PSD2 AND OPEN BANKING

THE EUROPEAN REVOLUTION IN BANKING

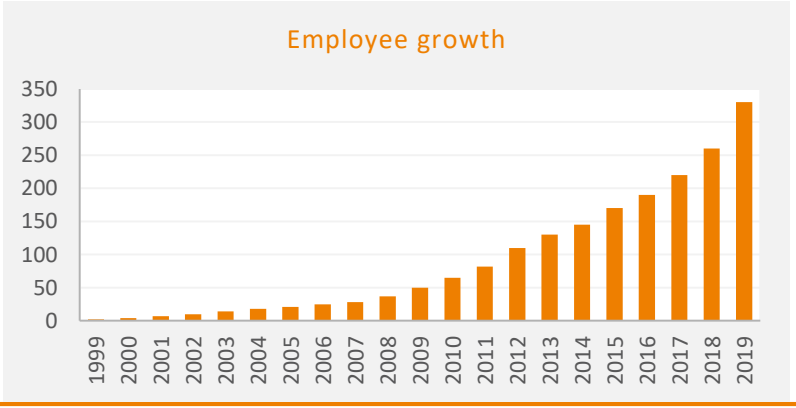
Why Latest Banking Regulation Matters – For Banks, For Merchants, For You

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)

Great Place To Work.®
2019
Beste Arbeitgeber™
Deutschland

Photo: Great Place to Work©

Photo: Great Place to Work

Photo: Great Place to Work©

100 % ENTHUSIASM OF RENOWNED CUSTOMERS

RELIABLE PARTNER FOR DIGITIZATION

WE ACCELERATE INNOVATION.

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

Foto: Rainer Viertlböck

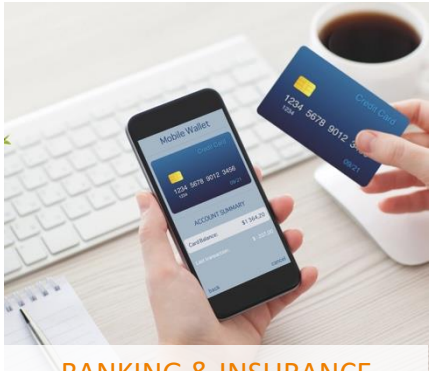
OUR EXPERTISE AND SERVICES

- 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 …

First, let's introduce the Payment Services Directive (PSD)

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).

New players and services needed to be regulated

Since the PSD, the digitalisation of the European economy has steadily progressed. New services, provided by new players, have appeared for online payments. Problem: they were outside the scope of PSD, and therefore not regulated at EU level. An update of PSD was needed.

Towards an increasingly integrated EU single market

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.

▶ 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!

PSD II – PAYMENT SERVICES DIRECTIVE II

RTS – REGULATORY TECHNICHAL STANDARDS

XS2A – ACCES

SCA - STRONG

ASPSP - ACCO

PSU - PAYME

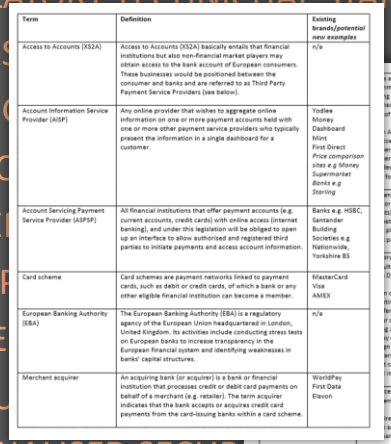
TPP - THIRD P

PISP - PAYME

AISP - ACCOU

PSC - PERSONALISED SECUR

…



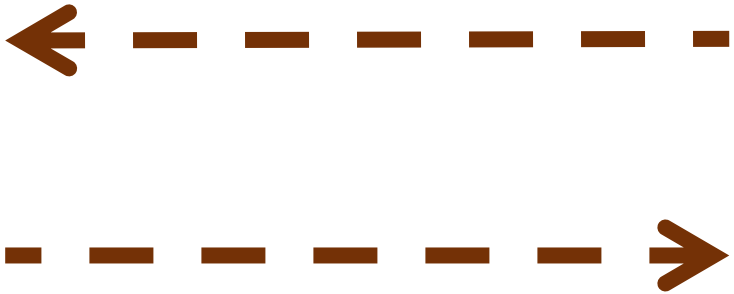
Term	Definition	Existing brands/*potential new examples*
Access to Accounts (XS2A)	Access to Accounts (XS2A) basically entails that financial institutions but also non-financial market players may obtain access to the bank account of European consumers. These businesses would be positioned between the consumer and banks and are referred to as Third Party Payment Service Providers (see below).	n/a
Account Information Service Provider (AISP)	Any online provider that wishes to aggregate online information on one or more payment accounts held with one or more other payment service providers who typically present the information in a single dashboard for a customer.	Yodlee Money Dashboard Mint First Direct *Price comparison sites e.g Money Supermarket* *Banks e.g Starling*
Account Servicing Payment Service Provider (ASPSP)	All financial institutions that offer payment accounts (e.g. current accounts, credit cards) with online access (internet banking), and under this legislation will be obliged to open up an interface to allow authorised and registered third parties to initiate payments and access account information.	Banks e.g. HSBC, Santander Building Societies e.g Nationwide, Yorkshire BS
Card scheme	Card schemes are payment networks linked to payment cards, such as debit or credit cards, of which a bank or any other eligible financial institution can become a member.	MasterCard Visa AMEX
European Banking Authority (EBA)	The European Banking Authority (EBA) is a regulatory agency of the European Union headquartered in London, United Kingdom. Its activities include conducting stress tests on European banks to increase transparency in the European financial system and identifying weaknesses in banks' capital structures.	n/a
Merchant acquirer	An acquiring bank (or acquirer) is a bank or financial institution that processes credit or debit card payments on behalf of a merchant (e.g. retailer). The term acquirer indicates that the bank accepts or acquires credit card payments from the card-issuing banks within a card scheme.	WorldPay First Data Elavon

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?

TPP

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

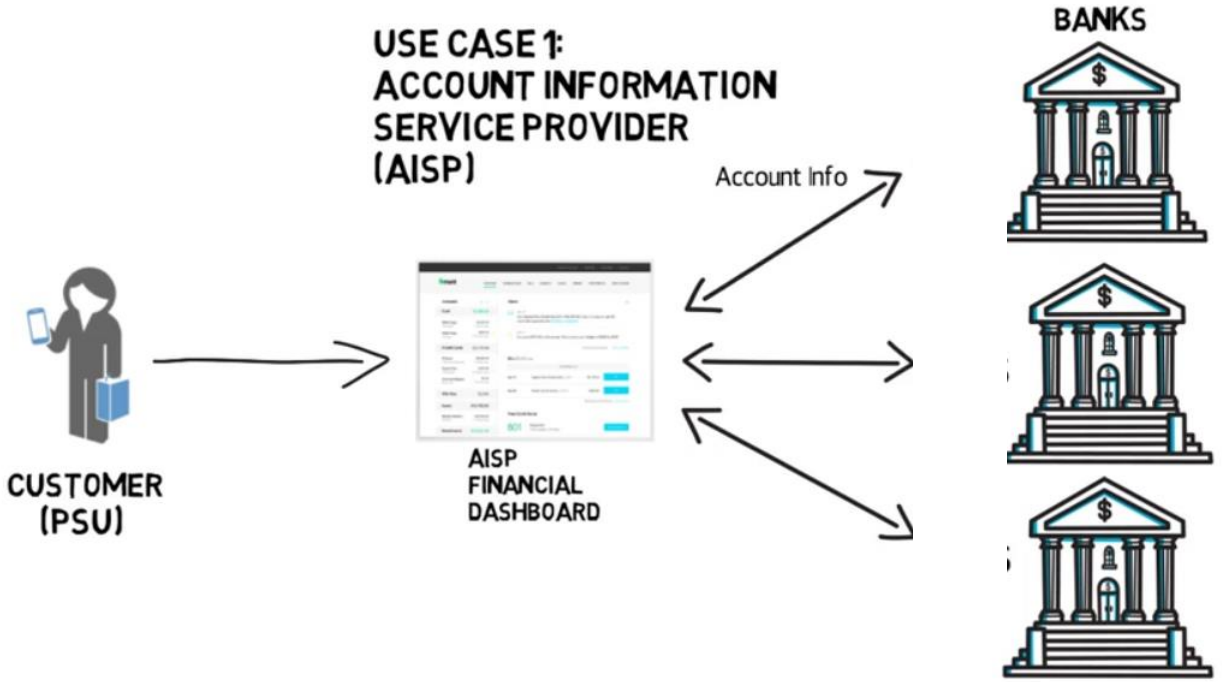
PSU

They make and/or receive payments. Can be either natural or legal persons. They interact as customers with all these organisations.

CBPIISP/PIISP/CISP
Card Based Payment Instrument Issuing Service Provider

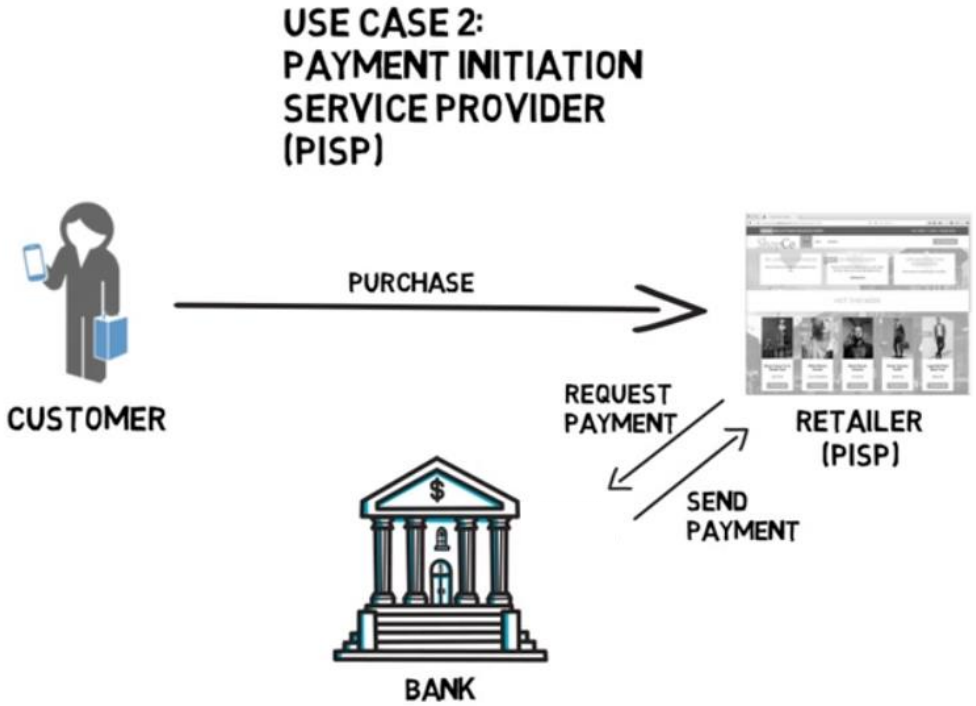
USE CASE ACCOUNT AGGREGATION

Useful for personal financial planning, tax declaration, loan application …

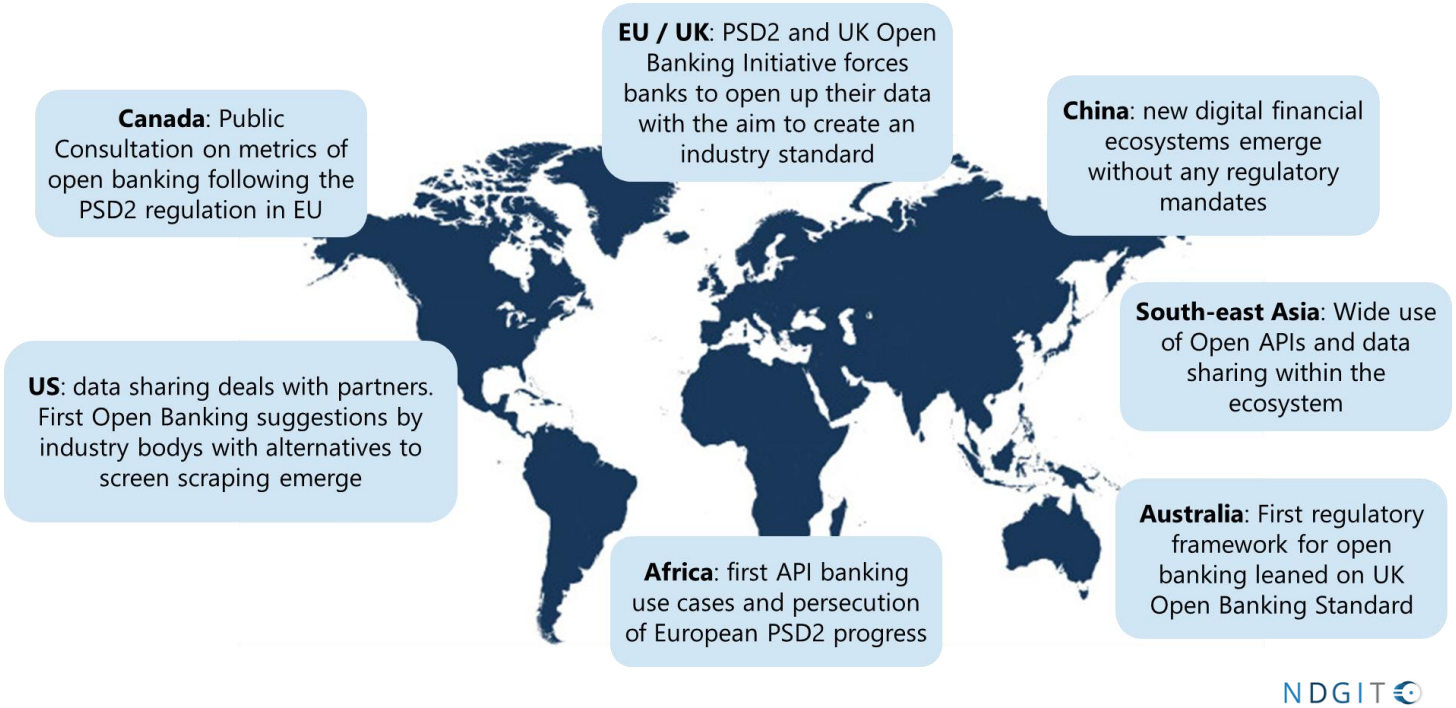


USE CASE PSD2 PAYMENT

Cheaper and more secure than card payment or direct debit …



EUROPE IS LEADER IN A GLOBAL OPEN BANKING MOVEMENT



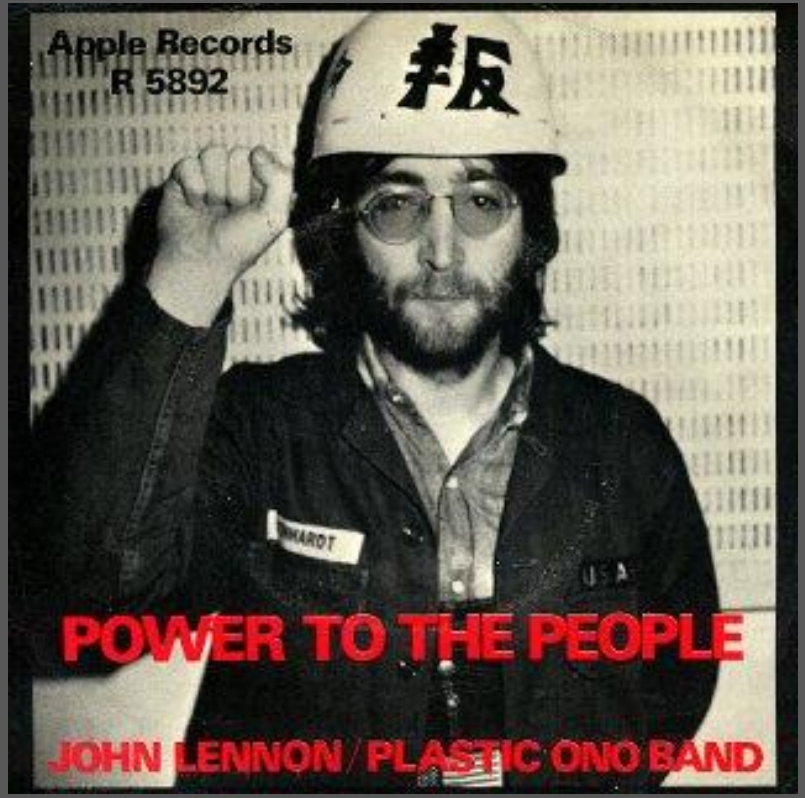
NDGIT

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

TPP

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).

CBPIISP/**PIISP**/CISP

Card Based Payment Instrument Issuing Service Provider

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 >=**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 | Possession | Inherence

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

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

Table 2 — Non-exhaustive list of possible possession elements

Element	Compliant with SCA?*
Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	Yes
Possession of a device evidenced by a signature generated by a device (hardware or software token)	Yes
Card or device evidenced through a QR code (or photo TAN) scanned from an external device	Yes
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	Yes
Card evidenced by a card reader	Yes
Card with possession evidenced by a dynamic card security code	Yes
App installed on the device	No
Card with possession evidenced by card details (printed on the card)	No (for approaches curre observed in the marl
Card with possession evidenced by a printed element (such as an OTP list)	No (for approaches curre observed in the marl

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

Table 1 — Non-exhaustive list of possible inherence elements

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

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.

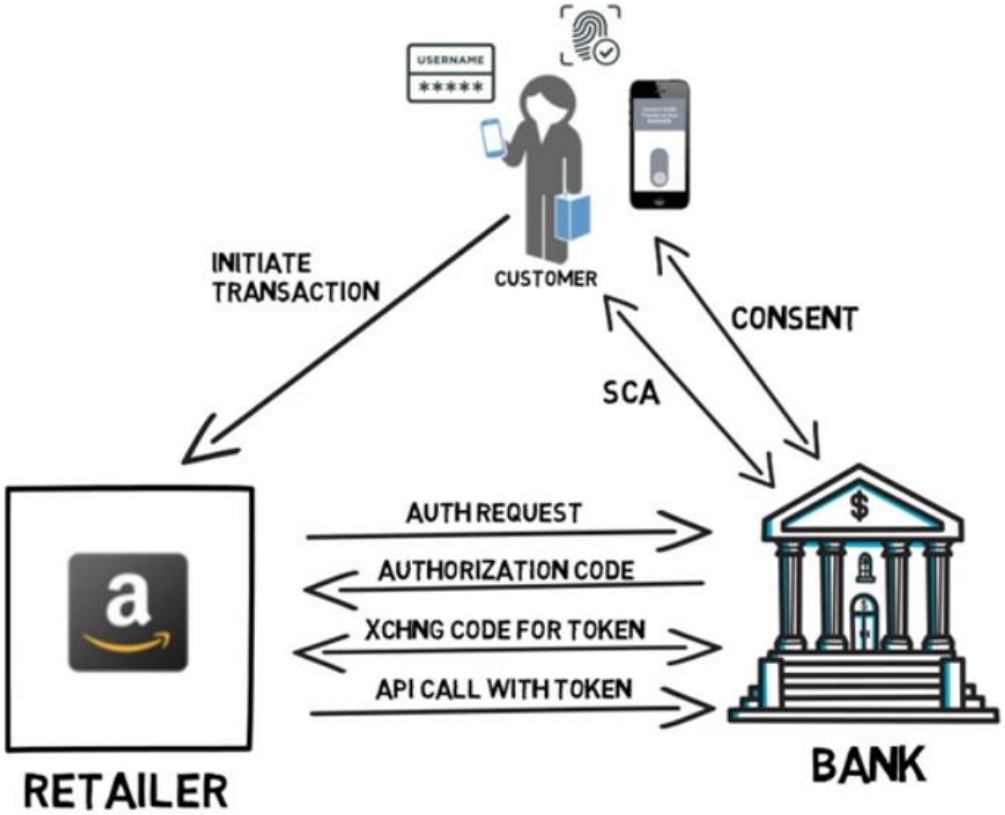
- Each time the user makes a payment, except in certain situations (exemptions), such as:

Below a certain amount.

If the beneficiary is already identified.

and many more ...

CUSTOMER AUTHENTICATION AND CUSTOMER CONSENT



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

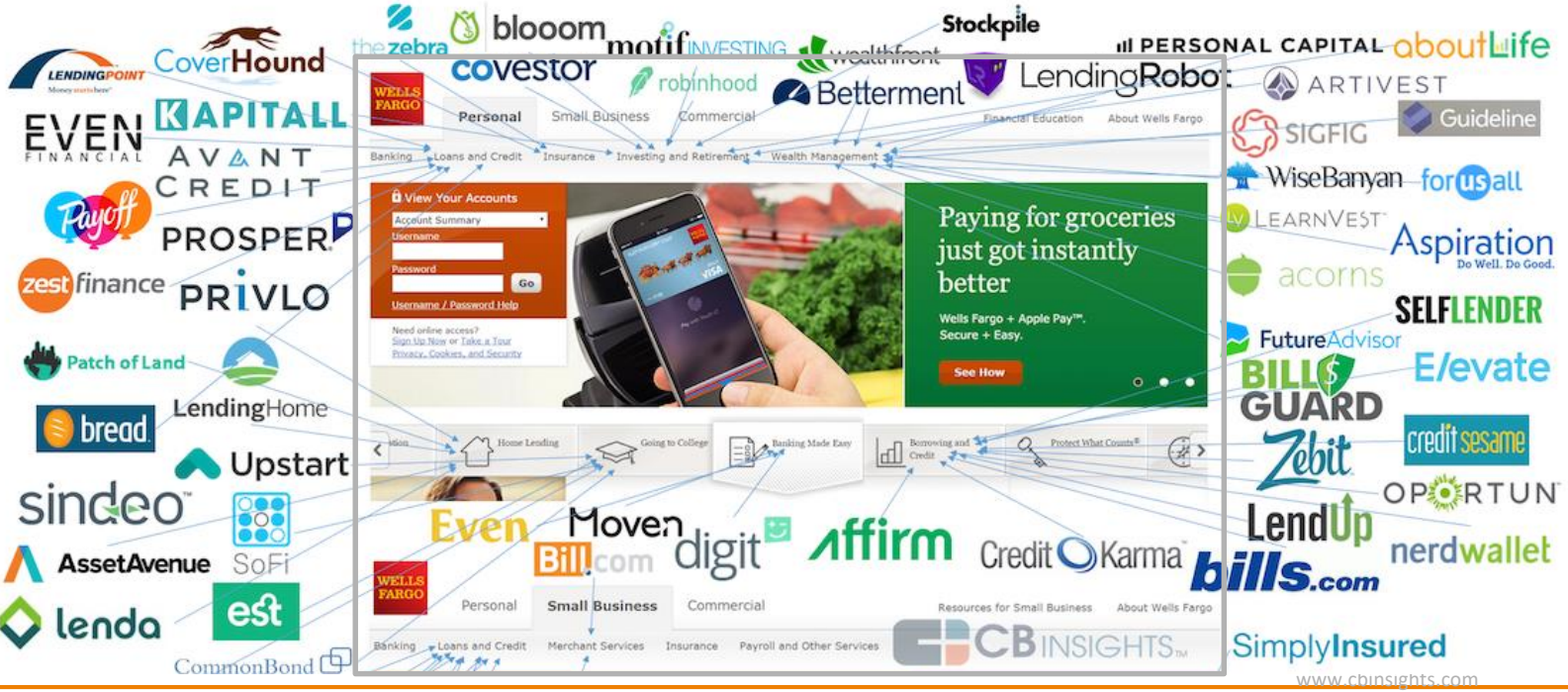
ASPSP

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



PSD2 AND OPEN BANKING

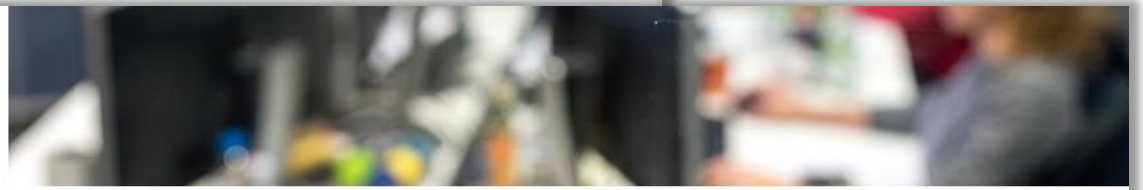
Global brands make people **forget with whom they bank**

CHECK24 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 übe mit Negativzins.



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, Handykontrake 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)

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

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 PSD2s 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

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

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

Verlorenes Android-Gerät orten | Mein Gerät suchen | Fundservice: Verlust online mel | Posteingang (8) - weiss100g@g | Neuehrenfeld - Google Maps

https://www.google.com/android/find?hl=de&u=0 120%

Cal | Principles | Jambit | AI School | DSGVO | Geld | Links | Crypto | Python | Electronic library. Dow... | Rubber Guns | Fidor

Google Mein Gerät finden

Motorola Moto G (5S) Pl

Gerät nicht erreichbar

LIDL Connect

82%

KLINGELN LASSEN

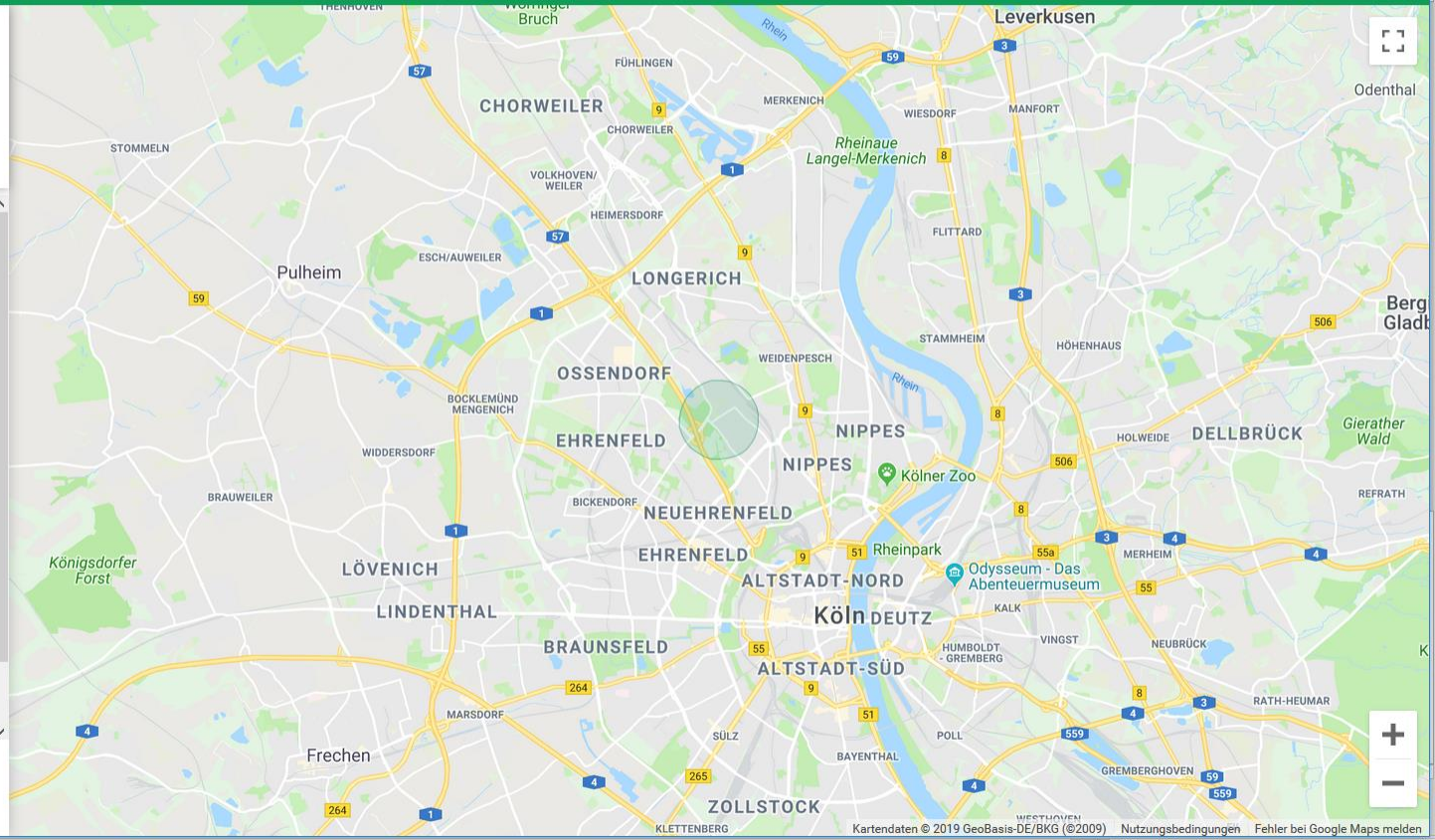
Das Gerät klingelt fünf Minuten lang, selbst wenn es auf "Lautlos" gestellt wurde.

GERÄT SPERREN

Das Gerät wird gesperrt und aus dem Google-Konto abgemeldet. Du kannst eine Telefonnummer oder eine Nachricht auf dem Sperrbildschirm deines Geräts anzeigen lassen. Nach dem Sperren kannst du das Gerät weiterhin orten.

DATEN VON GERÄT LÖSCHEN

Sämtliche Inhalte auf diesem Gerät werden gelöscht. Nach dem Löschen der Inhalte kannst du das Gerät nicht mehr orten.



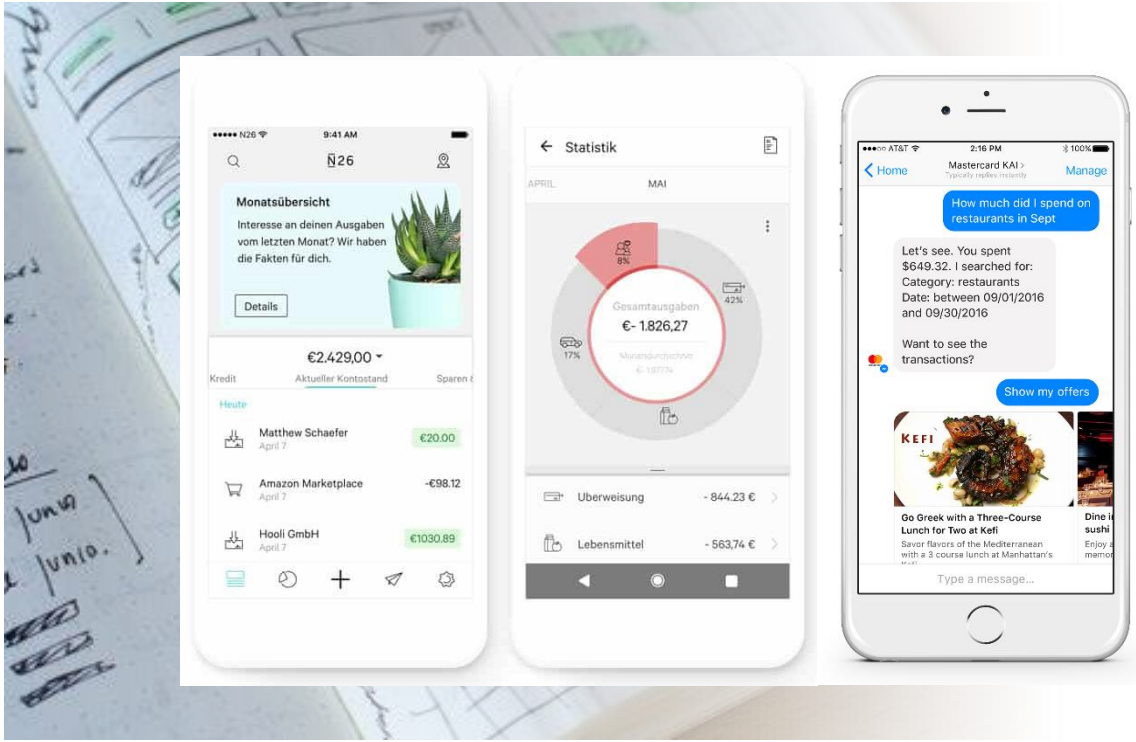
Folie 2 von 2 | Deutsch (Deutschland) | Notizen | 110 %

Zur Suche Text hier eingeben

DEU 11:43 01.10.2019


jambit

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

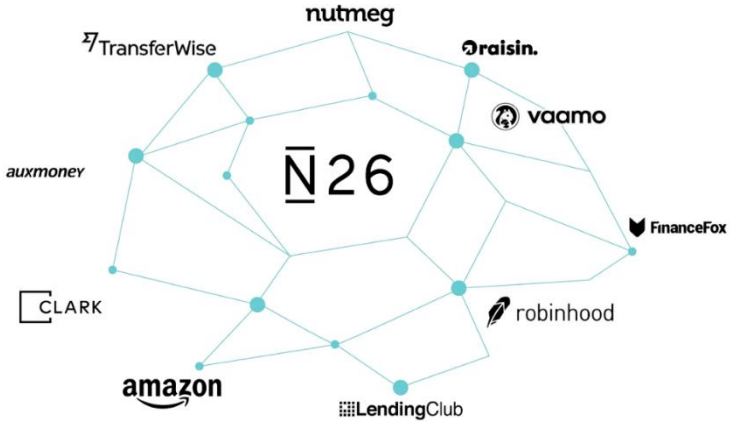
Data driven (PSD2 helps) Contextual Authentic

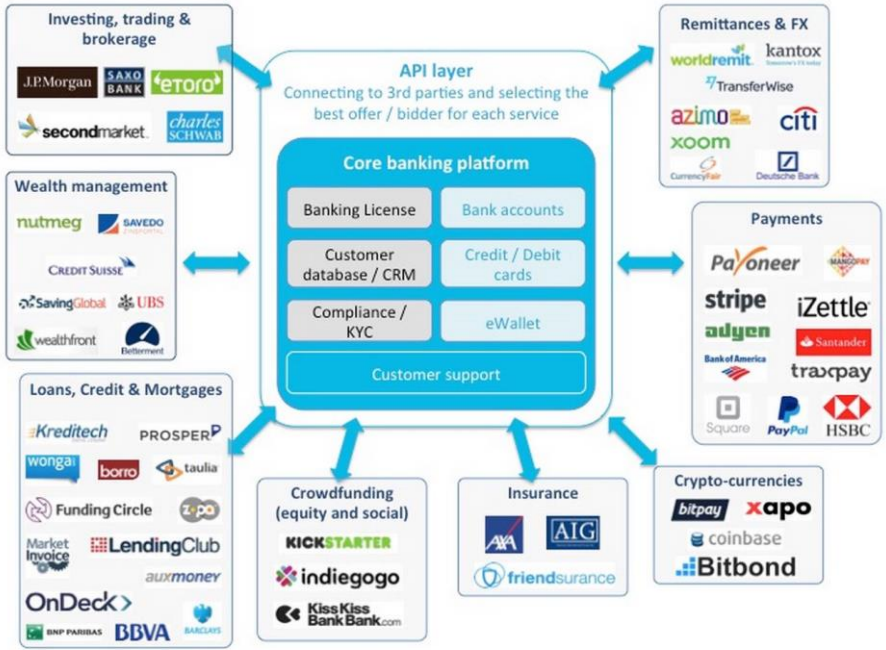
Cross Selling / Up Selling

Own offerings Partner offerings

www.accenture.com/everydaybank

NEOBANKS LEAD THE GAME, INCUMBENTS FOLLOW





jambit
WHERE INNOVATION WORKS

Great Place To Work. 2019 Beste Arbeitgeber™ Deutschland

SOFTWARE & SYSTEM DEVELOPER
INNOVATION PARTNER
COFFEE LOVER

Geschäftsführer:
Peter F. Fellinger, Markus Hartinger

Erika-Mann-Straße 63 | 80636 München | +49.89.45 23 47 - 0
Meitnerstraße 8 | 70563 Stuttgart | +49.711.21 95 28 - 0
Klostergasse 3 | 04109 Leipzig | +49.341.22 178 - 0

office@jambit.com
www.jambit.com

Dieses Dokument ist vertraulich. Eine Weitergabe an Dritte ist nur mit Zustimmung von jambit möglich.

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