Setting up pan-Europe mobile P2P payment solutions

Over 50 mobile peer-to-peer payment solutions ('mP2P') have been launched in Europe; these solutions allow payments to be initiated via users' mobile devices using a contact's mobile number, but tend currently to be limited by geography. Dr. Michael Salmony, Executive Adviser at Equens SE considers the setting up of a pan-European mP2P service, which would enable the transfer of money without geographical restriction within Europe, and discusses the requirements and issues involved in setting up such a service.

The increasing proliferation of faster/instant payments and of mobile phones begs the question as to whether money cannot be transferred more easily, quickly and safely between people than with current methods. Today people hand each other cash, write out cheques, initiate online bank transfers using bank account numbers (such as IBANs), enter card details (16-digit numbers with added security codes) into little web browsers and more - would it not be better to send money by clicking on a mobile contact? We all have the mobile number of our contacts (unlike the IBAN) and initiating a payment from our ever-present mobile devices - if done securely and conveniently - is surely the future.

mP2P solutions are typically local, working only in a particular geography (e.g. Swish in Sweden). Under the Single European (Digital) Market it seems apposite to think of pan-European solutions allowing anyone in Europe to send money to anyone else independent of either's geography. Thus it is only consistent that the European Retail Payment Board ('ERPB'), comprised of representatives of all key payment stakeholders and chaired by the European Central Bank ('ECB'), has identified the promotion of pan-European mP2P as one of its two current strategic initiatives.

This article discusses some of the considerations in setting up such a pan-European mobile payment service.

Approach

A solution could be based on many infrastructures (cards, ACH, etc.), initiation/identification methods (QR codes, phone numbers, social media handles etc.) and technologies (tapping phones together, sending SMS, etc.). However, since bank accounts and mobile phones are likely the most pervasive across Europe for the purposes of this article we consider only initiating a bank transfer via a mobile phone number. For this a mapping service has to be set up that maps any mobile phone number to any bank account (IBAN) in Europe. This would mean that users of local solutions could then not only send and receive money within their local community (e.g. within the UK), but could in future send and receive money anywhere in Europe - with their accustomed local solution. This would enable not only classical cross-border mP2P payments (e.g. paying a friend in Portugal from Germany) but also allow a traveler to pay in a foreign country (e.g. a tenant from the UK to pay the landlord of his French holiday home).

Typical application

The typical paradigm in mP2P is that a user invokes a banking or payment app on their smartphone where they enter the amount to be transferred and select the intended recipient from their contact list. 'Behind the scenes,' this mobile number is translated into a destination bank account. This is typically done by a distributed database service, currently mapping local phone numbers and accounts, but in future accessible from anywhere in Europe.

For practical reasons it may be best to map not only the phone number into an account number, but also return the name of the account holder. Thus when the user selects a mobile number to send to, the system will return to them - before the payment is initiated - the name of the person that the system has associated with that number. The user can then verify that this is indeed the person they intend to send the money to and then press 'send money' and thus the money is sure to reach the right recipient. Any manual 'typos' in the mobile number, accidentally selecting the wrong contact, outdated mobile numbers in contact lists on the personal mobile, a user who has forgotten to deregister his mobile from his local directory, the telco reassigning an unused number to another user, etc., then do not cause erroneous payments to the wrong recipient. This avoids frustration for the users and expensive dispute resolution procedures for the providers.

Some communities - with very stringent privacy policies - have elected not to return the name of the user from the lookup. Other communities consider returning the photo of the payee to be less sensitive, etc. Maybe this issue of what is considered private and what is not will be better resolved once we have more harmonised privacy legislation across Europe.

The above already indicates the need to look at the topic of mP2P not only from a technical perspective (e.g. a database mapping service) but also - more

importantly - from the many non-technical perspectives.

How does one reconcile different privacy preferences across communities and users? What is the business model? Who decides who can take part in the system? Does the mP2P initiate a standard SEPA Credit Transfer ('SCT') - maybe with an immediate guarantee - and/or are funds immediately available for further use? Who can change entries in the databases? What happens if something goes wrong - i.e. how to resolve disputes and define liabilities? How does one communicate the pan-European solution to users? If two accounts are associated with the same mobile number, which one is to be used? etc. These are some of the many important, non-technical questions.

Some of these issues are already covered in the underlying payment scheme (e.g. SCT, in future real-time enabled) at least as far as the interbank sphere is concerned. As it makes sense to base the new mP2P solution on existing standards (ISO20022, ePI, etc.), existing solutions and existing governance structures, it is worth considering the possibilities to re-use as much of this scheme as possible.

We here single out only a few such considerations of particular relevance to these non-technical changes/additions vs. the basic SEPA Credit Transfer ('SCT') scheme relevant for mP2P.

Privacy

Clearly the system needs to conform to local and European data protection legislation[1]. In particular any data in any system must only be made accessible to those actors and for those purposes authorised and agreed with the user. Data can only be used/inserted/edited with explicit consent from the user. No data may be retained beyond its need and no data beyond what is needed can be stored. There must be a right to be forgotten, etc.

A mapping service has to be set up that maps any mobile phone number to any bank account (IBAN) in Europe. This would mean that users of local solutions could then not only send and receive money within their local community (e.g. within the UK), but could in future send and receive money anywhere in Europe

One consequence of this is that it will likely not be possible to enrol users automatically into the mapping service - even if this were technically possible (the bank typically already having both the customer's IBAN and their mobile number).

Thus although it would aid the uptake of the mapping service immeasurably if everyone were automatically registered (with the possibility to opt-out), this cannot be recommended for privacy and data protection reasons. Instead the explicit consent of each consumer must be sought, as to whether they are ready to accept that their mobile number will be associated with their IBAN and made available to those seeking to send payment. Many solutions in the market have failed by not implementing this solution legally, elegantly and conveniently, and by not making the advantages (and risks) clear to the user and this must thus be a point of very special attention.

The solution that balances both convenience and KYC/privacy may be found in modern bank-based solutions: the user has already been vetted and can thus, with a simple 'tick' in their mobile banking app - once - confirm that they are interested in receiving money from others and thus enrol conveniently in the system. It must be made clear, of course, that in so doing they are making their name potentially visible to anyone who has their phone number and are thenceforth subscribing to the T&Cs of the service.

Security

Since the pan-European mapping service contains the account numbers and mobile phone numbers of many people[2] in Europe it will be a 'honeypot' for hackers.

Thus all conceivable security measures must be adopted to ensure that no unauthorised party can access any lookup service, modify any entry or penetrate any database. Thus only special selected parties (who need to be specially vetted, maybe even licensed, and continuously monitored) can be allowed to access the mapping service and manage the mapping between phone numbers and account numbers through a standard, highly controlled interface.

Of course, not only external access (e.g. capturing of IBAN by unauthorised parties) but also the 'internal system' of the solution must be heavily protected against cyber attacks e.g. database pollution, unauthorised modification of entries, etc.

Liability, dispute handling, branding, governance, and business model, etc.

Since any of the above topics can 'go wrong,' it is necessary to have a structured dispute handling process to assess where the problem is, how to resolve it and who is liable to redress any damage.

It is to be evaluated whether a pan-European mP2P service needs a brand to make it recognisable across Europe. It needs to be decided who bears the costs for the maintenance of the local data and the distributed service. It must be assured that any mP2P specifics (e.g. the lower limit than normal online banking) that suggest themselves for compliance be implemented. In short all elements of an underlying (e.g. SCT) scheme need to be reviewed to see whether any adaption for the mP2P solution may be necessary. It

should be the goal to have as few changes to the standard scheme as possible.

One critical non-technical decision that will have to be taken in this context is who to assign the management of the pan-European mapping service to and what the governing body should be. Having several parallel European mapping services (whilst welcome from a competition point of view) may lead to fragmentation and customer confusion so should be considered with care. In any case the governing body of any solution will surely wish to opt for multiple providers for competition and redundancy reasons.

Each community may also have different rationales for adopting mP2P and different business models. Some countries have government initiatives in place to reduce cash[3] - and thus see mP2P as a viable electronic alternative. Some see mP2P as a stepping stone towards mP2B (payment of merchants) with attractive business cases. Some consider mP2P as a strategic initiative to put bank accounts back into the centre of (e/m-)commerce - and not leave the critical topic of payment (and its data) to non-bank third parties.

Future of mP2P

Once the above considerations are in place and a safe, secure, easy to use pan-European payment system is emerging, it will surely not be long before the 'person-to-person' scenario is extended to paying the babysitter, the window cleaner and then merchants in general - and more.

Mobile P2P may become integrated into mobile phones (e.g. having a 'pay' button during a call to send the person on the line money immediately). Another version of 'integrated' mP2P payments we will surely see is to have the mP2P payment function integrated into third party applications. Rather than explicitly initiating a payment with a dedicated payment/banking app, the payment is part of a more complete solution including much more of a holistic workflow than just the payment step. For example someone advancing a restaurant bill may use a 'bill splitting app' into which they enter the contacts that attended the dinner. The app will then calculate how much everybody owes, request this amount from each contact, wait to be paid by each diner (using integrated mP2P in the guests' bill splitting apps), remind guests and finally show completion to the host. Technically the way this will likely be implemented is by banks or payment service providers offering open APIs for mP2P payment services to third party developers. Then anyone who can program an app can implement a function to initiate a payment from any bank account in Europe to any other. This functionality can then be integrated into a whole host of new applications that integrate mP2P payment into a wider, complete solution.

Summary

One promising way in which to build pan-European mP2P solutions is to base mP2P on a mapping service from a mobile telephone number to an account identifier and account holder name. In order to implement such a pan-European mapping service in a practical way one should leverage existing local community mapping services (over 50 exist in Europe). Setting up such a pan-European mapping service raises a number of technical issues, where existing, tried solutions and standards should be employed.

Managing such a system will require non-technical political, policy and commercial decisions to be made beyond the technical issues. It is recommended to explore possibilities to re-use existing solutions/schemes and governance structures and only extend these as far as is strictly necessary for mP2P.

Links to other relevant regulations (PSD2/API ('payment initiation from account'), SeCure Pay (mobile authentication), etc.) need to be explored. Particular attention must be paid to ensure that the mapping service conforms to all regulatory, technical and consumer issues especially to the particularly critical topics of privacy, security and data protection.

mP2P solutions will likely evolve into person-to-business and other solutions and may become integrated into mobile phones as a standard feature and become the basis for more holistic solutions incorporating payment using API technologies. Above all it is to be ensured that the system is:

a) open to all who wish to participate (technically, commercially) if the rules laid down by the governance structure are committed to (security, privacy, liability etc.); and

b) no-one is forced to use this system but free competition and an open market are assured.

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

1. Including, but not limited to, the data protection clauses from Article 8 of the 2000 EU Charter of Fundamental Rights, the EU Data Directive of 1995 and the coming EU General Data Protection Regulation.
2. Ideally, if such a service takes off as envisioned, then a large proportion of Europe's 740 million consumers will be registered.
3. If mP2P can help to reduce a little of the €86bn cash handling costs that fall especially on banks and merchants every year, a business case surely seems viable. Over 80% of all retail transactions in Europe are still cash.