

Open Banking: advancing customer-centricity

Analysis and overview

Open Banking Working Group

CONTENTS

Executive summary	4
1. Introduction	7
2. Customer control through the customer's eyes	9
3. Open Banking as the basis for customer control	16
3.1 Open Banking revisited	16
3.2 Customer requirements and regulation as a key driver	17
3.3 API technology as enabler	20
3.4 Digital identity: key asset defining user experience from a customer control point of view	21
4. Strategic implications of customer control through Open Banking	25
4.1 Open Banking: pivot for product creation and distribution	25
4.2 Product impact through APIs	26
4.3 Distribution impact through APIs	26
4.4 Four platformisation levels of Open Banking in the financial value chain	27
Appendix: Glossary	30

Copyright © 2017 Euro Banking Association (EBA)

All rights reserved. Brief excerpts may be reproduced for non-commercial purposes, with an acknowledgement of the source.

The information contained in this document is provided for information purposes only and should not be construed as professional advice.

The information paper is the result of an analysis carried out by the Open Banking Working Group and Innopay.

The EBA does not accept any liability whatsoever arising from any alleged consequences or damages arising from the use or application of the information and give no warranties of any kind in relation to the information provided.

FIGURES AND PICTURES

Figure 1: Transition from a product-centric to a customer-centric approach	4/9
Figure 2: Three key dimensions of Open Banking	16
Figure 3: Overview customer requirements 'Reach', 'Conversion' and 'Cost'	17
Figure 4: The services ('Fintech') layer on top of the infrastructure layer	18
Figure 5: Open Banking Platform Model	21
Figure 6: Three aspects of digital identity: identification, authentication and authorisation	22
Figure 7: RTS requirements for interaction scope XS2A	24
Figure 8: APIs are the pivot between products and distribution	25
Figure 9: Four platformisation levels of Open Banking	27
Figure 10: High-level impact assessment platformisation levels of Open Banking	29

EXECUTIVE SUMMARY

The power of putting customers at the centre of the corporate business strategy has been a well-known concept for decades. Many organisations across various industries have followed such a customer-centric approach to differentiate themselves and build a competitive advantage. However, in the digital era the customer-centric approach evolves to the next level, in particular, with regard to customers' financial assets, personal data and digital service experiences and service options.

As a result of accelerating digitisation, the next level of customer-centricity allows both private and business customers to move from being only the focal point ('customer-centricity 1.0') to being increasingly in control of the product/proposition and channel dimension of their financial services (customer-centricity 2.0). Customers will be able to more effectively manage their financial assets and data based on their specific needs and anytime, anywhere, on any device (ATAWAD). This transition is depicted in the figure below.

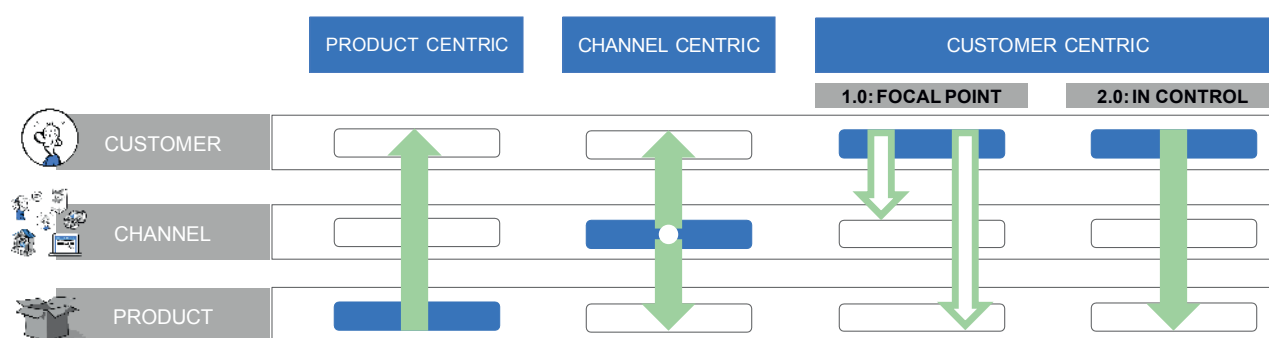


Figure 1: Transition from a product-centric to a customer-centric approach

For banks this next level customer-centric approach manifests itself in the rise of the Open Banking¹ development, in which banks have the opportunity to work in a scalable fashion with innovative technologies and players, resulting from the rising Fintech movement. This major trend opens up avenues to put customers more in control as to what 1) products and services they consume (product perspective) in relation to their bank accounts and 2) from which service providers they wish to buy the respective product or service (distribution perspective).

Putting customers 'in control' can mean different things, essentially, it reflects a response to customer's desires to operate in an increasingly connected digital ecosystem. For the financial world, this can mean:

- ▶ Connect third party apps directly to a bank account and vice versa, e.g. for initiation of payments,
- ▶ Connect bank account data to apps, e.g. for financial planning and lending,
- ▶ Login (identification and authentication) at third party websites (public and private) with existing banking credentials,
- ▶ Share personal attributes (e.g. name, age, email address) with third party websites after authorisation with existing banking credentials.

¹ Open Banking: Evolution of banking, leading to more transparency, customer choice and customer control over personal data (EBA information paper May 2015 '[Understanding the business relevance of Open APIs and Open Banking for banks](#)')

The Open Banking business model provides banks with an opportunity to respond to this demand for ‘customer in control’ value propositions. Other drivers of Open Banking include the push by regulators for more openness in banking through the revised Payment Services Directive (PSD2) provisions on “access to account” (XS2A) and the General Data Protection Regulation (GDPR, coming into effect May 2018) alongside the rapid extension of the use of Open API (‘Application Programming Interfaces’) technology in the financial services domain.

PSD2 will enable private and business customers to connect third party services to their payment accounts upon their explicit consent, allowing for payment initiation and retrieval of account information. GDPR equally enables customers to obtain active control, via verifiable consent, of:

1. which personal data is stored with which (kind of) institution,
2. what data is processed for what specific purpose and
3. what data is shared with other organisations.

In addition, customers will be able to take along their (historic) personal data upon their request and will have the ‘right to be forgotten’, i.e. they will be in a position to demand that their personal data will be deleted when the business relationship ends. In essence, this implies that institutions (including banks) must provide customers with ‘tools’ to exert such control over their financial assets and personal data. This offers an opportunity for innovative (data driven) propositions beyond mere compliance to PSD2 and GDPR, and a major threat (fines of up to 4% of revenue, reputation loss) if banks fail to comply with or implement GDPR compliance in a proper manner.

The Open Banking business model will require crucial developments in digital identity and APIs. Key aspects of APIs are the functional scope (possibly going beyond what is required by regulation such as PSD2), effective business and operating models, and the scope of standardisation in terms of technology, legal and operational matters.

Digital identity is a concept banks are already familiar with. Notably ‘Know Your Customer’ (KYC) and Anti-Money Laundering (AML) requirements have led banks’ need to know who exactly their customers are.

Over the years, the management of customer-related data has become digitised and extended with (mobile) authentication and authorisation services available for use with banking services. The increasing need for customer control extends the use of these digital identities outside the bank’s domain. It enables customers to create and manage dedicated access rights to personal data and financial assets, i.e. ‘consent or authorisation management’. This is comparable to re-using social media logins at third party websites where a user authorises which personal attributes (e.g. name, friends list, email) a third party may access for delivering its service.

Thus, the user experience of customer control propositions is likely to be very much defined by the possibilities and implementation of digital identity tools (authentication, authorisation) at financial institutions, making digital identity capabilities a crucial asset in any digital bank, next to the importance of digital identity in cybersecurity.

Customer-centricity and, in particular, customers being ‘in control’, therefore represents a fundamental value of Open Banking, offering banks the possibility to increase both private and business customer relevance in the digital era. For individual bank practitioners and their institutions, the opportunity is to derive competitive propositions from this concept and to define the extent of customer control (level of

‘platformisation’: integrator, producer, distributor and platform (see [Figure 9](#)) that is provided beyond compliance to PSD2 and GDPR.

From an industry perspective, Open Banking challenges include the need for proper standardisation of APIs (beyond pure technical dimensions) and collective customer education on new possibilities and secure behaviour when they are exercising control over financial assets and personal data in relation to third parties.

1. INTRODUCTION

The digitisation of the past two decades has brought many changes, both in our personal and professional lives. The constant availability of up-to-date information on personal and mobile devices adds to transparency and puts us in control of our increasingly digital life-style, both private and professional. Internet-connected devices allow us to work, shop, play, create, share, inform, communicate and transact in an integrated manner, on our terms, 24/7, across the globe.

Major industries such as social media, telecom and music have already been reinvented, powered by new digital technologies such as mobile technology, APIs and data analytics. The banking sector was quick to offer a digital banking experience by offering web access to its services already at the beginning of the millennium, but major new business models fit for the digital era were created outside of the financial industry.

After a decade of increased digitisation following the introduction of the smartphone, many financial innovations have surfaced, bundled under the term 'Fintech'. In particular, payments proved to be a hotbed of innovation, with many alternative payment options appearing on the market.

In 2013, the EBA Board initiated the Electronic Alternative Payments Working Group (eAPWG), following on from the Cash Displacement Working Group which had led the EBA community's investigation into digitisation developments since 2011. In 2016, the Board decided to continue the activities of the Electronic Alternative Payments Working (e-APWG) Group under a new umbrella heading that will better reflect the areas of focus of the working group to the broader open banking agenda. To this end the e-APWG has been renamed Open Banking Working Group (OBWG). Up to June 2016, the eAPWG/OBWG produced seven publications, covering relevant topics driving change in the payments industry.

These topics include customer requirements, digital identity, new infrastructure requirements, blockchain and Open Banking.

Open Banking has quickly evolved into a synonym for change in our industry. Driven by the revised Payment Services Directive (PSD2), this is now rapidly expanding beyond pure payments. The 'Opening up' can potentially impact both retail and corporate customer segments and banking business domains spanning payments, cash management, lending, savings, wealth management and mortgages.

The underlying trend of this concept of 'Open Banking' is the increasing level of control available for customers on how, when and where they want to use their retail and corporate banking services. Technology (e.g. mobile, API, data analytics) has already been making this possible in other industries for more than a decade (e.g. Social Media like Twitter, Instagram and Facebook). The success of the Fintech movement indicates that there are customer needs that are still underserved by existing service offerings, which has opened up room for innovative players to fill this gap by technology-enabled financial innovations.

Recent regulation has accelerated the move towards a customer-centric approach in the financial industry, notably the PSD2 and in particular the provisions regarding 'Access to Account' ('XS2A'). Customers will be given control as to how to connect other applications (and their associated providers) to their (personal and corporate) payment accounts for initiating payments and accessing transaction data. This will be effective by January 2018, however, as a transitional period until the Regulatory Technical Standards (RTS), which specify specific security measures, are in effect. These will most likely become available by November 2018 at the earliest. Existing TPP solutions and business models will remain valid² beyond January 2018.

² See pages 24-26 http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en

The European Banking Authority (EBA) published its final draft of the RTS at the end of February 2017, on the basis of which market actors (incumbents and new licensed service providers under PSD2) are expected to implement XS2A. Subject to adoption of the EBA RTS, APIs could be an effective and automated means to enable appropriately licensed Third Party Providers (TPPs) to connect to payment accounts in a secure manner, i.e. without compromising security standards and minimising exposure of sensitive (payment) data.

Another significant regulatory trend is the implementation of the General Data Protection Regulation (GDPR) by May 2018. This establishes a regulatory framework for customers' control of their data through consent mechanisms, the right to be forgotten and the right to retrieve all personal data for re-use at other service providers of choice, thereby preventing a 'lock-in' situation.

This information paper on customer control builds on the earlier EBA publications. Chapter 2 elaborates on customer control. Chapter 3 provides an overview of Open Banking and how this links to customer control.

2. CUSTOMER CONTROL THROUGH THE CUSTOMER'S EYES

In an increasingly digital world the role of customers vis-à-vis companies and governments has changed significantly. We are coming from a product-centric world of limited customer-control where products were 'pushed' to customers. In the second half of the 20th century marketing as a profession developed further, and segmentation and distribution became important levers for success in a world of increasing abundance of physical goods.

Segmentation developed further into customer-centricity, where marketers try to increase the number

of touchpoints and feedback loops with the customer to improve marketing strategies. In a digital world, the interaction with the customer can be continuous, with 24/7 availability of services through an increasing number of digital channels. This advances the concept of customer-centricity to the next level, from the customer being merely the focal point (1.0) of marketing professionals (with limited feedback loops) to customers being in control (2.0), offering instant and continuous feedback. The figure below depicts this transition.

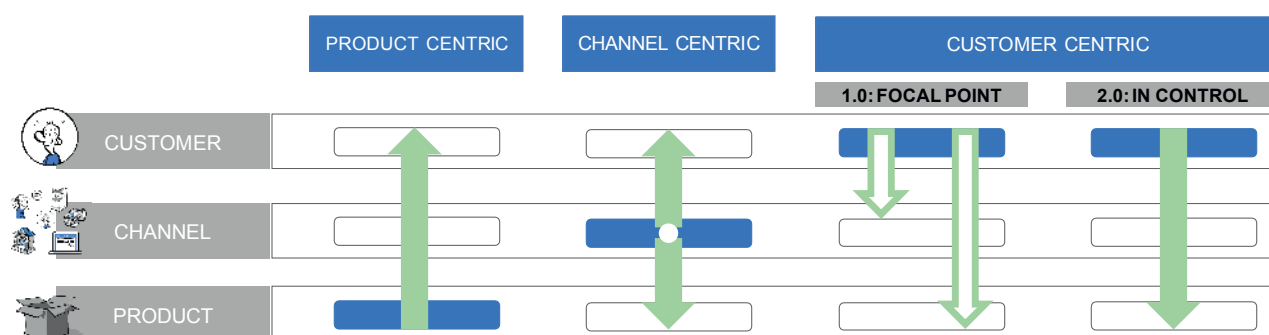


Figure 1: Transition from a product-centric to a customer-centric approach

In a 'customer-centric world', the customer is in control over what, when and where he buys goods and services, by making instant and continuous, fit-for-purpose choices on channels and products. Channels can change several times per day: for instance, a customer withdraws money via an ATM in the morning (first touchpoint), in the afternoon he checks his account via a third-party app on his mobile phone (second touchpoint), and in the evening, he logs in directly in the internet banking environment of his bank (third touchpoint).

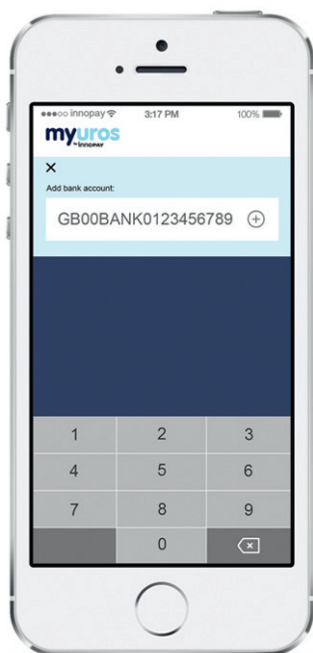
Banks are essential for putting customers in control of their financial services. So far banks have been leading in developing digital channels of their own, such as internet banking and mobile banking. In an "Open Banking" environment, however, customers will be able to use third party services to access

financial data stored by their bank. Uptake of these alternative digital channels depends strongly on trust and a consistent and attractive user experience and user interface (UX and UI), similar to bank channels. Therefore, accelerated innovation of digital bank channels can strengthen customer interaction, increase brand recognition, mindshare and customer relevance.

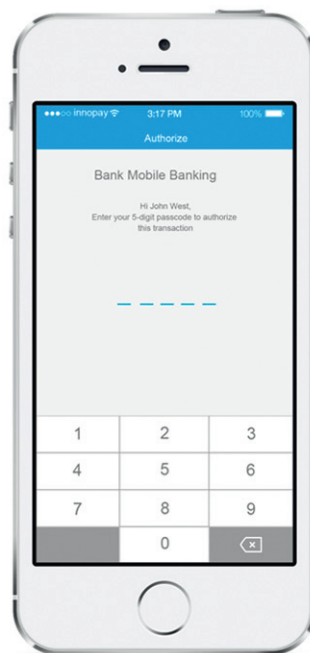
In this chapter, we guide you through some illustrative examples of what customer control could look like from a UX/UI point of view. It is based on the fictitious apps 'MyUros', 'JITFinTech' and 'Finance-App'. The four following use cases illustrate customer control from the point of view of the customer and show that the customer stays in control of his bank account because he defines who has access, at what moment and for what specific purpose.

Use case 1: MyUros app

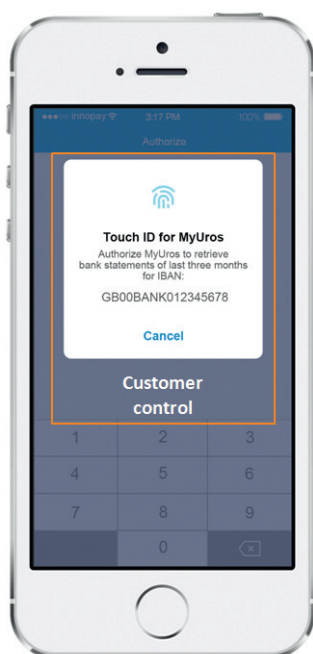
1. Connecting MyUros app to one or more payment accounts



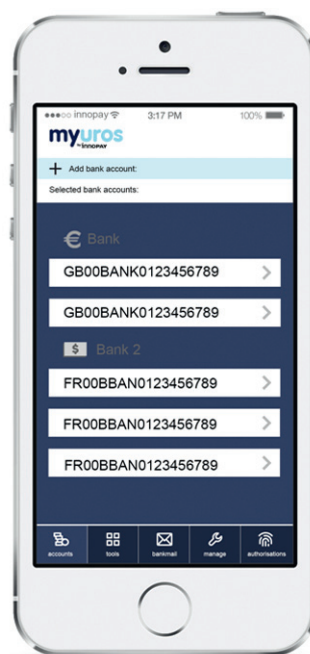
Customer connects selected payment account to MyUros app



Customer confirms account linking via own bank authentication credentials



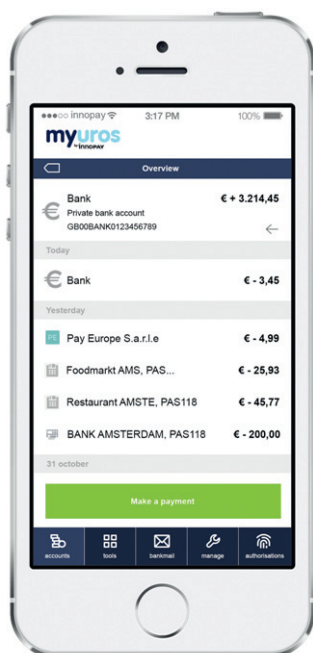
Customer authorises MyUros to retrieve bank statements of last three months for respective payment account. User can repeat this process multiple times to add different accounts



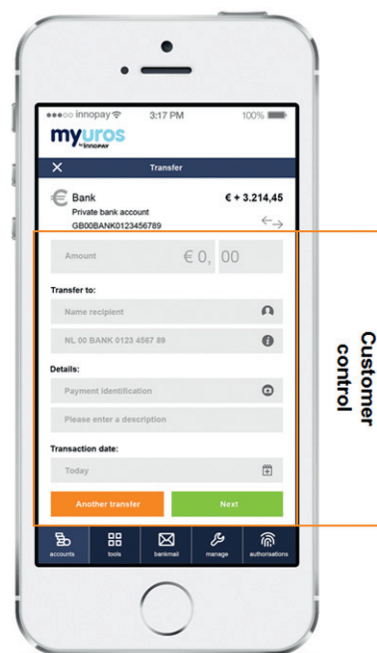
Customer has control over multiple payment accounts within the MyUros app

Use case 1: MyUros app

2. Connecting MyUros app to one or more payment accounts



Customer has transaction overview over multiple payment accounts connected to the MyUros app



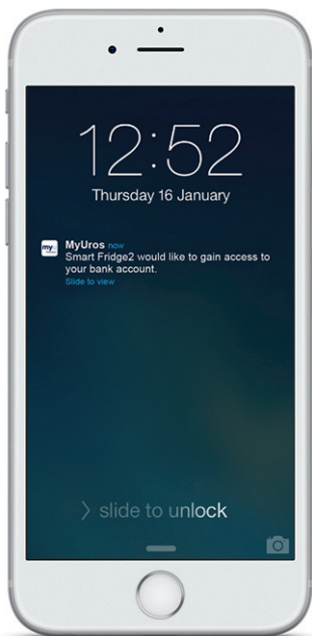
Customer can initiate payments from linked payment accounts through MyUros app. Customer authorises payment through existing banking credentials (screen not shown)

This first use case shows how a customer can exert control over his account(s) by providing explicit consent (i.e. authorisation) to link accounts, obtain account information for a specific period and initiate payments. The customer's existing banking credentials are key to exert this control.

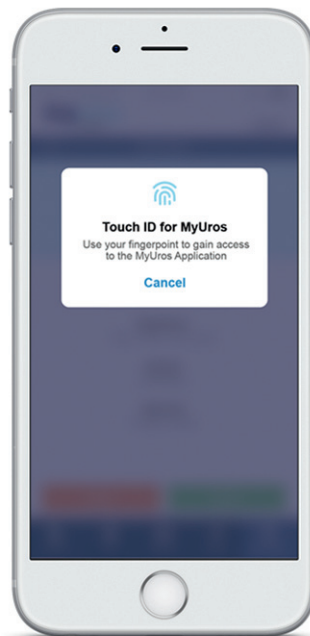
The user experience of the security measures would be determined by the provisions in the RTS and by additional bilateral agreements (between banks and the (authorised) third-party provider) in case certain use cases are not covered under PSD2.

In the next pages an additional use case of the MyUros app is shown where a 'smart fridge' is connected to a payment account for automated ordering and payment of groceries as well as two other use cases: request for personal loan (JITFinTech) and Personal Finance Management (FinanceApp).

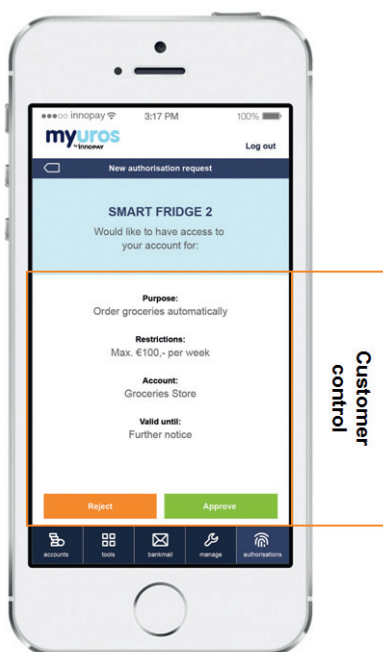
Use case 2: Smart fridge – authorising smart fridge to order and pay groceries



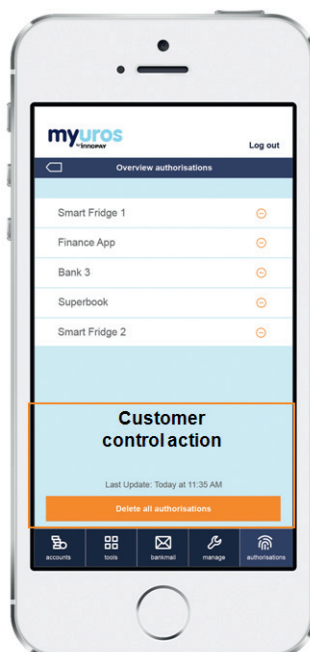
Customer's fridge asks for authorisation



Customer accesses the MyUros APP to grant authorisation

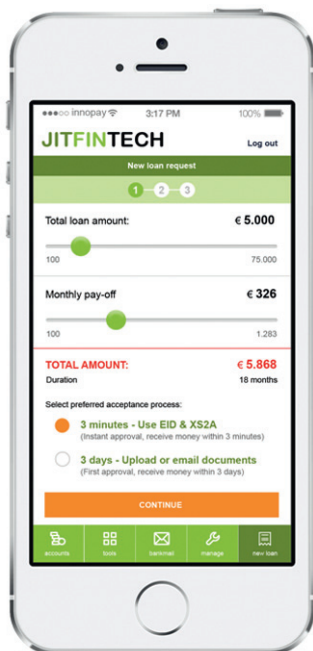


Payment initiation (recurring): summary of authorisation for smart fridge to order and pay for groceries up to maximum amount of 100 EUR per week

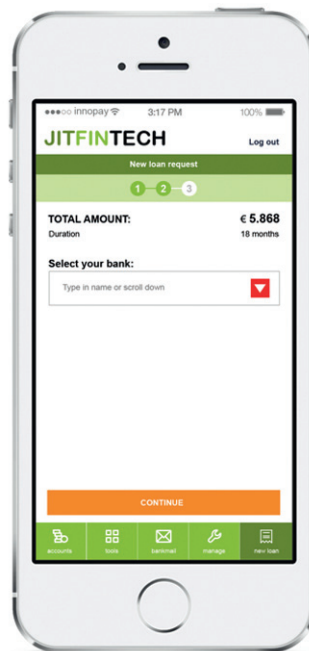


Overview of various authorisations and management options (delete, edit, revoke) are shown in the MyUros app

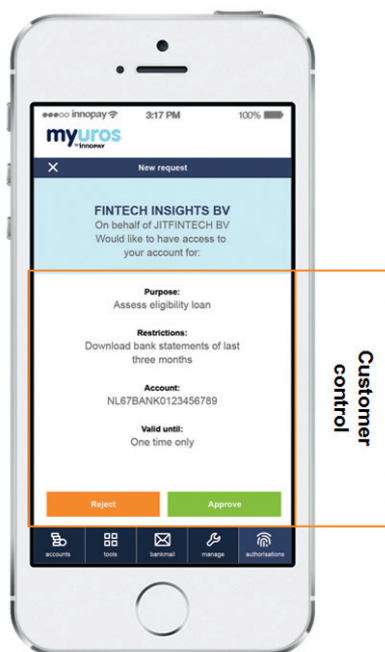
Use case 3: JITFinTech – Requesting personal loan by one-time sharing of account data



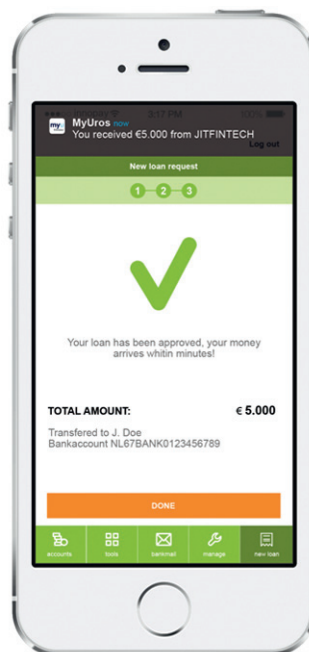
Customer configures loan request



Customer selects bank account for sharing account information



Customer authorises lender (JITFinTech) for one-time access to account data for specific period. Note that the lender has outsourced this process to another provider, i.e. FinTech Insights BV



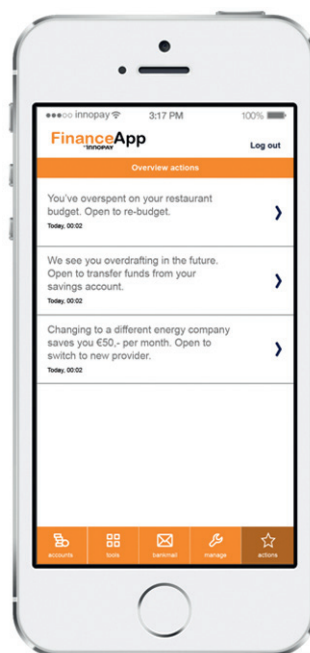
Customer receives confirmation of loan and an instant payment to immediately access the funds

Use case 4:

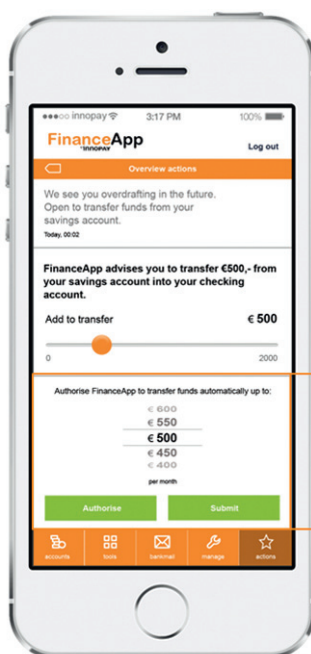
FinanceApp – Cash flow prediction and financial advice based on account data



Customer sees predicted cash flow based on account data

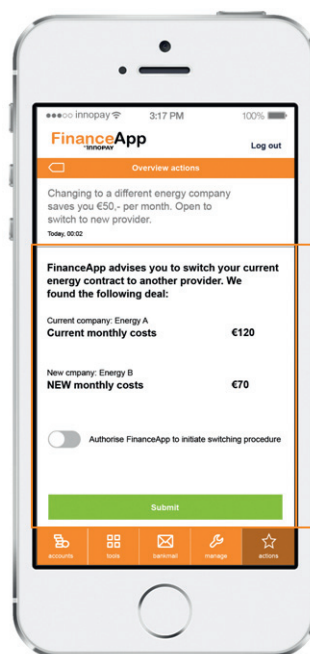


FinanceApp provides financial advice and presents possible actions to the customer



Customer control

FinanceApp also enables user to initiate a payment and to automate such transfers in the future



Customer control

FinanceApp provides users with suggestions for best offers based on benchmarking

The use cases illustrate what putting customers 'in control' could look like to customers who are used to operate in an increasingly connected digital ecosystem. The financial world is on the doorstep of these possibilities, which have already been well established in other industries.

In this changing world, bank apps no longer have exclusive access to bank accounts. Rather, customers are put in control and are enabled to connect third party apps of their choice directly to their bank account(s) to benefit from additional innovative financial services if they wish.

3. OPEN BANKING AS THE BASIS FOR CUSTOMER CONTROL

In the previous chapter, we have seen how users may experience 'being in control' of their financial assets and account data. In this chapter, we elaborate further on how Open Banking serves as the basis of customer control. In Open Banking, all customer propositions will provide some form of customer control, as we have seen in the use cases in the previous chapter.

Open Banking brings many opportunities for banks in terms of potential new (data driven) revenue streams, reduced time-to-market and cost, new partnerships and, above all, increasing choice and control for customers regarding how they deal with their financial assets and data. More information on the business relevance of Open Banking can be found in the information paper *Understanding the business relevance of Open APIs and Open Banking for banks* published in May 2016.

This chapter summarises the main dimensions of Open Banking and highlights how customer control manifests itself from a business perspective.

3.1 Open Banking revisited

The key dimensions of Open Banking are threefold: a driver (customer relevance and regulation), an enabler (Open API technology) and a key bank asset (digital identity). This combination allows for attractive, secure propositions and successful partnerships between bank and non-bank service providers of financial and non-financial services. These three dimensions are depicted in Figure 2.

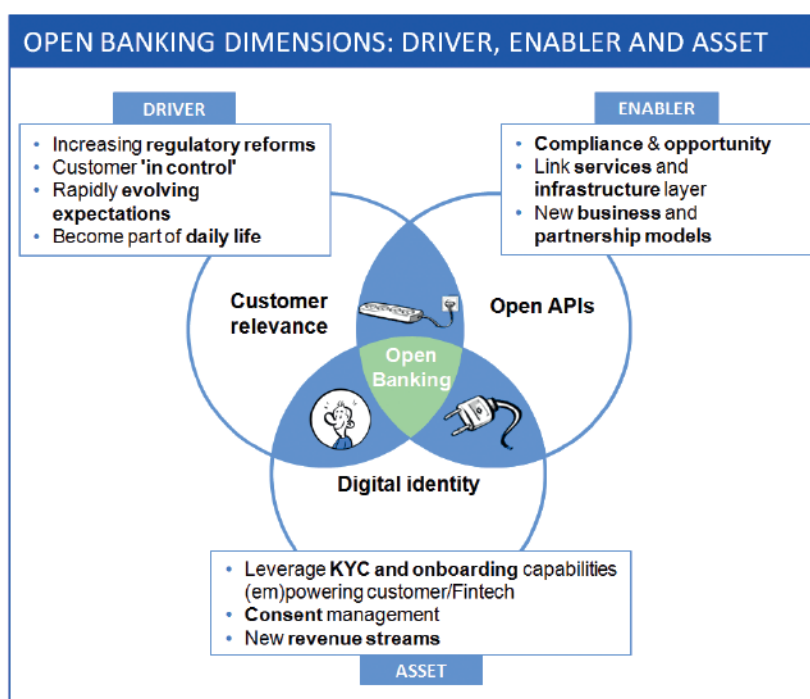


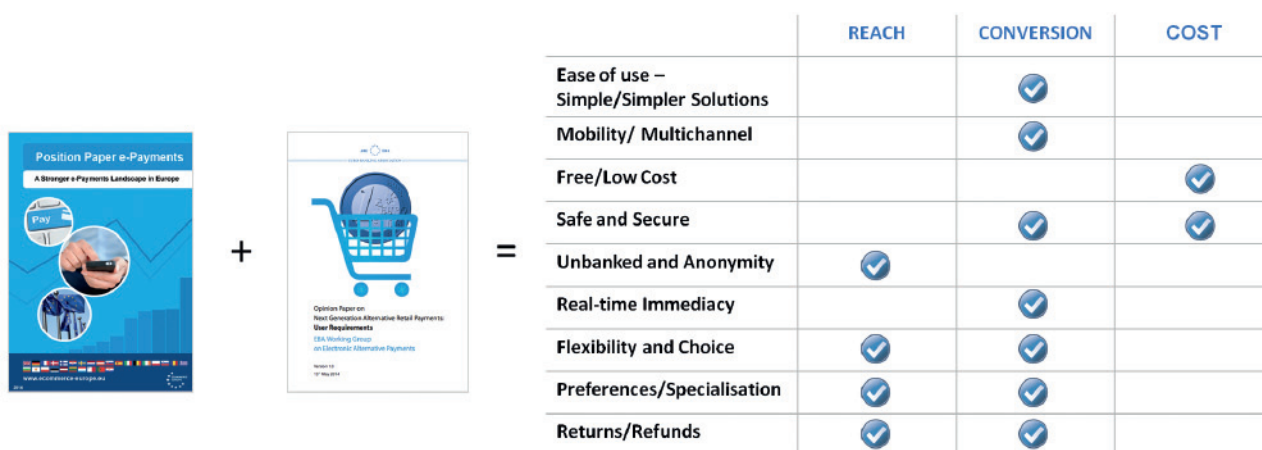
Figure 2: Three key dimensions of Open Banking

This section further analyses and describes these three important dimensions of Open Banking as seen by the Open Banking Working Group (OBWG).

3.2 Customer requirements and regulation as a key driver

In the EBA *Opinion Paper on Next Generation Alternative Retail Payments: User Requirements* we have seen that customer requirements by payers and payees exist in many forms. Combined with the over-

arching customer requirements of reach, conversion and costs (as defined by *Ecommerce Europe*), the following matrix emerges:



	REACH	CONVERSION	COST
Ease of use – Simple/Simpler Solutions		✓	
Mobility/ Multichannel		✓	
Free/Low Cost			✓
Safe and Secure		✓	✓
Unbanked and Anonymity	✓		
Real-time Immediacy		✓	
Flexibility and Choice	✓	✓	
Preferences/Specialisation	✓	✓	
Returns/Refunds	✓	✓	

Figure 3: Overview customer requirements 'Reach', 'Conversion' and 'Cost'

The relative importance of the above requirements has evolved over the years moving increasingly towards real-time, flexibility and choice.

Considering these requirements, we see that traditionally 'reach' and 'conversion' are comparatively more important requirements, while 'costs' only follows when the former two requirements are satisfied.

In Open Banking, 'Reach' from the perspective of customer control refers to the numerous options customers have as to which third party services they can use and connect to their bank account. 'Reach' implies interoperability between providers, based on standards in technology, messages and practices (functional, legal and operational). This is a collaborative topic, for example at the Euro Retail Payments Board (ERPB)³, where PSD2 access to the account has entered the agenda in June 2016.

'Conversion' in this regard refers to customer experience, i.e. the ease of use with which customers can use third party services. In particular, it refers to the ease of use of securely connecting and managing the relation between one's bank account including its financial assets and data and a third-party provider.

Successful customer control needs to address both 'Reach' and 'Conversion'

Digitisation makes new functionalities possible for new transaction and banking contexts, which were not feasible before. This is where Fintech players see opportunities, by addressing various un- or underserved customer needs, i.e. by offering services which have a better conversion through advanced functionalities.

³ <https://www.ecb.europa.eu/paym/retpaym/euro/html/index.en.html>

As we saw in the *Opinion Paper on Next Generation Alternative Retail Payments: Infrastructure Requirements*, an innovative Fintech layer on top of banking infrastructure leads to a disconnection in terms of reach and conversion. Banks have created trusted 'reach' based on the regulated SEPA-infrastructure, whereas Fintech players create attractive (payment)

propositions ('conversion') in this services domain though they typically lack reach. Customers then face the problem that they cannot pay everywhere when they would like to use new and innovative payment solutions. This relationship between the infrastructure and services layer is depicted in the figure below.

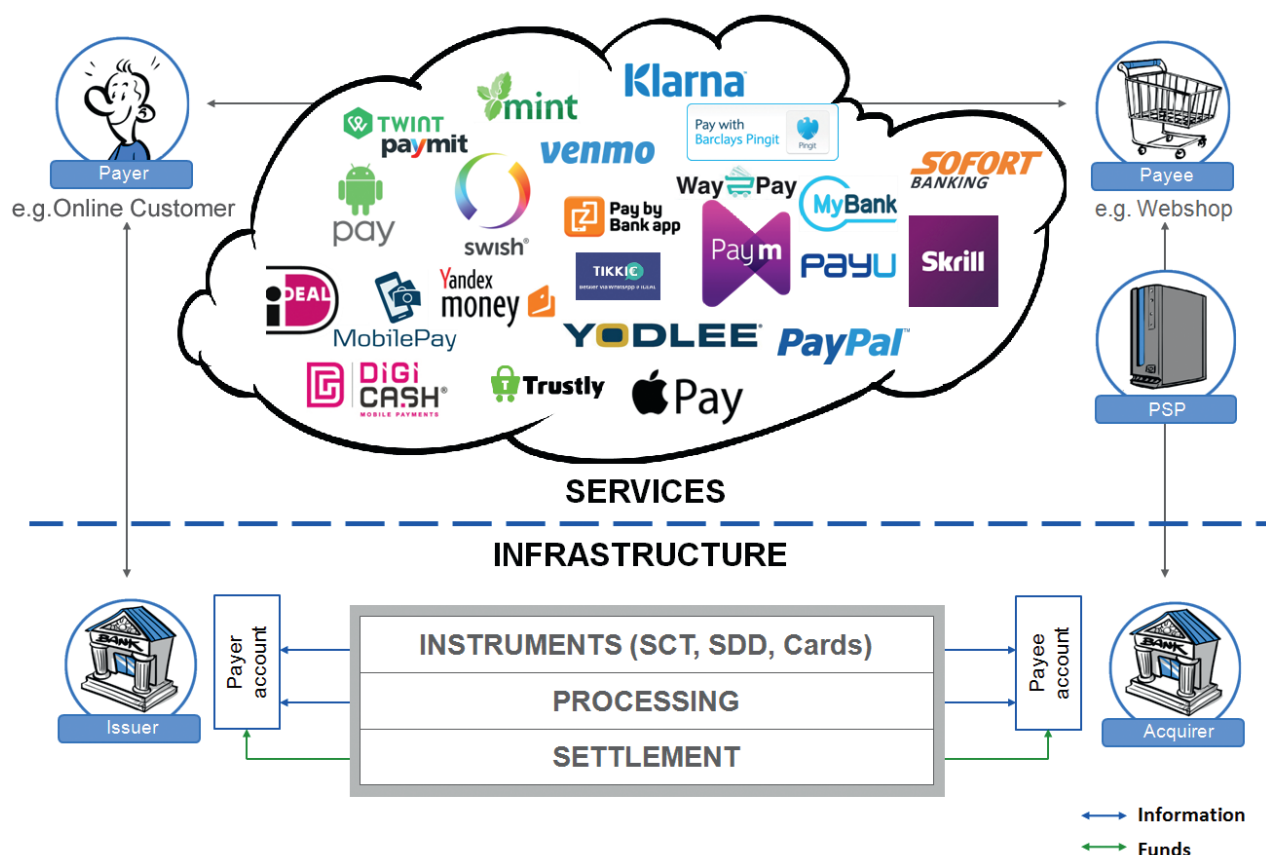


Figure 4: The services ('Fintech') layer on top of the infrastructure layer

The logic of customer requirements regarding reach and conversion implies that banks with their trusted reach can either embark on developing their own innovative propositions or alternatively they can

develop propositions collaboratively with Fintech players, embedding 'customer control' as the prevailing paradigm.

Reach, conversion and cost further explained

In terms of the payment system, reach is determined by the number of people that can be reached with the end-to-end trust, processes and infrastructure that is offered by the common network of banks. The main interest of end-customers in any network service (mail, email, telecommunications, etc.) is whether they can reach their counterparty. The relevance of any payment method depends on whether payer and payee can actually interact. In commerce, reach can be described as the number of (web) shop visitors that are potential buyers.

Conversion can be understood as the percentage of all actors that can use a method that actually do so. In commerce, this can be rephrased as how many potential buyers are 'converted' into actual buyers. Ease of use is a key driver of conversion. This category also comprises the functionalities of different payment methods. Payment methods cater for different contexts, all having their own specific requirements. When reach is satisfied, the functionality (fit-for-purpose) of the payment service

should be the top priority (Innopay, 2007, Journal of Payment Strategy and Systems, 'Understanding buyer and seller behaviour for improved product development').

The cost of a payment method determines the degree to which a trade turns out to be profitable for both sides. The cost of payments is always of interest for payers and payee and involves fees, but in some cases also cost of fraud (or counter-fraud measures). It should be understood that for both parties, the total cost of the trade is more than only that of the payment. The fact that a trade can be made in the first place (reach) and the fit of a certain payment method for a specific context (conversion) are factors that precede the issue of pricing.

Many examples can be found where the payment method of choice is not the cheapest, but the one that balances reach, conversion and cost best.

Combining reach with conversion implies that customers would be able to use bank propositions and functionalities provided by Fintechs in the context of managing their financial assets and bank data. To enable this securely, banks need to provide 'control' tools and a seamless experience to their customers.

The role of PSD2 and GDPR regulation for customer control

Regulators are sensitive to the disconnection between trusted reach of banks and innovative propositions by Fintech providers, which address possibly unmet customer needs. This is identified by regulators as 'inhibiting innovation' in the banking and payments landscape. PSD2, and in particular the provisions for XS2A, was published in its draft version in

July 2013 with the intention of stimulating innovation and competition. Under the PSD2 regulation customers will receive the right to connect authorised third party applications to their payment accounts for the purpose of payment initiation and account information services, i.e. customer control tools to operationalise this wider choice of services.

Another regulation regarding increasing (data) control by customers is the GDPR which will come into effect in May 2018. Under this new regulation, customers must provide verifiable consent to organisations before they can use customers' personal data. Customers will also have the 'right to be forgotten' and can retrieve their personal data for re-use at other service providers of choice, preventing a 'lock-in' at certain service providers.

These two regulatory developments (PSD2 and GDPR) strengthen the need to provide customers with the required tools and technologies to put them in control of their financial assets and data. Innovative services ‘on top of’ banking services with seamless customer experience, effectively addressing specific customer needs are required to differentiate and compete in the digital era. Needless to say, banks also have the opportunity to offer such Fintech-like services themselves and some banks are already active in this area.

3.3 API technology as enabler

In the previous section on customer requirements we have seen that combining reach and conversion

is key to ensure the large-scale uptake of innovative and ‘customer control driven’ payment and banking propositions. The emergence of such propositions is accelerated by regulatory developments such as PSD2 and GDPR. From a technology point of view these new propositions are enabled by using Application Programming Interfaces (APIs).

APIs come in many shapes and forms, varying from private (internal, within one organisation), to partner (between organisations) and public (“open”) versions. In all instances, APIs come with technical specifications, testing facilities and clarity under which legal and operational conditions the APIs can be used. ‘Open APIs’ are APIs, which are open to third parties to digitally connect services.

APIs in brief

APIs are interfaces between software applications, both within as well as between organisations. More specifically: APIs enable communication between software applications where one application calls upon the functionality of another application.

Every API is an interface, but not every interface is an API. API is a specific software architectural

approach based on the view that interfaces should be **scalable**, **reusable** and **secure** while offering ease of use for developers through self-service. APIs therefore hold the promise to reduce cost, complexity and lead time of interfacing between systems, allowing for faster, cheaper and better innovation on a larger scale.

Open Banking can be characterised as a technology-driven evolution of the banking business leading to more transparency, customer choice and control over financial assets and personal data. Open APIs are a key enabler of this evolution.

As such Open Banking is a movement ‘bridging two worlds’, i.e. making it possible for customers to use their banking and payment services in the context of other authorised third party (non-bank, Fintech) services, thereby combining innovative functionalities from banks and non-banks with reach through infrastructure. The figure below depicts the Open Banking

Platform Model where a ‘base banking’ layer is defined with an API layer which allows connectivity with third party financial services. In this way, the customer is given both choice and control. This mirrors the relationship between the services (‘Fintech’) layer and the infrastructure layer depicted in figure 5 as the platform model shows ‘services’ on top of a banking infrastructure under the secure control of the customer.

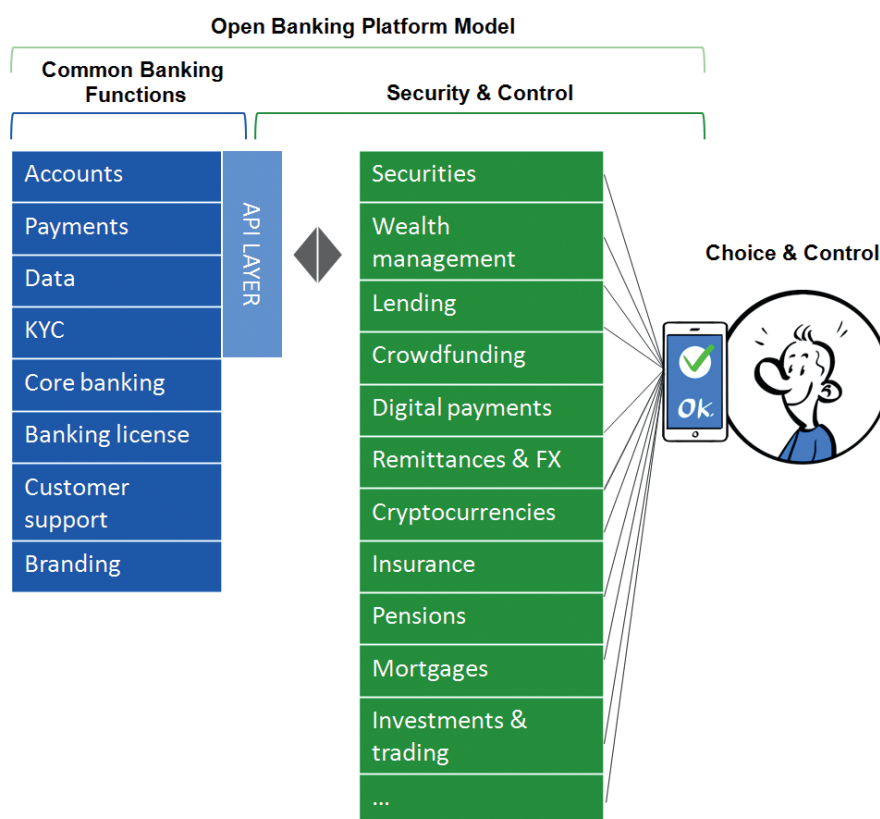


Figure 5: Open Banking Platform Model

The illustration shows that from the bank's perspective the strategic importance of Open Banking lies in the ability to redefine both product creation and product distribution strategies by engaging with third parties. From the customer's perspective, this translates back into 'control'. In the next chapter, we will elaborate further on these strategies. Let us first look into the third dimension which defines Open Banking: digital identity.

3.4 Digital identity: key asset defining user experience from a customer control point of view

Security and compliance are a 'conditio sine qua non' for banks to operate. Know-Your-Customer (KYC) is essential for the banking business: to be able to identify customers and to verify their identity when offering banking services are prerequisites for secure

banking operations. With increasing digitisation, identities also have become digitised, leading to the concept of digital identity.

Digital identity can be regarded as a service which banks have historically used in their own context, but which can increasingly be applied beyond the banking domain in the digital age. This provides opportunities to re-use banking identities and to offer digital identity 'as a service' through APIs towards authorised third parties, i.e. enabling bank customers to re-use their banking credentials for logging in but also to securely connect to authorised third party providers, by registering an authorisation that the third party can act on the customer's behalf (consent mechanism, as we have seen in chapter 3).

Introduction to digital identity

Within digital identity there are two main actors: the user and the relying party. The user wants to share

his digital identity with a third party, who then relies on the identity provided by the user. Hence ‘relying’ party.

Digital identity has three core functionalities:

1. **Identification.** This is done through attributes of a person or an entity. Think of name, social security number, registration number, address, age, IP-number, MAC-address etc. Attributes can be anything connected to a natural person, legal entity or machine and its use for identification depends on the usage context. Someone’s or something’s identity is simply a set of attributes which uniquely defines them in a particular context, e.g. in a bank this may be a bank account number or a customer number, in the context of government this may be the social security number.
2. **Authentication.** This is a procedure to verify someone’s or something’s identity. Often we talk about Strong Customer Authentication (SCA),
3. **Authorisation.** This defines what one can do and/or access after identification and authentication. Think of authorising the bank to initiate a payment on one’s behalf, or providing access rights to certain information.

The picture below shows the attributes and the three applications of digital identity in the context of different user and relying party segments: persons (consumers/citizens), businesses and governments.

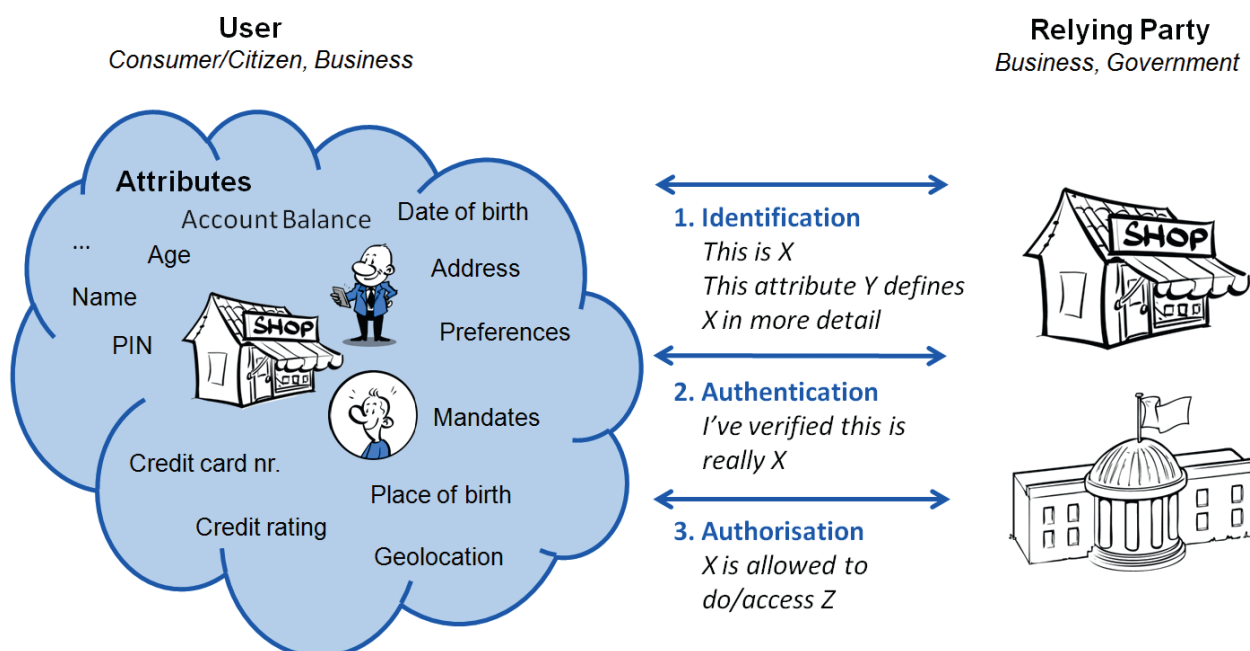


Figure 6: Three aspects of digital identity: identification, authentication and authorisation

The combination of the three aspects of digital identity is crucial for making Open Banking a reality. For customers to give authorised third parties controlled access to their account for payment initiation or account information, require a thorough security process along the principles described above. At the same time, banks support putting their customers in control by offering their verified identities ‘as a service’ to Fintech players, for example for onboarding and account sign-up processes.

Digital identity defines Open Banking user experience

To make Open Banking a reality customers must be given the ability to formally provide consent to their bank to enable a certain app or online service to access their bank data. The bank should also be able to verify this consent. The customer should be able to revoke this permission (i.e. authorisation) instantly. When using the app or service, the bank should also be able to verify that it is really the customer who is conducting a transaction through the respective app, therefore authentication by the bank is needed.

The user experience of Open Banking is strongly influenced by the digital identity user experience, through e.g. mobile, SMS or one time codes (e.g. a transaction authentication number (TANs).

The whole user experience could be very much like what many people have become accustomed to when using non-financial identities, e.g. when they login with Twitter, Facebook and Google. These services also offer the possibility to review one’s authorisation already given and to revoke it. The APIs behind this standard (Open standard for Authorisation – OAuth) are one of the most frequently used on a daily basis.

An area where banks already have a similar infrastructure in place is the mandate management for

direct debit. The debtor has a basic form of ‘consent management’, i.e. the option to maintain a blacklist and whitelist of creditors. As such direct debit (and also cards) can be seen as a form of ‘access to account’, but then a first-generation version, including a clear scheme and legal framework governing its operation.

Digital identity and the Regulatory Technical Standards under PSD2

The EBA has delivered its long-anticipated final draft RTS⁴ on strong customer authentication and secure communication in February 2017. As such, the RTS can be viewed as the ‘manual’ on how to deliver ‘customer control’ from a regulatory perspective, because it sets the basis for the user experience by prescribing principles on strong customer authentication.

The RTS are considered key to achieve the PSD2 objectives of enhancing consumer protection, and to promoting innovation through competition and improving the security of payment services across the European Union.

The figure below depicts and frames the security and authentication challenge that emerges from enabling authorised third party provider (TPP) access to payment accounts held by Account Servicing Payment Service Providers (AS-PSPs, typically banks) in the context of Payment Initiation Services (PIS) and Account Information Services (AIS) under PSD2.

⁴ Available online at: <https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf/679054cf-474d-443c-9ca6-c60d56246bd1>

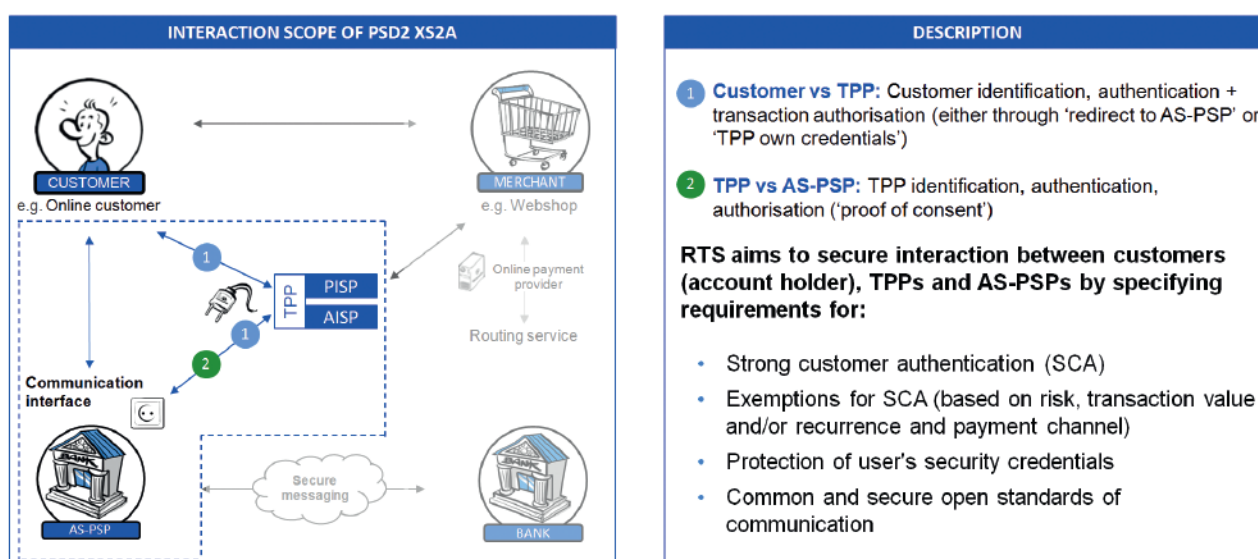


Figure 7: RTS requirements for interaction scope XS2A

The RTS are supposed to address the relationships between actors involved in an XS2A transaction (i.e. PIS and AIS) involving authorised TPPs by defining adequate security measures. However, different market actors (TPPs, AS-PSPs) will wish to employ different security technologies (static/dynamic, classical/emerging, risk-dependent, device fingerprinting, etc.). Customers will freely choose those actors that best serve their needs. In any scenario security and authentication options must comply with the EBA's RTS.

The RTS states that authorised TPPs have the right to rely on the authentication procedures provided by the AS-PSP to the customer. In such cases, the authentication procedure will remain fully in the sphere of competence of the AS-PSP, underlining that the AS-PSP provides the customer control experience.

The only situation when the transaction would be authenticated within the sphere of competence of the PISP is when a PISP issues its own personalised security credentials to customers. This would however require a prior contractual agreement between the PISP and the AS-PSP on the acceptance of such credentials. Such agreement would also be outside of the scope of PSD2. The RTS implies reusing the

bank issued digital identities to customers also in the context of XS2A, providing customers more control over TPPs and PISPs in particular about transaction authorisation.

In this chapter, we have described the three key dimensions of Open Banking. Customer requirements, APIs and digital identity together put the customer more in control of his/her own financial assets and data when interacting with third party service providers, with a leading role for digital identity when it comes to user experience.

In the following chapter, we will continue with the strategic impact areas of Open Banking.

4. STRATEGIC IMPLICATIONS OF CUSTOMER CONTROL THROUGH OPEN BANKING

In the previous chapter we have reviewed the drivers (customer requirements and regulation), technological enabler (APIs) and asset (digital identity) of Open Banking from a customer control perspective.

This chapter will summarise the strategic implications of customer control through Open Banking for banking practitioners, and show how Open Banking creates new opportunities in product creation and distribution with a focus on how this relates to customer control.

4.1 Open Banking: pivot for product creation and distribution

On the one hand, APIs enable organisations to dissect their products into services, functionalities and even into raw data, while, on the other hand, Open Banking enables new forms of distribution and enhanced servicing capabilities, in a scalable and secure fashion, with a widespread distribution network through third party partnerships.

As such, Open Banking offers customers control and choice. For banks, Open Banking offers greater reach: existing customers are given more options for usage and interaction with their existing banking relationship, while new customers are given more options to sign-up and embark on a new banking relationship.

Banks will have to make strategic choices with regard to the role they want to play in creating value for their customers and how they want to define their relationship with the Fintech community and the customers of this community.

Traditionally, banks have not only provided their customers with products but have also been responsible for the distribution of these products, i.e. the bank distributed its payment products through its own banking channels, such as mobile, web and branches. In this traditional scenario, the bank controls the entire product and distribution chain. Open Banking redefines both product and distribution as the principles (re-usable, scalable, secure, self-service), technologies and agreements of Open Banking allow for new

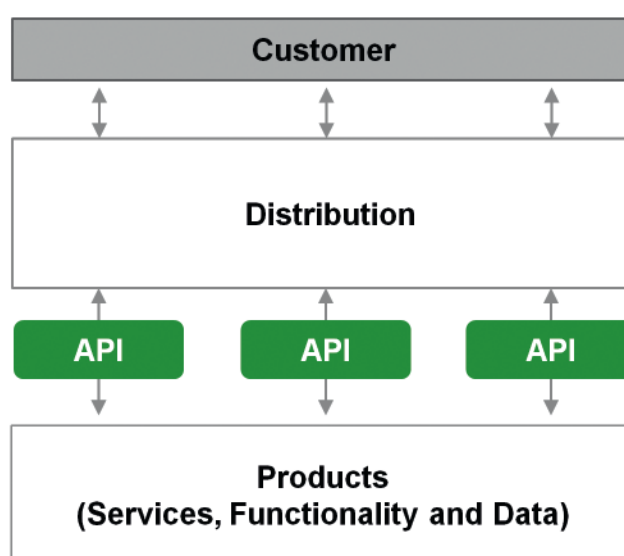


Figure 8: APIs are the pivot between products and distribution

possibilities. The below illustration shows where APIs fit in between products and distribution.

Using APIs for interfacing between product and distribution enables banks to decouple these functions. The combination of decoupling and opening up allows banks to play different roles in the financial value chain with regards to the offering of products and the distribution of these products.

4.2 Product impact through APIs

Bank products are impacted by the evolution of Open Banking because APIs allow for the creation of 'smaller products' (also referred to as 'micro services'), often subsets of today's banking products. These 'micro services' can be used as a component in authorised third party services. For instance, in the case of data products based on the bank statement, every line item (or collection of line items) of a banking statement could be seen as a data product, e.g. incoming payments, salary payments and certain cost categories. Digital identity services can be offered separately, i.e. 'unbundled' from a payment and combined to be used outside the banking context. Regarding transactions, examples are data elements such as status, reference, amount, receiver ID, message, fees and timestamp.

In the non-financial world, we have witnessed considerable innovations that emerged by dissecting an organisation's products into services, functionalities and even into raw data and making that available through APIs, examples include Amazon (IT services), Salesforce (CRM data) and Google (map and advertisement data). Similar dynamics are also expected in the financial industry where authorised third parties will be enabled to create new products and services 'on top of' banks' services, functionalities and raw data. PayPal was the first mover in the financial world introducing APIs in 2010, and today

maintains a community of developers. Customers will be put in control and decide which authorised third parties can make use of their financial assets and data in order to make an attractive offering for the customer.

4.3 Distribution impact through APIs

Banks are used to doing most of their distribution in a direct manner, e.g. through branches, ATM, call centre, web and app. API technology fundamentally alters distribution of bank products to customers by making it possible to have many distribution arrangements with third parties, without excessive cost or channel conflicts. With APIs, it becomes possible to distribute complete products or components through a potentially unlimited number of authorised third parties, alongside banks' own (digital) channels. Examples include KYC services, download of bank statements in ERP software and connection to payment initiation services (see chapter 3 for more examples).

Large players in the non-financial world have demonstrated that APIs can provide for an important revenue channel. For example, the travel site Expedia claims to sell at least USD 1.6 billion via their APIs (2012), by means of their affiliate network. eBay also sells at least 30% through third parties who connect to their APIs, whereas Amazon is also reported to sell at least 40% via their API-driven affiliate program.⁵

In the financial world, there is a similar development expected, implying that a major source of customer contact, reach and revenues will come via third parties, all driven by customers who will have choice and control with which third parties to interact and transact. In this future reality, it is up to banks and Fintechs to draw up partnerships and to define mutually beneficial propositions for their mutual customers.

⁵ <https://hbr.org/2015/01/the-strategic-value-of-apis>

4.4 Four platformisation levels of Open Banking in the financial value chain

When extending the concept of 'API as pivot', decision makers of incumbent institutions face two fundamental strategic questions:

1. **Who is distributing my products, which I make accessible via my API, to existing and new customers?**
2. **Who is creating the products that I will be distributing to my own customer base?**

Based on these two questions, four generic roles in the financial value chain may be defined: integrator, producer, distributor and platform. The roles indicate the 'platformisation levels of Open Banking'. Each level correlates with increasing customer control when looking from the customers' perspective as illustrated below.

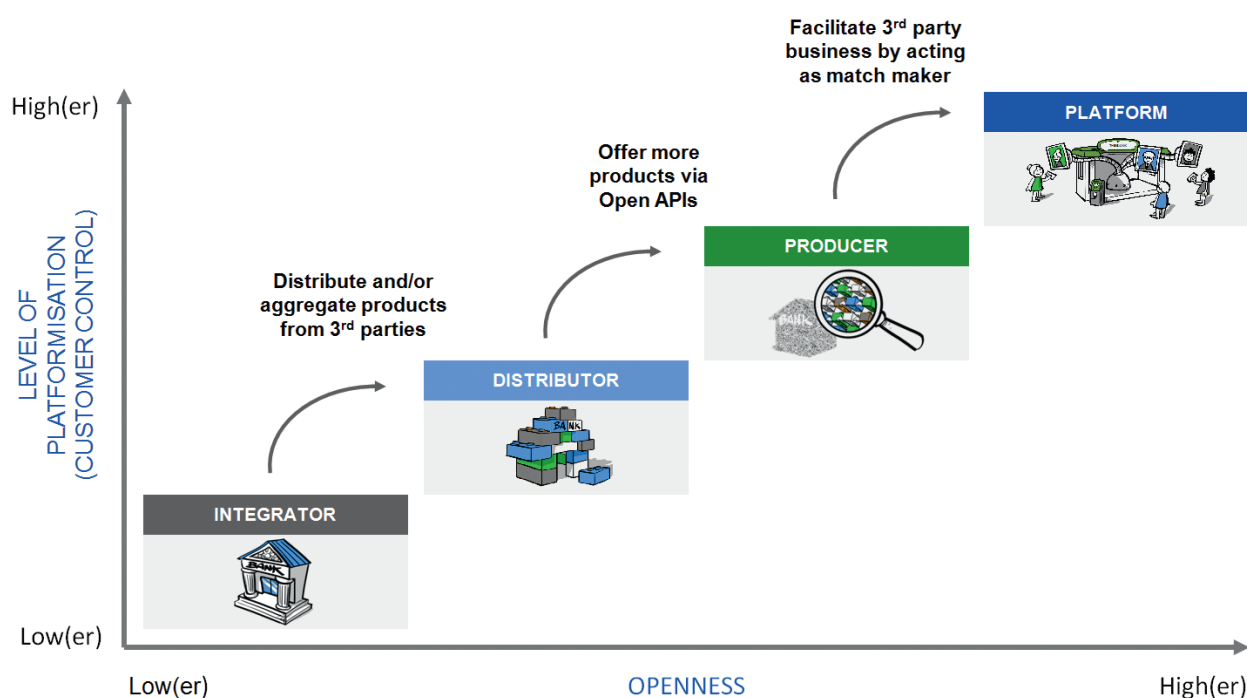


Figure 9: Four platformisation levels of Open Banking

Most of the larger financial institutions already play roles 1, 2 and 3 (integrator, distributor and producer) at the same time (often assigned to different business lines or products), whereas role 4 (platform) is still at a very early stage of its development. Note that the PSD2 and its provision for Access to the Account are part of the 'producer' level. The producer level is larger than PSD2, since this comprises also products (i.e. beyond payment initiation and payment accounts) which are not mandated by PSD2.

The four roles depict varying levels of customer control, where the integrator role has the lowest platformisation level and the platform role the highest. The roles are further elaborated below.

Role 1: Integrator

In this role, the offering to the customer is exclusively created and distributed by a single party, i.e. bank. The result is that distribution and products are provided under one brand and that the customer experience

is fully controlled by the bank. Currently, most banks play the role of integrator, as they control the whole value chain, and have also done so in the digital space since the early days of the Internet. For instance, account information and payment services are distributed via the bank's online and mobile channels to the consumer. In the emerging PSD2 era, the dominance of this model can be expected to decrease, since banks must facilitate access for appropriately licensed TPPs when their customers provide their explicit consent.

In terms of customer control: the amount of control is defined by what the bank offers in terms of services. The channel is defined by the bank.

Role 2: Distributor

With banks opening up and other non-financial service providers adding Open API access to their services, banks could consider to extend their digital market presence by distributing third party services and thereby adopting the role of a distributor.

In this role, a bank offers third party products through its own distribution channels, leveraging its own distribution strength. In PSD2 terms this means that a bank would itself become a TPP, although the product scope is limited to what PSD2 prescribes.

In terms of customer control: the amount of control is higher because of the increased number of products offered via the banking channel.

Role 3: Producer

In this role, the offering to the customer is created by a minimum of two parties. The bank creates the service, while an external party (e.g. traditional channels or Fintechs) distributes the service to the customer, who is often also a customer of the bank.

The XS2A provisions under PSD2 trigger the emergence of the producer role as banks open up and move from the integrator to the producer role, in particular with regard to account information and pay-

ment initiation services. While most of the larger banks are working on a Fintech collaboration strategy (beyond PSD2 scope), some banks are less inclined to adopt a producer role. Extra revenues and innovation may seem attractive, but may carry with them increased regulatory and compliance risks by introducing dependencies on third parties.

Despite these risks, the producer role is being increasingly explored by banks nowadays, as is evident from the number of bank sponsored 'accelerators', 'incubators', 'developer portals' and 'hackathons' across the globe. The early stage of platformisation is well underway in financial services.

In terms of customer control: the amount of control is greater because of the increased number of channels and associated services the customer can choose from.

Role 4: Platform

A platform as a 'business model' facilitates the business of others by acting as an intermediary. Put differently, the bank does not act only as a provider or distributor, but as a facilitator for third parties and the bank's customers. This is often referred to as 'peer-to-peer' business. As the most advanced form of platformisation, banks could offer the following capabilities, e.g. matching of parties, security and Know Your Customer (KYC). Note that the meaning of 'platform' as a business model is different from platforms in the IT world, where a platform refers to the physical IT infrastructure needed to run a bank in general.

Banks as platforms are not common, although Fidor Bank could classify as an example. Several Fintech market participants have adopted this model as a starting point in lending (Lendify, Zopa), crowdfunding (Kickstarter, Ecocrowd) and 'broker' roles (eToro, DeGiro).

In today's networked and digital era, the competitive landscape is increasingly defined by plat-

forms, which have transformative potential (e.g. Uber, Airbnb, iTunes) in keeping with the motto “build a better platform, engage a community and you will have a crucial advantage”. For the financial industry, the phenomenon of platforms still has to be further developed. For payments and personal information this is expected to gain traction through the XS2A provisions under PSD2, as third parties can engage in service provisioning without actually owning bank assets. Open Banking extends this concept further. From the customer’s point of view it means increased choice and control over financial assets, data and the service providers having access to this.

In terms of customer control: the amount of control is maximised because of the increased number of channels, products and providers the customer can choose from, all within the context of their own bank.

Summarising the four platformisation levels of Open Banking

Embracing a new role in the financial value chain with a limited or extended level of platformisation entails transformational challenges as it requires changes in the business and operating model. Criteria to consider when evaluating the level of strategic change include customer choice and control, customer loyalty, market propositions, cost efficiencies, innovation culture, employer attractiveness, business and IT alignment, available means for investing and possibly outsourcing.

Business leaders within banks therefore are faced with significant strategic challenges, entailing the full classic spectrum of rewards versus risk as a first high-level qualitative analysis shows in figure 10:





	INTEGRATOR	DISTRIBUTOR	PRODUCER	PLATFORM
				
IMPACT ON				
REVENUE	-	+/-	++	+++
RISK EXPOSURE	+/-	-	--	---
OPERATING MODEL CHANGE REQUIRED	+/-	+	++	+++

Figure 10: High-level impact assessment platformisation levels of Open Banking

Opening-up and giving customers more control can have a positive impact on revenues (and profits) as successful open (platform) models in the non-financial industry have shown in the recent past. Risks in terms of increased compliance challenges and increased competition are mounting as well, all potentially to be mitigated and adequately managed by changes in the operating model. Each level of platformisation comes with varying challenges, where the pursuit of a ‘doing nothing’ strategy is not an option.

This is a crossroad which every bank could face in the next 1-3 years. The minimum engagement in ‘opening-up’ is what the PSD2 will prescribe in terms of access-to-account, i.e. a limited ‘producer role’ and thus limited level of platformisation, while the current Fintech and innovation boom poses growth challenges regarding business strategies for partnering and product propositions towards third parties.

The ever-changing customer expectations will drive this need for more advanced levels of platformisation enabling ultimate customer choice and control options.

APPENDIX: GLOSSARY

API – A language and message format used by software applications to communicate with each other.

Account Servicing Payment Service Providers (AS-PSP) – Banks that provide current accounts with a payments functionality to their customers.

API Design – The design of an API with the aim of assuring performance, scalability and simplicity, the most popular design principles being SOAP and REST.

Closed API – Communication of applications within the same organisation using APIs.

Co-creation – The process of creating customer value through collaboration between multiple parties.

Conversion – The provisioning of seamless, easy to use payment services towards payers and payees.

Data Access – The process of controlling access to data. The most commonly used standards for this being SAML and OAuth 2.0.

Data Exchange – The format in which API data is encoded with JSON and XML being the most popular formats.

Developer – The technical function of third parties, making the connections to the APIs. Often used as a synonym for third party.

Disintermediation – An economics term related to the elimination of middlemen in a supply chain.

Distributor – A role in the financial value chain where banks use their own channels to offer third party products.

Fintech – New solutions which demonstrate an incremental or radical / disruptive innovation development of applications, processes, products or business models in the financial services industry.

Fragmented – The state of a payment network where payment methods lack reach.

General Data Protection Regulation (GDPR) – is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Infrastructure layer – The part of the payments infrastructure characterised by SEPA (including the standardised payment instruments SCT, SDD and cards) and the clearing and settlement systems that offer end-to-end trusted reach.

Integrator – A role in the financial value chain where the offering to the customer is exclusively created and distributed by a single party.

KYC – Know Your Customer is the process of a business identifying and verifying the identity of its clients.

OAuth 2.0. (Open standard for Authorisation) – API data access standard.

On-boarding – Actions that need to be completed by the financial services provider such as providing know-your-customer procedures to offer customers a particular financial service.

Open API – Communication of software applications of different organisations using APIs.

Open Banking – A term that is currently still under construction but is aimed at promoting transparency as well as free and unrestricted access to knowledge and information.

Open data – Open data is the idea that some data should be freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control.

Open government – Open government is the governing doctrine which holds that citizens have the right to access the documents and proceedings of the government to allow for effective public oversight.

Open innovation – A paradigm developed by Henry Chesbrough that assumes that organisations can and should use external ideas as well as internal ideas, and internal and external paths to market to advance their technology.

Partner API – APIs for use by partners based on bilateral agreements.

Payment Services Directive (PSD2) – European Commission directive to regulate payment services and payment service providers throughout the European Union (EU) and European Economic Area (EEA). The Directive's purpose is to increase pan-European competition and participation in the payments industry also from non-banks and to provide for a level playing field by harmonising consumer protection and the rights and obligations for payment providers and users.

Platform – A role in the financial value chain that enables a multi-sided market as it facilitates business of others by acting as an intermediary platform.

Private API – APIs for exclusive use within the boundaries of an organisation.

Producer – A role in the financial value chain where the offering to the customer is created by a minimum of two parties. The bank creates the service, functionality and data, while a third party (Fintech) distributes the service.

Public API – APIs open for use by anyone.

Reach – The size of the network of participating payers and payees and an indication of the utility of participation in a payment network.

RTS – Regulatory Technical Standards issued by the European Banking Authority (EBA) proposing high-level principles on strong customer authentication and secure communication. The RTS are key to achieving the PSD2 objectives of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union.

SCA – Strong Customer Authentication is a procedure including at least two out of the following three factors: 1) something only the user knows, e.g. passcode or PIN; 2) something only the user possesses, e.g. mobile phone or token; 3) something the user is, e.g. fingerprint.

Services layer – The part of the infrastructure characterised by the presence of Fintech parties that perform a customer-facing, user experience function on top of the infrastructure layer.

Sign-up – Actions that need to be completed by the customer such as providing identification and passwords to make use of a financial service.

XS2A – Access to Account for authorised third parties who, with explicit customer consent, can provide Payment Initiation and Account Inf

Contact details

For any additional information, please contact:

Daniel Szmukler
Director
d.szmukler@abe-eba.eu

Euro Banking Association (EBA)
40 rue de Courcelles
F - 75008 Paris
TVA (VAT) n°: FR 12337899694

layout: www.quadratpunkt.de
cover: © [In60Seconds](#)