Access to accounts: benefits for banks of an open future

In this article, Dr. Michael Salmony of Equens SE, a pan-European payment processor, provides his perspective on the recent access to accounts initiative proposed by the European Commission. Michael argues that open access to bank accounts has the potential to lead to an explosion of potentially disruptive innovation, competition and new services, but that banks need to position themselves proactively in this new environment.

On 24 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 Second Payment Services Directive (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.

When IBM pioneered information technology in the last few decades, their initial approach was to build a closed system. But only when IBM and others opened up (through the advent of the open internet) did the IT revolution really gain momentum. The market share of the (open) Google Android operating system has surged to around 80% globally, again demonstrating the inexorable rise of open systems. 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). 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 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. In view of the success of PayPal, 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. 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.

Most of the current 'winners' in online payments are overlay services riding on bank infrastructure. These alternative providers face difficulties establishing innovative payment solutions for example 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, degraded to commodity providers and losing many transactions to TPPs.

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) this must happen in a controlled, secure, trusted, safe and fair way.

The important thing is that this platform access is not open to everybody but only to those who comply with the rules. 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. 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. Third parties need to be certified and regulated, e.g. 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. The negotiation on the degree of access, quality of any guarantees etc could be based on a mutually fair 'dual consent' system. 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.

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].

The fight in online payments is not lost to anybody, but all players (especially banks, the current incumbents) face significant opportunities that should now be addressed

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 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 let a fair and safe infrastructure develop and everybody wins. Especially in payments one particularly critical issue is security. This is why this article develops the need for a Controlled Access to Payment Services (CAPS).

According to the PSD, the initial CAPS services will likely focus on two types: balance information/sufficient funds requests and payment initiation. 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. 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 the 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 and also maybe in a harmonised way across credits/debits and card payments). 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.

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, selected banks are already 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.

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 8pm?' click 'Pay,'[4] and that's it.

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, including checking and card accounts. The PSD2 defines new actors in the payment space, the 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 under lie 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 this or passing it on. In general, the PSD is now extended to cover all transactions made through IT devices (mobile, internet etc.) that were previously exempted.

Conclusion

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 best for their interests and for consumers and merchants. If open access is an inevitable step, then banks should act 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)[5], positioning on the value chain, designing own service offerings, and seeking 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 also been shown in other industries, much better off than today.

Dr. Michael G. Salmony Executive Adviser
Equens SE
michael.salmony@de.equens.com

This article first appeared in the Journal of Payments Strategy and Systems Volume 8 Number 2 (http://www.henry stewartpublications.com/jpss). Cecile Park Publishing wishes to thank Henry Stewart Publications for the permission to publish this abridged article in the E-Finance & Payments Law & Policy journal.

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 the EuroCommerce 'Basic Payment' Paper, August 2012.
4. 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 from 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, location/movement data, 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.
5. 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 etc) 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.