Published in
JPSS Journal of Payments Strategy & Systems, Vol 8 No 2 pp157-171 May 2014
and a significant extract/preview was published in/endorsed by the EPC in
EPC European Payments Council Newsletter January 2014 [5]
also significant subset published in Journal
E-Finance & Payments Law & Policy, Cecile Park Publications,
Volume 8 Issue 5 pp12-14 May 2014
also to be published in full in the German book
(under the title „Zugriff auf Bankkonten durch Dritte – Chancen für Banken durch Öffnung“)
Trends in Zahlungsverkehr, 2. Auflage, mit Bundesbank, Hrsg Egner, Dittrich,
Bank-Verlag 2014
also short extract published in
Equens EQ Magazine, Vol 5 pp28-29 June 2014
and extracts published in the cover story under
“Open Access Banking - The Threat from Non-Banks” in the
Cover story of The Banker magazine, Financial Times, pp16-21, August 2014

Access to accounts – why banks should embrace an open future

Keywords: PSD2, XS2A, Access to Accounts, CAPS, TPP, Open Bank to Third Parties, Lessons to banking from other industries, Liberalisation, Proactive rather than reactive approach by banks, Controlled Access to Payment Services, Embracing Change

Michael Salmony
Equens SE, Mainzer Landstr. 201, 60326 Frankfurt am Main, Germany.
Tel/Fax +49 172 6867163; e-mail: michael.salmony@de.equens.com

***Dr Michael G. Salmony** is Executive Adviser at Equens SE, the first and leading pan-European full-service payment service provider, which processes over 10 billion payment transactions and 4 billion POS and ATM transactions per year. He represents national geographies, banking consortia and international industry sectors within such bodies as the European Commission, the European Payments Council and the European Association of Cooperative Banks. He is much in demand as a keynote speaker at international conferences, has published extensively in books, national newspapers and trade periodicals and appears regularly on broadcast and digital media. He studied at Cambridge University,UK before beginning a long management career in the application of innovation to business value at IBM, to now working especially in the internet and financial services space*

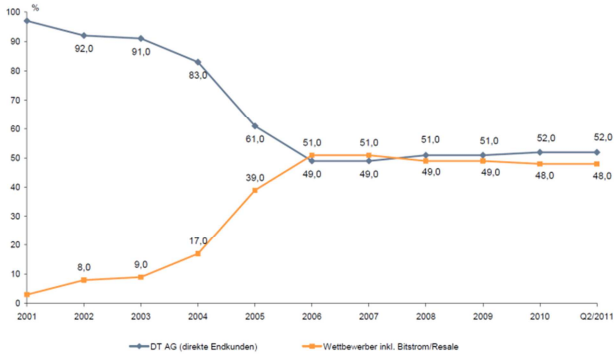
Abstract

This paper provides a fresh perspective on the recent access to accounts initiative proposed by the European Commission. There is a history of success of open versus closed systems (e.g. IBM, Telecoms, etc), and it is now the banks' turn to open up. As it is better to disrupt yourself rather than letting others disrupt you, the author proposes an open standard interface for controlled payment services: CAPS (Controlled Access to Payment Services). The recent PSD2 regulation proposal provides some of the necessary prerequisites of such an approach – but many questions remain to be answered and severe changes need to be made if the success of other industries is to be replicated here. Open access to bank accounts has the potential to lead to an explosion of (potentially disruptive) innovation, competition and new services. New revenue streams will evolve and the banks themselves could even be one of the main beneficiaries of this dynamic development. Yet banks need to position themselves proactively in this new environment. The access to accounts will be reality in the not too distant future – the regulator will enforce this (although he still has to set some boundary conditions for success) - so banks should now prepare to shape this business opportunity to their advantage. This can lead to a situation where banks, payment service providers, merchants and customers are markedly better off than today.

Background

On 24th July 2013, the European Commission published a "Proposal for a directive of the European parliament and of the Council on payment services in the internal market", discussed as the Payment Services Directive 2 (PSD2).[1] One key element is the access to accounts proposal, which will require banks to open their customer accounts to third party providers ("TPPs"). An intense debate was ignited even before this date around whether and how banks should open up. Especially the "how" is still unclear for many market participants and some suggestions will be made in this paper on how the opening can be conducted in a safe, secure, regulated and fair way. For this it is already clear that for some further boundary conditions need to be set.

First it is worthwhile to step back and have a look into other industries. When IBM pioneered information technology in the last decades, their initial approach was to build a closed system. Interoperability and connectivity were limited to IBM hosts, IBM peripherals and IBM networks. But only when IBM and others opened up (through the advent of the open internet) did the IT revolution really gain momentum. Today, not only the economy has benefited tremendously from open, interconnected IT, but so did IBM particularly as well. This is due to the fact that IBM embraced the change, shaped it actively and also due to the fact that all participants developed a mutually beneficial ecosystem: contracts regulated liabilities, fair market-based fees were paid for services rendered etc. Another example is to be found in the former situation of national monopolies enshrined by law well into the 80ies, e.g. in telecommunication, rail, electricity or the postal system. Telecommunications players had initially resisted liberalisation as long as they could. Yet today, across all major European markets, the previous market leader (indeed the ex-monopolist) generally still commands as much as all the other new market players together – in a hugely bigger market – even in recent topics such as mobile (see Figure 1).



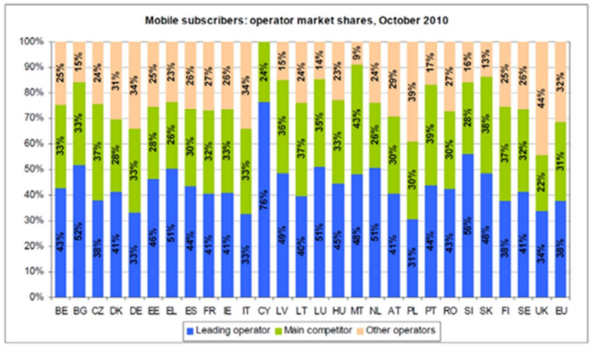


Figure 1: Telekom example of effects of liberalisation: Market share of dominant, ex 100% monopolist player typically settles at ca. 50% against all other competitors together after opening up to third parties – in a hugely bigger market.

[Source: Bundesnetzagentur Tätigkeitsbericht Telekommunikation]

This is largely true across Europe and even for new topics like Mobile – ex monopolist (dark/blue) commands 50% and thus roughly equal to all other competitors together

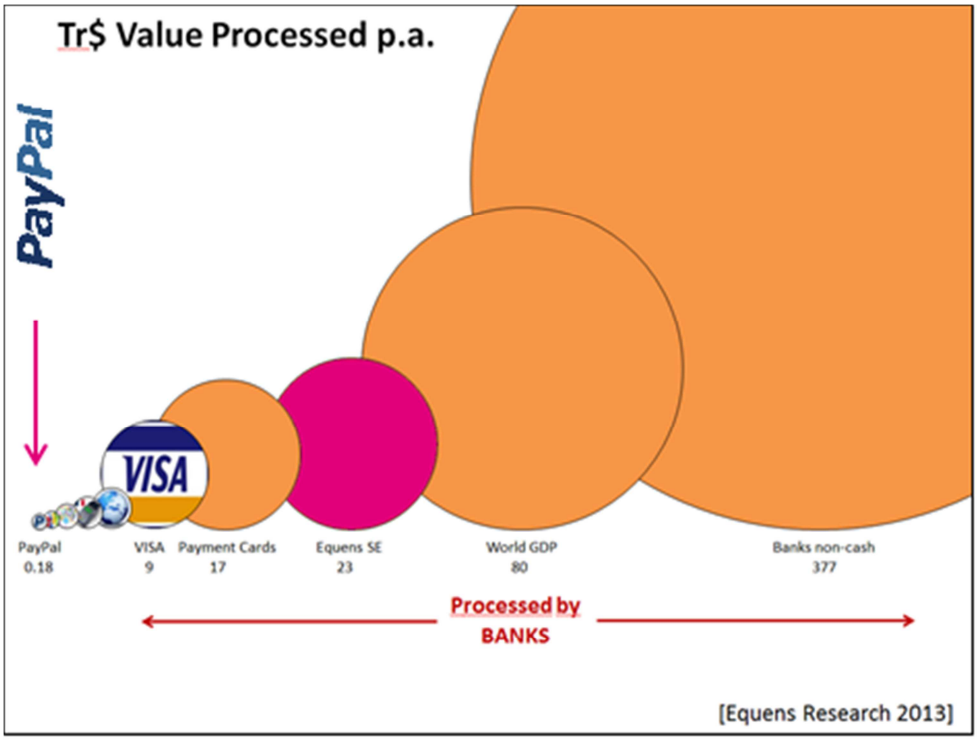
[Source: European Commission Digital Agenda Scoreboard: Electronic Communications Market Indicators]

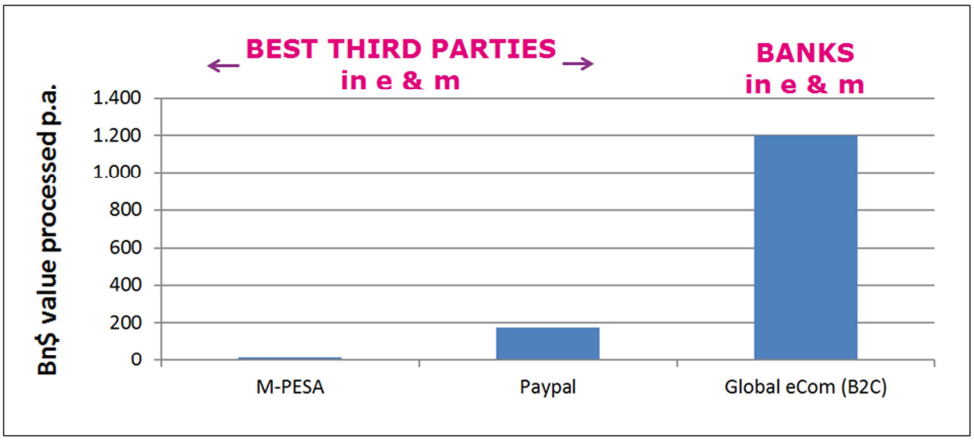
Thus in most countries the formerly ex-monopolist telecom players are the winners since they not only hold by far the largest market share but also because the whole market grew massively (the telecommunications market grew by a factor of x33 in ten years – an unimaginable development in a closed world dominated by a monopoly incumbent). Also here the telecoms, while being forced to open up, were granted the right be paid for the use of the "last mile" to their customers and other services they provided to the new entrants – and thus everybody won. This - for some very surprising - result that ex-monopolist are not destroyed by the new, nimble competitors but instead continue to be the dominant winner – in a massively bigger market – and is thus the main beneficiary of liberalisation can be seen in many other industries. The latest example, from the smart phone arena, demonstrates the rapid surge of market share of the (open) Google Android operating system to around 80% globally, again demonstrating the inexorable rise of open systems [1]. Thus we can see that open systems tend to win in the end and that liberalisation and opening up to third parties is typically of benefit to the whole economy and – surprisingly in particular – of benefit to the ex-incumbent. Will this apply to financial services and payments too ?

Time to open up in payments

While open systems can thus often be beneficial even (and especially) for the incumbents, they sometimes have to be forced into their luck (Apple was forced to open its initially closed app store through jailbreakers, Telecoms were forced to allow third party access through regulation). It is now the banks' turn to open up. The PSD2 proposal is clearly demanding access to bank accounts (or more correctly: to payment services) for third parties. Banks can potentially be those benefitting most, if they take the right decisions now and if the regulator and market ensure a fair ecosystem where – as in the successful examples in other industries above - contracts regulate liabilities and fair prices are paid for services rendered.

Looking into the current e- and m-commerce space, there are already strong alternative payment solutions including PayPal, Amazon Payments and diverse Overlay Services, even without access to accounts legislation. PayPal offers proprietary virtual accounts and so far the majority of their transactions in Europe are funded from the user's current account via a direct debit mandate (i.e. without paying anything to banks for use of their infrastructure). In view of the success of PayPal (currently 148 million active accounts, double digit growth rates, increasing fees etc), some may think the fight in Online is lost for the banks. However, it is worth noting that despite 15 years of active market development, good growth rates and huge media attention, PayPal's processed volume still only represents under 0.05% of global electronic transactions and is really putting no dent at all into banks' business (see Figure 2). The fight in online payments is thus not lost to anybody, but all players (especially banks, the current incumbents) face significant opportunities that should now be addressed.





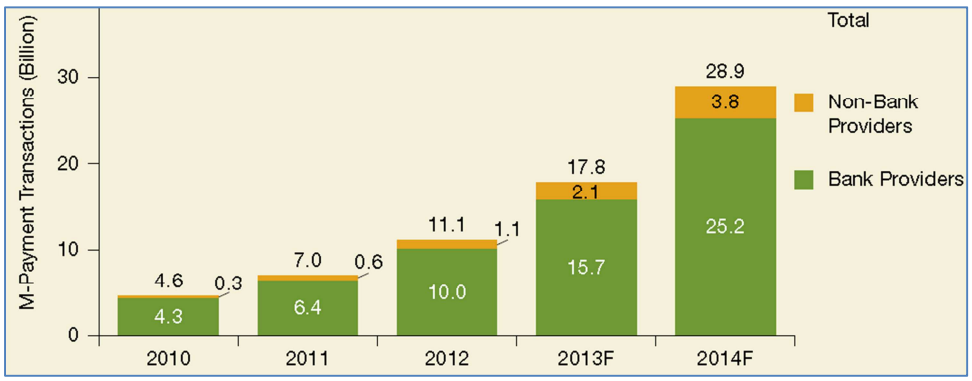


Figure 2: The battle for future payments is not lost to PayPal, MNOs etc – Banks still winning by far both globally and in internet and mobile

[Sources: Equens Research 2013 (top Figures) and CapGemini World Payment Report 2013 (bottom Figure)]

Most of the current “winners” in online payment are overlay services riding on bank infrastructure. Building on banks’ card or ACH networks, these overlay services provide significant additional convenience to consumers and merchants. On the one hand, most of these service providers have not signed contracts with banks for infrastructure usage, are thus not tied into any liability partitioning, hinder harmonised communication, dispute management and redress procedures, and no compensation is paid for providing the underlying infrastructure, compliance, issue resolution and contact points in case of problems and much more. On the other hand, alternative providers face difficulties establishing innovative payment solutions, e.g. due to the diversity of payment products across markets, or due to the lack of a standardised interface to online banking. The absence of a standardised online banking interface in most European markets is one of the barriers for TPPs to enter the market more widely and in a pan-European (SEPA) harmonised way.

In this world of overlay services, banks run the risk of being increasingly disintermediated (see Figure 3), degraded to commodity providers and losing many transactions to TPPs (e.g. through wallet-to wallet, in-game or mobile-to-mobile transactions without any connection to the bank account) .

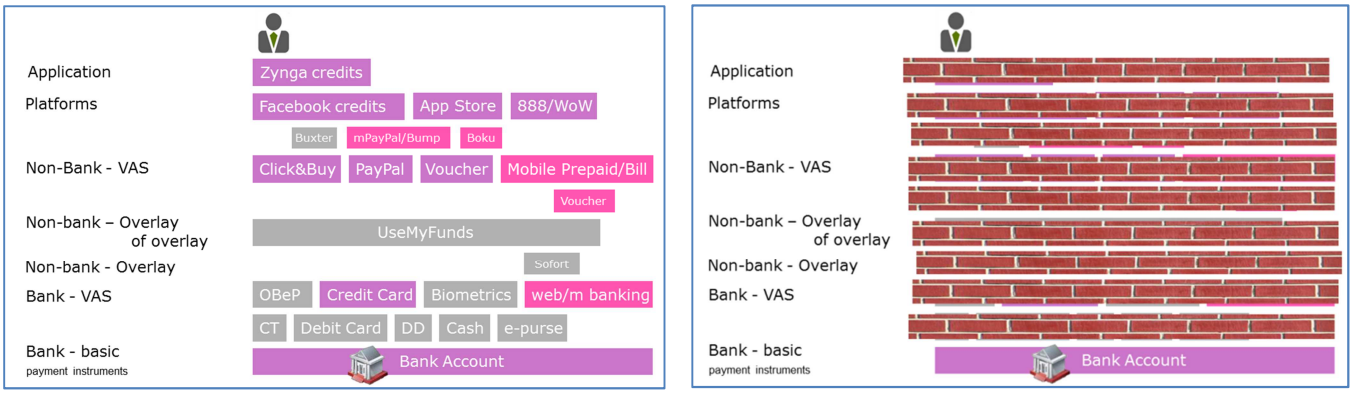


Figure 3: Illustration of the current layers between the consumer and the bank account - Banks being disintermediated online
[Source: Equens 2014]

AT Kearney predict that through this effect one third of banks' revenues will migrate to these non-bank players (See Figure 4):

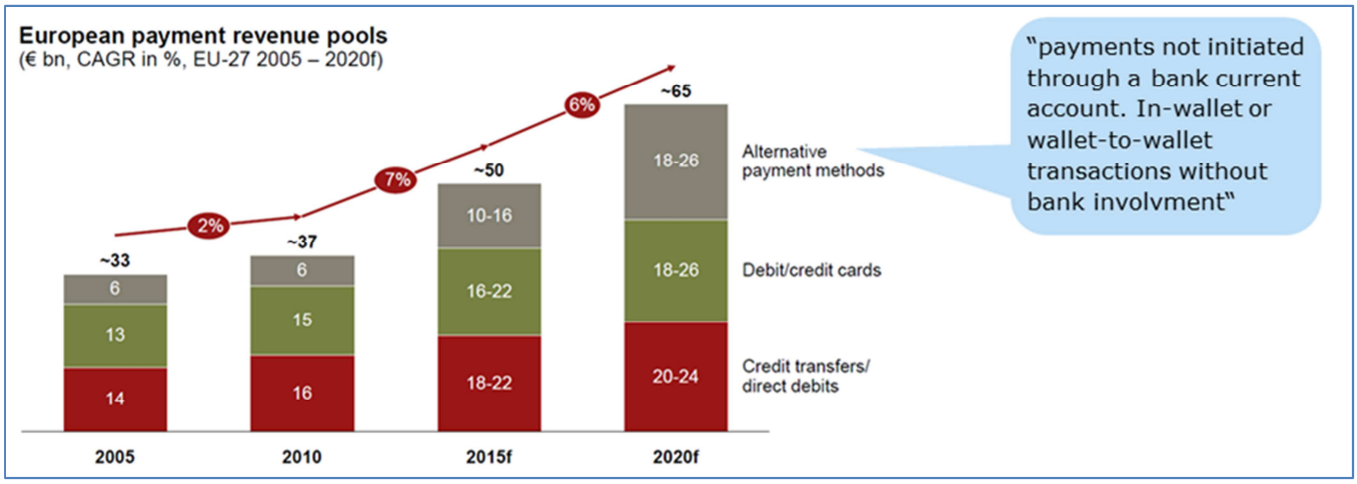


Figure 4: Payments moving to Third Parties – away from Banks
[Source: AT Kearney European Payment Strategy Report, May 2013]

Thus also banks have an interest in consumers (or their applications) using the customer's bank account *directly*, see Figure 5 (via a standard payment service interface) rather than the current multiple layers of third party intermediaries:

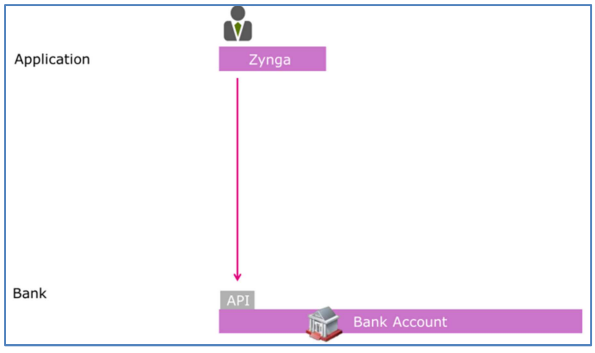


Figure 5: With CAPS/API the user's application goes straight to the bank account
[Source: Equens 2014]

Controlled Access to Payment Services – CAPS

If bank accounts (or online payment services) are to be opened up to third parties (as the new PSD stipulates, and as may be of benefit to the market and the banks as shown in the first section) this must happen in a controlled, secure, trusted, safe and fair way. An analogy may be seen in the app store model provided by e.g. Apple or Google (see Figure 6).

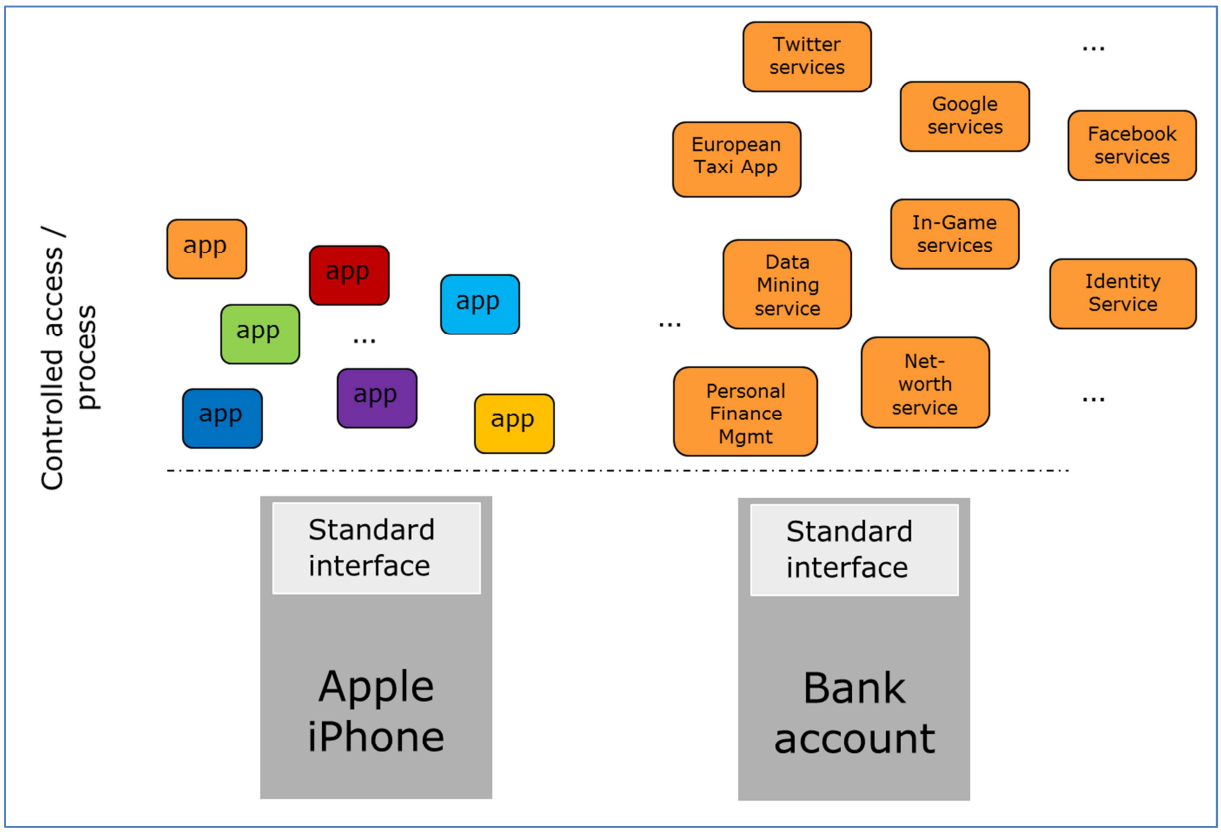


Figure 6: The App-Store model: Payments as a Platform
[Source: Equens 2014]

What they do is to provide a platform with a common standard and interface and allow third parties to develop applications under a well-defined set of rules. These rules specify i.a. what the liabilities of the parties are, how the revenue is shared, how conflicts are handled in a harmonised way – to the benefit of all. This is highly attractive for both developers and Apple or Google, as a clear commercial framework ensures benefits sharing and a worldwide standardised platform ensures harmonised use, rules, communication and distribution. It has also led to an explosion of creativity and innovation benefitting Apple, Google, their users, the developers and the whole market. The important thing is that this access is not open to everybody but only to those who comply with the rules. And thus since everybody can calculate their risks and have a benefit, everybody aims to enhance the system and everybody wins.

The alternative is that the banks are forced, against their will, to provide the new services in a risky way (without commitment to a joint a legal framework to regulate liabilities etc) and/or for free. Despite being unsafe and unfair, this would also be a major tactical mistake: it will only lead to years of open and covert battles, resistance and wrangles - and everybody loses. Instead, as proposed here, let a fair and safe infrastructure develop and everybody wins.

Especially in payments one particularly critical issue is security: no consumer or bank would endorse a situation where unregulated third parties would be granted uncontrolled access to users' accounts. This is why this paper develops the need for a Controlled Access to Payment Services, with CAPS as the acronym. This is in contrast to current practices where the users' full online banking credentials are passed on to third parties allowing them potentially full access to everything on the account: past history, salary incomes, security settings etc.. It cannot be in the interests of the user and of a secure financial ecosystem to allow access to an *account* (XS2A) – instead we should insist only on certain controlled, secure, individually controlled *payment services* (CAPS).

The new payment services defined in the PSD (information on funds, payment initiation) must only be permitted under specific conditions to ensure the risks will be contained. This is essential since, if the infrastructure were to be compromised, all electronic funds would be endangered, posing not only a risk to users and banks but even a severe systemic risk to society and the economy. For this not to happen, some prerequisites for the success of CAPS need to be fulfilled. Third parties need to be certified and regulated by PSD2. There need to be contracts[2] with banks and merchants in place that clarify the liability partitions etc. This is clearly seen jointly by Customers, Merchants and Banks [2]. The negotiation on the degree of access, quality of any guarantees etc could be based on a mutually fair "dual consent" system such as described in [3]. The system needs to be secure, handling access to accounts in a controlled way with authentication being given only for specific accesses. Transactions need to be entirely controlled by consumers to avoid a situation where consumer account data is exploited without permission. And last but not least, there needs to be a fee attractive enough for all parties, including merchants, banks and TPPs, to provide the infrastructure, develop innovative services and provide customer support. But what would be a fair price? This is a discussion of its own, and no definite answer can be provided here. However it seems only fair that cost-based fees in recompense for the infrastructure be set for basic services (e.g. yes/no answer to a query on availability of a fund) and value-based fees for premium services (e.g. to allow TPPs to do extensive data analytics or send guaranteed payments across Europe)[3]. No-one can expect the premium fees extant in the Apple, Amazon or Vodafone ecosystems (where 40-60-80% margins are de rigueur), nor the margins that some perfume and clothes retailers command, but modest[4] and fair recompense to the banks (like the "last mile" charge for third parties to use the incumbents' telecommunications network) seem only fair and reasonable. Let the market forces decide.

According to the PSD, the initial CAPS services will likely focus on two types: balance information/sufficient funds requests and payment initiation (though more can be envisaged, see Figure 7):

Service	Acronym	Parameters in	Result out
Payment initiation	CAPS-PI	from IBAN, to IBAN, amount, [QoS] TPP cert	CT initiated w best effort [guarantee, real time, ...] /insufficient funds/other error
Sufficient funds	CAPS-SF	IBAN, amt, reserve time, TPP cert	yes/no, reserved until <timestamp>
Balance information	CAPS-BI	IBAN, TPP cert [all accts=y] [past=n days/all]	balance[s], [past statements]
Account verification	CAPS-AV	IBAN, TPP cert	yes/no account exists
Identity information	CAPS-II	type of info requested, TPP cert	age verification, identity verification, postal address, mobile number, ...
Sign service	CAPS-SS	IBAN, doc/mandate, TPP cert	confirmation (e.g. mandate number) or fail code
...	...	...	...

Figure 7: Potential CAPS standard services
[Source: Equens 2014]

The former requires parameters of the IBAN, amount, reserve time and TPP certificate (reliably identifying third parties to ensure that only trusted/regulated players may ask for the account information in the name of the user). The payment initiation service needs two IBANs (from/to) and optionally a quality of service (best effort, guarantee, real time etc) ruling the funds transfer. Through these services an application can directly access the bank account without the need for multiple layers in between (as was seen in Figure 3). Several options exist for physically implementing such a standard interface, ranging from a pan-European standard API across all banks to local solutions such as these services being provided by iDeal in the Netherlands. Unsecure techniques (e.g. “screen scraping”) where a third party impersonates a user versus the bank must clearly not be allowed. In the interest of TPP developers and in line with a harmonised pan-European SEPA vision, the variability of standards across Europe should clearly be minimised. A developer should be able to write an application that works across all European banks in a harmonised way (avoiding individual interfaces for each of the 7000 banks). The TPP should contract (for reasons given before) with contract aggregators, speaking for and bundling banking groups across Europe, to avoid having to negotiate with each bank individually. The above rules and control are imperative for account access to work and CAPS can provide some cornerstones of a framework within which the full potential can be unlocked.

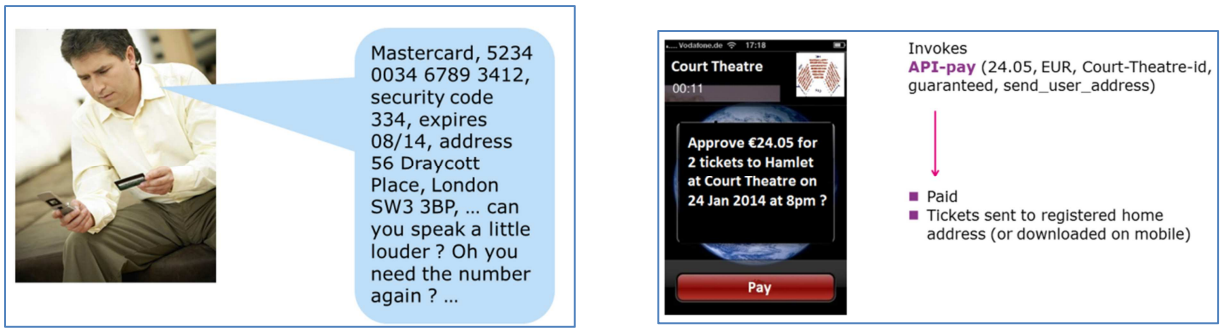
This *controlled* access to specific payment *services* (as opposed to a free access to *all* data and settings and information on an *account* as the term XS2A suggests) is infinitely safer and overall better for users from the current situation where online banking credentials are passed on to often unregulated third parties who can then potentially do *everything* on the user's account. Thus maybe the misleading and potentially dangerous "XS2A" term should indeed be dropped in favour of the safe, controlled term and concept "CAPS".

The Future is Already Happening

Although even this controlled access to payment accounts by third parties may sound very disruptive and futuristic, there are already some examples from the payments industry that today demonstrate this potential of open innovation. PayPal has already opened up its services to the developer community in 2009, allowing developers to leverage PayPal assets for innovative services. Indeed PayPal actively invites third parties to develop new and creative ideas on how to use their payment services – they even host developer conferences and sponsor competitions to energise the payment market. The provision of the PayPal payment APIs, supporting tools and a community network has already led to some interesting services, including Venmo, Playspan or Expensify. Not only new innovative third party providers are attracted to this: the API has also enabled more traditional payment players (Discover, Moneygram) to deposit/withdraw funds easily to/from PayPal. Coinstar counting machines to be found in many US supermarkets allow the coins deposited/withdrawn to be added/taken out of PayPal accounts. Greendot (prepaid voucher cards) and many more specialist developers are jumping on this opportunity to grow with PayPal. PayPal already has several hundred partners enrolled and is known to be in talks with Google, Facebook and large internet and mobile players to allow their services to be charged to/from PayPal (rather than clumsily inventing their own wallets (Google) or own currencies (Facebook)).

But it is not only PayPal that has understood the potential of opening up. Selected banks are also active in the field, for instance Crédit Agricole with controlled access to CA Connect and co-creation of services between consumers, developers and the bank. Crédit Agricole has signed contracts with independent developers and makes their apps available on the CA Store. Since its launch in 2012, this offering has already attracted more than 50 outside companies and individuals who develop applications on the platform. These "digiculteurs" create new applications (like "Pimp ma banque") in less than 3 months.

CAPS will allow for secure and convenient use cases. Instead of laboriously entering credit card details, CCVs, 3D secure codes, home address, title of registered name etc the consumer could simply get a screen like "Approve €24 for 2 tickets to Hamlet at Court Theatre on 24 Jan 2014 at 8 pm?", click "Pay"[5], and that's it. When paying within an app, the consumer will need to provide their bank credentials once and can grant permission for this app to access the balance on any future occasion (see mock-ups in Figure 8).



- User **starts app** to buy something, to get some information, …
- The **app calls an API** e.g. "send x€ from user's account to IBAN/BIC-y„
- This invokes a **reroute** to the user's **banking app**
  (The first time, the user is asked what his bank is, via drop-down/type-in list; this is then stored in app/device for future)
  - The **banking app verifies** the legitimacy of the invoker (**TPP** securely authenticated)
  - **User** logs into his banking app with his usual **bank credentials** (e.g. PIN)
  - User sees his current balance (to see if he can afford the purchase)
  - **User authenticates** payment of x€ to y with usual bank **transaction** credentials (e.g. one-time TAN or biometric finger scan)
  - This initiates a SCT
  - The **banking app returns control** to the TPP which **securely informs** the merchant app that the **SCT** was **initiated**
- The merchant thanks the user for his purchase

Figure 8: Sample Use case – "now" and "future with CAPS" with associated internal flow
[Source: Equens 2014]

And there are many more – highly to be controlled - services one can think of, like a balance query across multiple banks by the consumer to get instant "net worth" status and allow better cash balancing/management across accounts, an e-mandate, or indeed more general signing service, or an information request that builds on online banking credentials to authenticate the consumer in wider non-banking scenarios (eID rather than the current dozens of userids and passwords), provide a bank-verified postal address to the merchant, or his bank-verified age (as opposed to the current ridiculous "I am over 18" button click), the mobile number or other pieces of data in a secure and controlled way – always under full user control. (See summary of some potential CAPS uses cases in Figure 9) These provide very valuable services to merchants via the TPPs and thus solve many problems in current e/m-Commerce and thus finally add tremendous value, security and convenience to users and the online economy.

Payment

1. An online room booking via AirBnB on mobile/tablet/PC invokes API to make **guaranteed payment** for room. Allows AirBnB **to accept customers from all banks**. Customers **don't have to set up separate wallets** and get **bank grade security**.
2. cross/upsell: a consumer buys at a web shop an expensive TV and gets a payment options in installments. **In real time a personal loan is issued (**based on **name, address, income and date of birth** details as registered at his bank**) and the merchant receives the full amount.**

Information

3. a consumer **aggregates** his payment information **from multiple banks** at a third party service. Recommendations are made how best to **balance funds** across accounts.
4. Allowing a third party access to my accounts to **analyse** how much I am spending on **insurance per month**. Recommendations how to **optimise**.

Identity

5. The bank API, verified by banking credentials/PIN/ thumbprint/voice/… **proves it is me** and allows **single sign in** to web sites (not different mechanisms and password for each), **access**/opens doors, …
6. A consumer buys at a webshop. Using his bank credentials, the consumer **does not need to fill out new forms,** the **merchant can rely on the data** provided (**automatic shipping address**, …)
7. A consumer **proves he is of age** and is granted access to age restricted material/services

Figure 9: Sample use cases from CAPS
[Source: Equens 2014]

The PSD2 proposal answers some questions but creates others

The PSD2 proposal lays the foundation for CAPS in many ways. Article 58 clarifies that access to payment account information will need to be granted. The PSD2 defines new actors in the payment space, the third party providers ("TPPs"), offering payment information and initiation services to consumers and merchants and includes these TPPs in its scope. These TPPs will thus need to become licensed and registered and underlie security and consumer protection requirements similar to banks insofar as the PSD is concerned. This is an important step towards a safe and level playing field in payments. The TPPs will be obliged to refund the amount in case of unauthorised transactions, take full responsibility for the parts of the transaction under their control, ensure the user has full control of information accessed and refrain from storing these or passing them on. In general, the PSD is now extended to cover all transactions made through IT devices (mobile, internet etc.) which were previously exempted.

In general the requirements on third parties to enter the payment space without endangering customers or the financial system are:

Third parties
- Are **regulated** (PSD)/certified
- Are **committed to joint legally binding arrangements** in an open, non-discriminatory way with bank, merchant to ensure liability partitioning, joined up user communication, dispute resolution, ...
- Are **secure** (cf SecuRe Pay), preserve **privacy**, reliably **identified** (no impersonation), …
- Are fully under **user control** (allow who to see what)
- Pay **fee** (use of infrastructure, new service etc.)

As one can see, there are still some white spots where further clarification is needed. First and foremost, no cornerstones for contractual agreements between banks and TPPs have been specified. A legal framework will however definitely be needed to specify liabilities, contact points, fees, redress procedures, harmonised communication, dispute management, etc. in the interests of all market participants.

A wealth of opportunities – with potential to benefit all parties

The emergence of overlay services building on bank infrastructure has led to a very layered online payments landscape, as Figure 3 illustrated. Several overlay service layers have driven a wedge between the consumer and the bank, sometimes easing the way consumers pay, but often confusing them with multiple virtual accounts, wallets, passwords etc. Banks are clearly being disintermediated in online payments and need to act. The underlying conviction is that a world where both transaction volumes and customer value are maximised is one with a key role for banks. Providing a standardised controlled access to the bank account can help reduce and simplify the multiple layers observed today and provide new value to both banks and alternative providers. The value creation potential is seen across the board. Merchants have been looking forward to this and demanding it unequivocally[6]. In a recent survey conducted within the Payments Innovation Jury, the experts were asked to name the biggest technology trend that is driving innovation in payments (see Figure 10) showing a large sector who consider open APIs as the key trend:

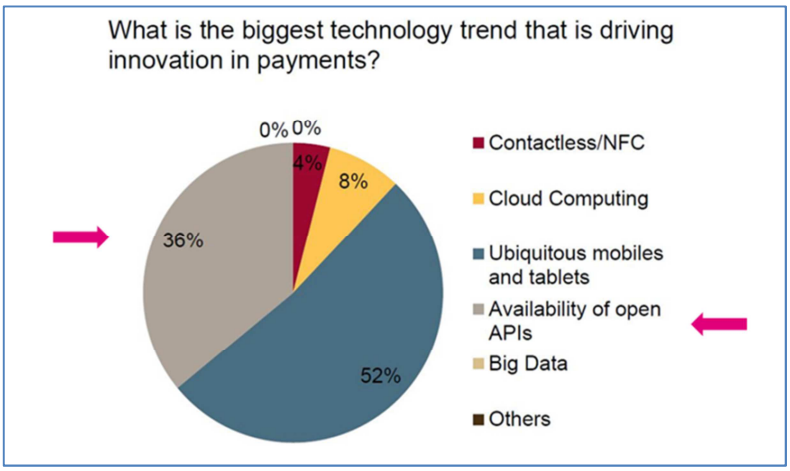


Figure 10: Innovation expected by Experts: Open APIs large driver
[Source: The Payments Innovation Jury Report 2013]

Consumers need not pass their banking credentials or card details on to merchants any more, the amazing resilience of cash [4] even in modern economies[7] can be reduced and many advantages more. Given that we already witness over 300 e-payment mechanisms in Europe today, innovation and competition will likely explode thanks to CAPS in the years to come.

The Way Forward

The next steps that can be considered by the stakeholders could be:

- the **regulator** must clarify some of the open issues[9] in the new PSD2 whilst leaving enough room for the market to manoeuvre. The latter means, for example, not laying down any technology-dependent security features, not specifying how the parties are to be contracted, leaving commercial arrangements up to the market participants (e.g. fair price, revenue sharing) etc.
- **banks**, beyond implementing what they are forced to by PSD2, could embrace this development and actively assist TPPs for example by hosting developer conferences (as Paypal does) to ensure that the new services are used and to promote common understanding of business rules and technical interfaces.
- **coalitions of the willing** between banks, TPPs, infrastructures/service providers and other relevant stakeholders could be formed to define common business rules, fair and open ways of working together to ensure that TPPs can unfold their full potential, that banks benefit for providing the basic underlying service and data, and that users have a secure and convenient interface for new services. The EBA may then wish to consider the results of this work as a basis for the future in the context of their mandate of the PSD.
- the **infrastructures/processors/service providers** could come together to agree on a common service layer (possibly like the CAPS APIs of Figure 7) so that developers can produce new apps, according to the app-store model, across Europe in a standardised way without having to tailor individually to the specifics of each of the 7000 banks in Europe.
- **standardisation** bodies such as ISO could develop standards inspired by the above ad hoc industry agreements. Note that the usual – other – way round (first many years of standardisation, then many years of interpretation/refinement to reality and implementation) has been shown not to work as well. The Internet and Mobile phone networks were established by companies first agreeing on the simple TCP/IP and GSM agreements, implementing them, and then letting the standardisation bodies loose afterwards.

If all stakeholders work together in this constructive way – in analogy to the Apple and Google app store models – we will see an explosion of safe, secure, innovative new services for users based upon bank and payment infrastructures. The European Digital Market, the developers, the infrastructure providers, the users and banks all win.

The disruptive potential and business opportunity from opening up accounts to third parties is not to be underestimated. New revenue streams will evolve and given the past history of open systems we expect that banks will benefit themselves (indeed may be the main beneficiary) from this dynamic environment – if they position themselves in a timely and proactive manner. It is fruitless to wait and see, or to try and resist until being forced by the regulator to open up in a way that might not be the best in their interests and for consumers and

merchants. If open access is an inevitable step, then banks should act already now to secure a vital role in the future of payments. It is not about fighting for a larger slice of a given pie, but about jointly growing the pie with the potential to make all parties better off. Banks could benefit from this by cooperating with the market and the regulatory authorities in order to get the rules right (and that includes the currently critically missing contracts and fair revenue sharing)[8], positioning on the value chain, designing own service offerings, and seeking for partnerships with TPPs. "Coalitions of the willing" between banks, TPPs, merchants and other market players are now being formed to encourage and shape this. All this can lead to an open yet controlled and secure environment where banks, payment service providers, merchants and customers are the joint winners and, as has been shown also in other industries, much better off than today.

- END -

It is better to disrupt yourself rather than to let others disrupt you

It is not about fighting for a larger slice of a given pie, but about jointly growing the pie with the potential to make all parties better off

Let a fair and safe infrastructure develop and *everybody* wins

The disruptive potential and business opportunity from opening up bank accounts to third parties is not to be underestimated

Notes and References

[1] The proposal amends Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repeals Directive 2007/64/EC

[2] A "contract" in the sense of this paper should not be seen as a traditional bi-lateral signed agreement (since this is clearly impractical given the large number of banks, TPPs, merchants, users). However a joint legal framework, however implemented, needs to be in place to clearly define the rights and duties of each party and commit them to their part of the total solution. This serves to specify jointly between the parties the limits of responsibility, liabilities, compliance, branding, contribution to harmonised communication, fault resolution, redress procedures, user management, security, archiving, commercial arrangements, contact points, dispute resolution and any other issue to ensure the smooth and joined up functioning of a system involving several parties.

[3] Merchants agree to a fair apportionment of value, even for basic services e.g. „Banks could charge a reasonable fee for the yes/no service" according to EuroCommerce „Basic Payment" Paper of August 2012

[4] See, for example and by comparison, the 0.2/0.3% the debit and credit charge interchange fees that are regulated for payment card service

[5] Or whatever security regime is agreed with the bank. This will in future be governed both by the SecuRe Pay recommendations of the ECB and whatever arrangements the bank makes with its customer. This can range indeed to the simple "pay" button if the user/his mobile is known and the risk/amount is low - up to a fully-fledged n-factor authentication for first-time usage with high risk/amounts/new clients. In this context it is critical to strike a balance between usability and risk/security. This is especially critical on the mobile – which is not suitable for long interactions and questions the use of additional external physical security devices/tokens/card readers common in online banking security. Fortunately it is exactly the mobile that offers many unique identification and verification possibilities (identification via sensors, personal identifications, behaviour patterns, preferences, secure binding of app to device, biometric recognition of voice/movement/usage/finger/face/ear/gesture, location/movement data, device fingerprinting, social graph etc) thus potentially making the reliable identification of the user possible both securely and conveniently (normally a contradiction). A unique advantage of the mobile device.

[6] "new non-banking providers must have secure access to account data" says the EuroCommerce position paper 2012, "web merchants encourage banks to 'open up their accounts' for third party merchant services, fostering innovation and competition" says E-commerce Europe 2012, and two of the Top10 requirements of the E-Payments Merchant initiative is "international and interoperable OBeP solution based on SEPA" and "clarity on the status of overlay banking services (security vs competition) and required standards".

[7] Even in a modern economy like Germany, 82% of all retail payment transactions are still in cash! [Bundesbank Statistics] The cost of this cash in Germany is estimated by Steinbeis University to be 12.5bn€ per year (of which 4.5bn€ are paid by banks, 6.7bn€ are paid by retailers and 1.3bn€ by consumers – every year). This is not only incredibly inefficient and a waste of resources but is also socially unfair. Reducing cash can only be achieved by banks and creative third parties coming up with convenient, safe and easy to use electronic alternatives.

[8] Not that these "missing" items should be specified in the regulation. Indeed it is better to lay down only the boundary conditions and cornerstones in the PSD ("principle regulation"). One is surely well advised to leave the detailed implementation (technology solution, security methodology, legal framework, commercial arrangements, …) out of any regulation and thus flexibly up to the participating parties and the market as solution maturity, user awareness, risk development/fraud attacks, technology etc develop.

[9] Regulator to even out the very variable regulation (where some topics are laid down in enormous detail, leaving other important questions totally open): Are all banks obliged to implement XS2A (e.g. even those without online banking) ? Clarify that transactions can only be authorised before, not after (§57.1); What about TPPs outside the EU ?; Clarify that the user cannot be an enterprise; Clarify use of separate credentials (esp if to be used beyond banking, e.g. eGovernment); Rejection by banks of TPPs with excessive errors/fraud; Clarify that screen scraping no longer permissible; etc.

[1] “The Future is Open”, Jonathan Rosenberg, Think Quarterly – The Open Issue, Google, October 2012, http://www.google.com/think/articles/the-future-is-open.html

„In 2009, Jonathan Rosenberg, then Google’s SVP of Product Management and now an advisor to Google management, wrote a memo outlining why open companies would win the future. Today, however, he finds a world that has outstripped even his wildest expectations.”

[2] Joint “Position Paper on the Issue of Access to the Payment Account”
by Consumers (Consumentenbond), Merchants (Thuiswinkel), leading payment scheme (Currence), National Bank (De Nederlandsche Bank) and Nederlandse Vereniging van Banken, April 2013, http://www.dnb.nl/binaries/711785_PositionPaper_tcm46-290153.pdf

[3] “A Dual Consent Approach for x-payments”, Ron Berndsen and Daaf van Oudheusden, De Nederlandsche Bank, Amsterdam, April 2012,
http://www.dnb.nl/binaries/A%20Dual%20Consent%20Approach_tcm46-273056.pdf

[4] “Why is the use of cash persisting? Critical success factors for overcoming vested interests”, Michael Salmony, JPSS Journal of Payments Strategy & Systems. Vol 5 No 3, April 2011, http://www.equens.com/Images/Salmony%20JPSS%20Oct%202011%20-%20How%20to%20replace%20cash.pdf

[5] “The Concept of an Open Standard Interface for Controlled Access to Payment Services (CAPS). Access to accounts – why banks should embrace an open future.”, Michael Salmony, EPC Newsletter Issue 21 January 2014
http://www.europeanpaymentscouncil.eu/article.cfm?articles_uuid=42210000-5056-B741-DB0CD1AA4E9F34EA