amount.
  - If the beneficiary is already identified.
  - and many more ...
CUSTOMER AUTHENTICATION AND CUSTOMER CONSENT

WHERE INNOVATION WORKS | 26

NO CONSENT, NO TEA!

(google it)
APIS FOR STANDARDIZED DATA EXCHANGE

The institution holding the payment account of the customer provides to these new players access to the account, for example via an Application Programming Interface (API). It can be viewed as a messenger enabling information exchanges, taking a request from the new player, and returning an answer.
SO EVERYBODY IS HAPPY NOW?
NEH, ...

Account Servicing Payment Service Providers

They provide and maintain payment accounts for customers.
Banks may see PSD2 as a threat ...
PSD2 AND OPEN BANKING

Fintechs are starting to eat away profitable parts of the business

Unbundling of a Bank
PSD2 AND OPEN BANKING

Global brands make people forget with whom they bank
Vergleichsportal

Check24 buhlt um eigene Banklizenz

Das Vergleichsportal Check24 macht sich weiter bei Finanzdienstleistungen breit und hat nun eine Banklizenz beantragt. So könnten künftig über Check24 mit Negativzinsen.

Check24 will auch eine Bank sein

Stand: 06.09.2019, 08:35 Uhr

Das durch reichlich Werbung bekannt gewordene Vergleichsportal Check24 will weiter expandieren. Das Münchener Unternehmen, das meist Gas- oder Stromverträge, Handykontrakte oder Reisen vermittelt, strebt nun auch ins Bankgeschäft.

Zu diesem Zweck wurde jetzt bei der Aufsichtsbehörde BaFin eine Banklizenz beantragt. Zwar vermittelt Check24 bereits über Partner klassische Bankprodukte wie Ratenkredite oder andere
# STATUS OF PSD2 API IMPLEMENTATION (OKTOBER 2019)

<table>
<thead>
<tr>
<th>Country</th>
<th>Unavailable</th>
<th>Not functional</th>
<th>Functional</th>
<th>Operational</th>
<th>Ready</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>33%</td>
<td>50%</td>
<td>0%</td>
<td>17%</td>
<td>0%</td>
</tr>
<tr>
<td>Belgium</td>
<td>22%</td>
<td>44%</td>
<td>22%</td>
<td>11%</td>
<td>0%</td>
</tr>
<tr>
<td>Denmark</td>
<td>40%</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>0%</td>
</tr>
<tr>
<td>Finland</td>
<td>57%</td>
<td>29%</td>
<td>0%</td>
<td>14%</td>
<td>0%</td>
</tr>
<tr>
<td>France</td>
<td>30%</td>
<td>40%</td>
<td>20%</td>
<td>10%</td>
<td>0%</td>
</tr>
<tr>
<td>Germany</td>
<td>25%</td>
<td>58%</td>
<td>17%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Italy</td>
<td>40%</td>
<td>40%</td>
<td>0%</td>
<td>20%</td>
<td>0%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>33%</td>
<td>33%</td>
<td>17%</td>
<td>17%</td>
<td>0%</td>
</tr>
<tr>
<td>Norway</td>
<td>50%</td>
<td>25%</td>
<td>0%</td>
<td>25%</td>
<td>0%</td>
</tr>
<tr>
<td>Portugal</td>
<td>0%</td>
<td>26%</td>
<td>47%</td>
<td>26%</td>
<td>0%</td>
</tr>
<tr>
<td>Spain</td>
<td>7%</td>
<td>40%</td>
<td>40%</td>
<td>13%</td>
<td>0%</td>
</tr>
<tr>
<td>Sweden</td>
<td>40%</td>
<td>27%</td>
<td>27%</td>
<td>7%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>26%</td>
<td>36%</td>
<td>23%</td>
<td>15%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Source: Tink Research, 2019 (data retrieved August 15, 2019)

### Legend

- **PSD2 API Ready = 0%**
  These PSD2 APIs meet the requirements and obligations to be compliant.

- **PSD2 API Operational = 15%**
  These APIs meet the requirements for an access interface but not all requirements to be compliant.

- **PSD2 API Functional = 23%**
  These PSD2 APIs support basic functions but not all requirements for being operational.

- **PSD2 API Not functional = 36%**
  These PSD2 APIs present significant obstacles.

- **PSD2 API Unavailable = 26%**
  These PSD2 APIs have not been published or remain unavailable even after contacting support.
## HOW BANKS PUT THIS „TO WORK“: 2FA

<table>
<thead>
<tr>
<th>Bank</th>
<th>App</th>
<th>Photo-Tan</th>
<th>Chip-TAN</th>
<th>mTAN</th>
<th>Default Weg?</th>
<th>Kosten mTAN</th>
<th>wie oft 2FA?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deutsche</td>
<td>ja</td>
<td>ja</td>
<td>nein***</td>
<td>ja</td>
<td>photoTAN App</td>
<td>Auftrag 9 Cent</td>
<td>„ewig“ mit Geräte-Bindung ****</td>
</tr>
<tr>
<td>Commerzbank</td>
<td>ja</td>
<td>ja</td>
<td>nein</td>
<td>ja</td>
<td>photoTAN push</td>
<td>Auftrag 12 Cent</td>
<td>App: 90 Tage</td>
</tr>
<tr>
<td>ING</td>
<td>ja</td>
<td>ja</td>
<td>nein</td>
<td>ja</td>
<td>App</td>
<td>keine</td>
<td>jedes Login</td>
</tr>
<tr>
<td>Volksbanken *</td>
<td>ja</td>
<td>ja</td>
<td>ja</td>
<td>ja</td>
<td>nein</td>
<td>variabel</td>
<td>90 Tage</td>
</tr>
<tr>
<td>Sparkassen *</td>
<td>ja</td>
<td>nein</td>
<td>ja</td>
<td>ja</td>
<td>nein</td>
<td>variabel</td>
<td>90 Tage</td>
</tr>
<tr>
<td>N26</td>
<td>ja</td>
<td>nein</td>
<td>nein</td>
<td>nein</td>
<td>nein</td>
<td>nicht angeboten</td>
<td>jedes Login</td>
</tr>
<tr>
<td>Postbank</td>
<td>ja</td>
<td>nein</td>
<td>ja</td>
<td>nein, aber App dominiert</td>
<td>nein, aber App dominiert</td>
<td>nicht (mehr) angeboten</td>
<td>jedes Login</td>
</tr>
<tr>
<td>HVB</td>
<td>ja</td>
<td>ja</td>
<td>nein</td>
<td>ja</td>
<td>nein, App dominiert</td>
<td>keine</td>
<td>„risiko-basiert“</td>
</tr>
<tr>
<td>Santander</td>
<td>ja</td>
<td>nein</td>
<td>nein</td>
<td>ja</td>
<td>App</td>
<td>keine</td>
<td>90 Tage</td>
</tr>
<tr>
<td>Comdirect</td>
<td>ja</td>
<td>ja</td>
<td>nein</td>
<td>ja</td>
<td>Photo</td>
<td>Auftrag 9 Cent</td>
<td>90 Tage + individuell</td>
</tr>
<tr>
<td>Targobank</td>
<td>ja</td>
<td>ja</td>
<td>nein</td>
<td>ja</td>
<td>nein, App dominiert</td>
<td>keine</td>
<td>jedes Login</td>
</tr>
<tr>
<td>DKB</td>
<td>ja</td>
<td>nein</td>
<td>ja</td>
<td>ja</td>
<td>nein, App dominiert</td>
<td>Auftrag 7 Cent **</td>
<td>jedes Login</td>
</tr>
</tbody>
</table>

Quelle: https://www.finanz-szene.de/digital-banking/die-psd2-strategien-aller-grossen-deutschen-banken/
2-FACTOR AUTHENTICATION MADNESS?!
SOME OF THE APPARENT PROBLEMS

- Customers without smart phones may be excluded or punished with high fees.
- Customers may be confused about when to use what factor. This makes them vulnerable to fraud, in particular phishing.
- Fintechs and account aggregation services must include a plethora of different authentication types and exemption implementation. This is both a technical and a UI/UX challenge.
  This is not OPEN Banking!
- Credit card payments: as e-merchants/PSP change to new standards customers will experience different flows in different shops.
KLINGELN LASSEN
Das Gerät klingelt fünf Minuten lang, selbst wenn es auf "Lautlos" gestellt wurde.

GERÄT SPERRN

DATEN VON GERÄT LÖSCHEN
WIN WITH UX

Top Design
Smooth Processes
Full Digital Speed
Omnichannel
Gamification
Smart Use Of
Biometrics, Voice and AI
WIN WITH RELEVANT CONTENT

Relevant To Customers’ Lifes
Data driven (PSD2 helps)
Contextual
Authentic
Cross Selling / Up Selling
Own offerings
Partner offerings

www.accenture.com/everydaybank
NEOBANKS LEAD THE GAME, INCUMBENTS FOLLOW
FRAGEN?

-> .net core, C# Backend Devs gesucht! <-

-> Java Backend, Angular/React Frontend Devs gesucht! <-

-> AWS / Azure Cloud Architecs, DevOps gesucht  <-

Stefan Weiß, MBA
@weiss2go
stefan.weiss@jambit.com