EUROPEAN CENTRAL BANK

EUROSYSTEM

ERPB SECRETARIAT **ECB-RESTRICTED**

30 April 2014

ERPB/2014007

Issues and way forward with electronic mandates for SEPA Direct Debit

1. Conclusive summary and next steps

Electronic mandates (without a paper-based signature) are very widely used for SEPA direct debits (SDD) in the euro area. Although the SDD Rulebooks offer one specific way to issue electronic mandates involving PSPs, the current market practice of issuing and accepting electronic mandates are very divergent across Europe and even within national communities. It remains to be seen what effect these very diverging practises will have on the cross-border use of electronic mandates for SDD.

In payment situations where there is no physical interaction between the debtor and the creditor, direct debits in combination with electronic mandates with lax customer authentication are very intensively used in several countries for reasons of costs and perceived user convenience. There seems to be no immediate prospect of a "big bang" style of migration to models involving stronger customer authentication and in particular to an e-mandate model as described in the SDD rulebooks.

As long as no significant levels of fraud are apparent, other electronic mandate models than the one described in the SDD rulebooks (which relies on strong customer authentication) may co-exist, but – within the current (PSD) and future (PSD2, once approved) legal framework – more clarity is needed on where the burden of proof is in case an unauthorised transaction is claimed; especially the level of customer authentication applied should be taken into account.

This clarity is also important as incentive for stakeholders to converge towards stronger customer authentication methods, in line with the recommendations made by EU supervisors and overseers (the SecuRe Pay Forum) and the direction taken by the PSD2 proposal of the EU Commission.

In addition, the issue of diverging national legal requirements for electronic mandates and the apparent lack of a supportive EU-wide legal framework for cross border use of electronic signatures should be brought to the attention of the EU Commission.

More forward looking, with a view to the need for a fully integrated market for electronic mandate solutions over the long term and the need for the emergence of pan-European solutions a ERPB working group could be set up to analyse the barriers and provide recommendations.

The ERPB is invited to

- ***discuss the issues and developments with electronic mandates outlined in the note***

For the short term

- ***agree suggesting to the EPC – as owner of the SDD schemes and within the context of the current (PSD) and future (PSD2) legal framework – to consider amending the SDD schemes rules in such a way that they: a) are more open to the diverse existing electronic mandate models, b) focus on the security of the technique used, and c) are more clear on which party has the burden of proof in case an unauthorised transaction is claimed depending on the level of customer authentication applied***
- ***agree that the lack of fully supportive EU-wide legal environment for a harmonised and integrated market for electronic signatures used in payment services should be brought to the attention of the EU Commission***

For the medium to longer term

- ***agree to set-up a ERPB Working Group with the mandate to prepare a report on the barriers (and how to address these) for market integration and the emergence of pan-European solutions in the field of electronic mandates***

2. Background

In creditor-mandate-flow (CMF) direct debit schemes the mandate (representing the authorisation for payment transactions executed under a direct debit scheme) is given by the debtor to the creditor. The most obvious form of a direct debit mandate is a paper mandate that contains the signed authorisation by the debtor as well as essential further details (e.g. name of creditor, unique mandate reference, creditor identifier, etc).

As in many other aspects legacy direct debit schemes differed from each other on what requirements they set for mandates to represent a valid authorisation. Most of the legacy schemes allowed for issuing a mandate in an electronic form (i.e. via telephone, fax or over the internet) with varying degrees of customer authentication across schemes and in varying legal environments across countries. In case of the debtor mandate flow (DMF) model legacy schemes the mandate was given to the debtor bank. Thus electronic mandates in these schemes were equipped with strong customer authentication, making use of the authentication procedures used for online banking and or telebanking.

At the set-up of the SEPA Direct Debit core scheme it was understood by most stakeholders that the scheme rules will cover the requirements for mandates not only in technical but also in business terms meaning that the Rulebook will tell all stakeholders in what format they can or cannot issue or accept paper or electronic mandates. For electronic mandates the scheme owner developed a 4-corner model based on strong customer authentication (via the debtor bank online banking solution) and qualified

electronic signatures[1] of service providers throughout the chain to ensure that the authorisation cannot be challenged by anyone later on (EPC's e-mandate model).

However, this e-mandate model was not in place and was not rolled out for use by stakeholders by 1 February 2014 in many banking communities. In addition many creditors in countries with a CMF legacy model simply refused the idea of adapting to this model referring to the possibility that the interference of banks in the mandate issuing process would entail additional costs / fees to be paid. Many of these creditors argue that since the paper mandate is based on a 2-corner model (i.e. no banks are involved in the mandate issuing and accepting process) there is no need for a 4-corner model in electronic mandates either.

The EPC, having seen the opposition from many stakeholders and the slow take-up of its own 4-corner model, issued a clarification letter to scheme participants in September 2013 in which it opened up the possible set of solutions for SDD electronic mandates stating that its 4-corner model is only an option and an electronic mandate can be used for SDD even if it was issued based on other types of models.[2]

It is very important to have an agreed framework and certainty in this field as non-paper (i.e. electronic)[3] mandates (e.g. over the internet, via telephone) are very widely used both for recurrent and one-off collections, especially in the large legacy CMF markets. Most of these mandates are issued in a 2-corner model. According to rough estimations[4], in Germany, the largest direct debit market in SEPA, around 27 % of creditors accept non-paper mandates. The share of non-paper mandates at these creditors is estimated to be around 63 % of all outstanding direct debit mandates. Around 5 % of the creditors who participated in the survey in had no paper mandates at all.

3. A categorisation of existing electronic mandate models

The set-up and use of electronic mandates is very diverging across SEPA in regards to the applied technical solution, the number of actors participating in the process and the final form of the electronic mandate issued. Therefore, it is difficult to categorise these solutions based on any other feature than the number of participants in the issuing and validating process. **Although strong customer authentication can be used in all model categories described below**, in practice there seems to be a positive correlation between the probability of applying strong customer authentication and the number of "corners" in electronic mandate models.

[1] A qualified electronic signature is an electronic signature which involves certification from a third party (as well as a time stamp) in regards to the identity of the signer. Due to the very high level of encryption used qualified electronic signatures cannot be forged or altered. See further details on EU-level legal requirements for electronic signatures in section 3.3.

[2] See: http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=639

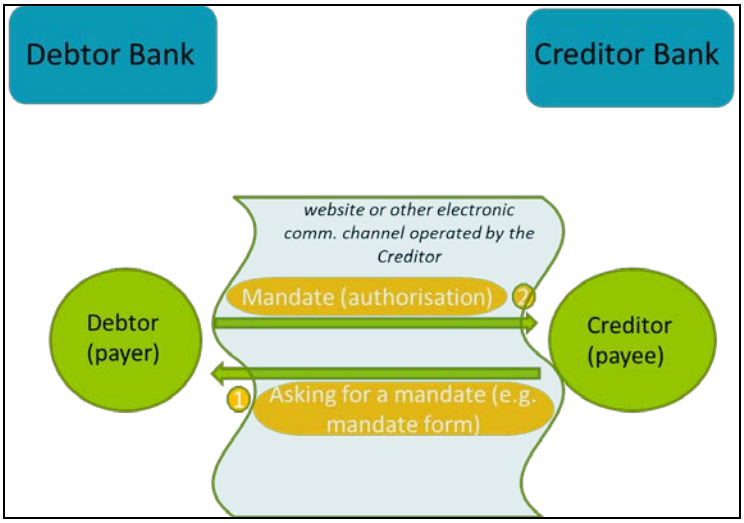
[3] This note uses the term 'electronic mandate' for all forms of non-paper mandates.

[4] "SEPA-Migration in Deutschland: eine Bestandsaufnahme" joint research by Ibi Research and BITKOM e.V., August 2013

3.1 2-corner electronic mandate solutions

The two corner electronic mandate solutions follow the basic logic of the paper mandate in that they do not involve banks or any other third party service providers. Simply, an electronic connection (e.g. online webform, or a phone call) is established between the debtor and the creditor where the debtor signals its authorisation for the collection(s).

Chart 1: The basic schematics for 2-corner electronic mandate models



In most of the cases the creditor does not carry out a prior identification of the debtor so there are no pre-agreed credentials which could be used for strong customer authentication[5]. This is especially true when SDD is used as a means of payment in e-commerce. A special subtype of this category is when the picture of the written signature is transmitted from the debtor to the creditor (e.g. a paper mandate is signed on the debtor's side, scanned and sent to the creditor, or the touchscreen of the device allows the debtor to "sign" the mandate form on the screen with his written signature). This subtype allows for a check at the debtor bank based on the specimen signature it has from the debtor.

3.2 3-corner electronic mandate solutions

Three corner electronic mandate solutions have two variants:

a) In the first case a (non-bank) third party service provider provides authentication services to creditors based on the prior registration of the debtors with this third party provider (even government institutions or post offices may provide such services to creditors).

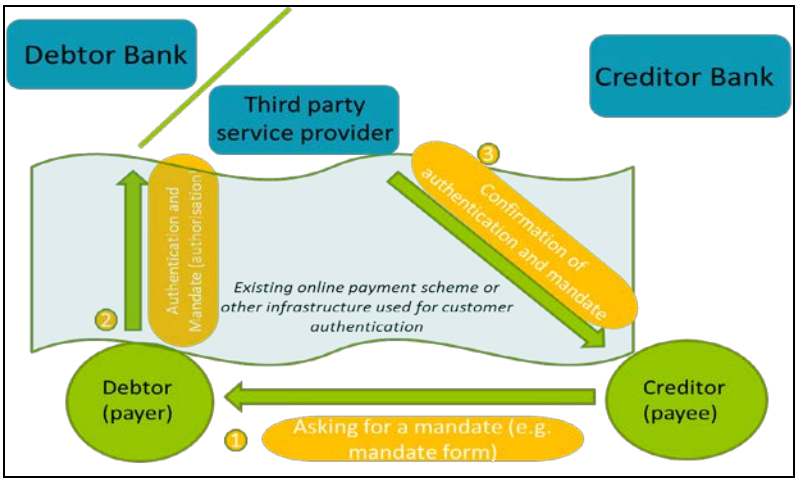
b) In the second case the debtor bank provides customer authentication and transmits the outcome via another existing (mostly SCT-based) online payment scheme (e.g. GiroPay, iDeal or Sofort) to the creditor (provided the creditor is using these services). In many cases under this variant the SCT

[5] An exception to this could be those long-lasting contracts with large creditors (e.g. utility or telco) where there have been physical contacts with the customer before the mandate is issued and / or a general purpose website is used with pre-agreed credentials to issue the mandate. In addition telcos may have an advantage for phone mandates since the nature of the underlying contract gives them a way of identifying the customer based on the phone number used to make the call.

scheme is used to confirm the identity of the debtor (i.e. a small amount SCT is made to the creditor first to prove customer authentication).

The creditor bank is not involved in the process in either of the variants.

Chart 2: The basic schematics for 3-corner electronic mandate models

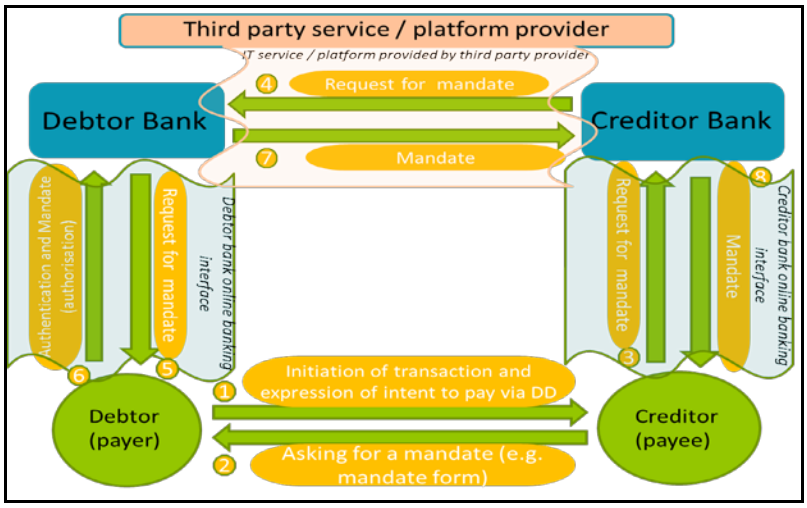


The common feature of three-corner solutions is that in most cases an existing online infrastructure is used for customer authentication and transmission of the mandate (authorisation) which had not been developed specifically for electronic mandates.

3.3 4-corner electronic mandate solutions

In 4-corner models both the debtor bank and the creditor bank is involved in the mandate issuing and maintaining process, with the former providing (strong) customer authentication based on existing customer credentials and its online banking service. A big advantage of the 4-corner model is that it provides real-time communication between the parties (which is often not the case in 3-corner models). In addition - due to the set-up - the creditor can be certain that the authorisation was actually given by the holder of the account. This reduces the probability of unauthorised transactions under the mandate to the minimum.

Chart 3: The basic schematics for 4-corner electronic mandate models



On the other hand 4-corner models are more costly to implement and they can only be used if the debtor bank and the creditor bank participates to the same electronic mandate solution (scheme). In practice the involved debtor and creditor banks outsource the operations of such a 4-corner model to third party service providers (e.g. IT service providers, operators of the technical platform used for intra-bank communication, electronic signature service providers, etc.), while keeping the contractual and business relationship with the end-users (creditor and debtor). In any case services to end-customers are provided by the payment service providers who are responsible for this service and for the third parties they employ.

3.4 EPC survey of existing solutions

The majority of respondents (mostly electronic mandate schemes or third party providers) to the EPC's survey (carried out in 2013) on existing or planned electronic mandate solutions use a 2-corner model for its service. Furthermore, it has to be noted that many online merchants are using electronic mandates in a 2-corner model without making use of any special services for customer authentication (i.e. only asking for the IBAN and the approval of the customer on their website to launch one-off direct debits). These online merchants did not take part in the EPC's survey and will most likely continue with their practice simply now using the SDD scheme.

Nevertheless, 4-corner model solutions conforming to the EPC's 4-corner e-operating model have been or are being set up in France, the Netherlands, Austria and Portugal, but are not in operation yet. In addition EBA Clearing's MyBank solution (intended for pan-European use) is currently being rolled out. Consequently, as of April 2014 the EPC's 4-corner model is still not – or just hardly – available to creditors and debtors in SEPA.

4. Legal requirements for electronic mandates for direct debits

4.1 EU-level legal environment

The Payment Services Directive (PSD) regulates high level business rules and responsibilities of parties in regards to payment services and execution of payment transactions. One of the basic principles is that all payment transactions have to be carried out on the basis of the consent (authorisation) given by the payer. The PSD allows parties to a payment service contract to freely define how consent (authorisation) is to be given for payment transactions, and does not promote or prohibit any techniques to be used in customer authentication.

However, the PSD requires that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for his

payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency.[6]

The SEPA migration end date regulation stipulates that the consent (represented by the mandate) has to be given to the payee (and indirectly to the payer's PSP) and specifies the minimum mandatory data elements to be passed on with the collections describing some features of the mandate. One of these data elements is the date on which the mandate was "signed". Some lawyers interpret the fact that the name of this data element contains a reference to "signing" in such a way that the EU legislator had the intent to make written or electronic signatures mandatory for SEPA mandates as method of authorisation. Notwithstanding the implication of this interpretation being that only paper mandates and electronic mandates with qualified electronic signatures can be given, it is unlikely that the legislators wanted to regulate in such detail the techniques of customer authentication in a technical annex of a Regulation.

4.2 Customer authentication vs. authorisation of payment transactions

It is important to distinguish the notions of **customer authentication** and **authorisation** of payment transactions. These two concepts are often confused in public discussions on validity of direct debit mandates. **Customer authentication** is the process of **identifying** the customer (e.g. payer or payee) in order to ascertain whether the person making a payment order or giving an authorisation is the same that the PSP is in contract with in relation to the particular payment service. **Authorisation** on the other hand means that a payer **agrees** to the execution of a payment transaction or series of payment transactions. The two concepts are independent in the sense that lax customer authentication (or even the lack thereof) does not mean that the transaction is not authorised. The payer can agree to the transaction even if he or she was not strongly (or anyhow) identified or authenticated by his PSP or the payee. However, the two concepts become strongly interconnected when the payer claims that an unauthorised transaction has taken place. In this case one of the most important factual element based on which the debtor bank can make the judgment on whether the authorisation can be proven or not and the refund (for unauthorised transaction) is due or not is the level of customer authentication used when the mandate was issued.

In the EU Commission's proposal for the review of the PSD ("PSD2") it is proposed to be clarified that in the absence of strong customer authentication the payer should only bear any financial consequences where having acted fraudulently. In addition, the payee or the payment service provider of the payee failing to accept strong customer authentication, shall refund the financial damage caused to the payer's payment service provider.

[6] It also has to be noted that EU Commission's proposal for the review of the PSD ("PSD2") contains an article (Article 87) on customer authentication which requires PSPs to apply strong customer authentication when a payer initiates a payment transaction. This reflects the intention to promote strong customer authentication in payment services, although the current wording makes it unclear whether this rule would be applicable to electronic mandates for SDD and in particular whether it would cover mandate models in which no PSPs are involved. On what constitutes strong customer authentication the EBA (in cooperation with the ECB) would issue guidelines to PSPs according to the legal proposal.

4.3 Legal and practical status of electronic signatures in the EU

One of the most obvious forms of electronic customer authentication is the use of electronic signatures. However electronic signatures have a very wide definition both in practice and in national laws. At the EU level Directive 1999/93/EC provides a legal framework for electronic signatures.[7] This Directive distinguishes three levels of electronic signatures allowing a very wide range of solutions at the lowest level (simple or plain 'electronic signatures') but putting forward stricter requirements at higher levels. The highest level is called 'qualified electronic signatures' which make use of very advanced cryptographic methodology (making use of a PKI infrastructure) and certification requirements both for the issuer of the certificates used for the signature and for the devices storing these certificates.

Although the aim of this Directive was to harmonise national requirements and to create a single market for electronic signatures in the Union and make their use widely accessible even between remote parties that have never met and even on a cross-border basis, it largely failed to achieve these goals and real harmonisation and integration have not taken place in practice[8]. For qualified electronic signatures the national legal framework and infrastructures have been set-up in almost all EU countries on the basis of the Directive, but these have their idiosyncratic features, are not inter-operable on a cross-border basis, and their use has not taken up even at the domestic level in most member states.[9]

Having seen this, in 2012 the Commission launched a proposal for the repeal of this Directive and to replace it by an enhanced EU Regulation.[10] The proposal already enjoys political support from Member States and the European Parliament is expected to approve it still during this spring. The Commission expects the entry into force of the new Regulation by summer 2014. However, the proposed new Regulation may also fail to achieve a breakthrough in the field of electronic banking as a) its focus is rather on public (the use of e-authentication in e-government services) than on private services, and b) it has no ambition to harmonise national law pertaining to the legal validity and formal requirements of contracts or documents used for authorisation.

In all, over the short term no break-through can expected in the issuance and use of qualified electronic signatures across national legal regimes in the Union. In case no further action is taken by the EU Commission or the EU legislators in this field it is unlikely that a fully harmonised and integrated market for electronic signatures for payment services emerge over the short or medium term in SEPA.

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF ; See more details on the relevant provisions of this Directive and EU-level developments in regulation since 1999 in the Annex.

[8] This is primarily due to the costs involved and the lack of a significant demand from market participants.

[9] One of the most notable exceptions being Estonia, where the e-government infrastructure makes a very wide use of national e-IDs and the system is also open for private (i.e. non-government) use.

[10] http://europa.eu/rapid/press-release_IP-12-558_en.htm?locale=en

5. Developments since September 2013

The clarification letter by the EPC[11] and the press release from the German authorities[12] issued in September 2013 provided some reassurance to creditors not planning to use the EPC's 4-corner e-mandate model that they can continue to use their existing legally valid[13] mandate procedures when migrating to SEPA, or at least that they do not have to use a solution by 1 February which was not actually rolled out for use by this date to the market. In the meantime the introduction of the 6-month grace period until 1 August gave a further legal leeway for those not yet migrating to the SDD scheme. Notwithstanding legal requirements SEPA migration is now in a stage where the majority of direct debit transactions are executed under the SDD scheme.

Upon issuing their clarification letter to scheme participants the EPC also concluded that the issue of electronic mandates within the SDD schemes should be revisited and they put work in this topic into their workplan for 2014.

Among creditors there seems to be no immediate plans for mass migration to 4-corner model electronic mandate solutions. In the short term (i.e. by 2015) such mass migration could only happen in France (Gemme), the Netherlands (iDeal), Austria (eMS solution), Portugal (SIBS) and possibly Italy (based on MyBank's strong presence in Italy). However in some of these countries original plans to launch these EPC-compliant solutions have been put on hold partly due to the focus on core migration and partly due to the uncertainty in regards to the necessity of implementing such a model.

In all, there seems to be a stalemate or at least hesitance by stakeholders to move in any direction in the field of electronic mandates. Many creditors (especially in e-commerce) hope to be able to continue with their current 2-corner model procedures often involving no or very lax customer authentication. Despite all the best intentions of the EPC to clarify the status of electronic mandate solutions not conforming to the EPC's 4-corner e-operating model, the exact treatment and liabilities of parties in the SDD scheme in this regard are still not entirely clear especially if an unauthorised transaction is claimed and there is a need to determine if the mandate was given by the payer or not.

6. ERPB considerations and the way forward on electronic mandates

The Eurosystem has been urging the roll-out of pan-European electronic mandate solutions ever since actual migration to SEPA payment instruments started. Given the apparent hesitance by stakeholders on the way forward the issue clearly deserves more discussion and guidance.

---

[11] http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=639

[12] http://www.bundesbank.de/Redaktion/DE/Downloads/Presse/EZB_Pressemitteilungen/2013/2013_09_12_sepa_lastschriften.pdf?__blob=publicationFile

[13] 'legally valid' means in this context that the solution applied to give or accept the mandate does not conflict with any existing piece of legislation be it national or European. However, as pointed out above, the fact that the way of authorisation was not against the law does not mean that in case of a claim by the payer that an unauthorised transaction has taken place, the creditor or the creditor PSP is in the position to prove that authorisation was given. In particular, in case of models with weak customer authentication this is often impossible in practice. In these cases the creditor and the creditor PSP have no other choice but to provide the refund to the payer as the burden of proof should clearly be with them.

The SecuRe Pay Forum (European Forum on the Security of Retail Payments) has already contributed to the guidance towards PSPs on strong customer authentication for electronic mandates used for internet payments[14]. In particular in 7.1 of the Forum's recommendations for the security of internet payments strong customer authentication is recommended to PSPs when they play a role in customer authentication for such mandates. Furthermore in recommendation 7.6 the Forum addresses directly payment schemes recommending them to apply a liability regime which provides incentives for strong customer authentication by scheme members.[15] In the assessment guide issued by the Forum for the above recommendations in February 2014[16] it is further clarified that PSPs are recommended to encourage the application of strong customer authentication methods by creditors even if the PSPs are not involved in the mandate issuing process.[17]

In addition, in the EU Commission's proposal for the review of the Payment Services Directive ("PSD2") a definition of strong customer authentication and an associated liability shift is proposed (at the general level) from the payer to the payee in case strong customer authentication was not used due to the latter.[18] Although this legal proposal is still subject to negotiations it clearly reflects the intention to converge towards strong customer authentication methods applied in payment services.

Based on the above considerations on the need for an integrated and harmonised electronic mandate landscape and the need to remain fully aligned with the recommendations of the SecuRe Pay Forum, the ERPB could take the following stance on the issue:

The SDD scheme rules **could be more** explicitly and transparently **open towards 2-, 3- and 4-corner models** of electronic mandates and focus the attention on the security of the solution rather than on the model it follows. **The *Rulebooks* could therefore allow different kinds of electronic mandate models,** if at the same time, **a better definition of which party bears the burden of proof in case of claims of unauthorised transactions are included**. In case an unauthorised transaction is claimed by the debtor (outside the 8-week period where refund is due regardless of any questions on mandates or other issues in case the SDD Core Scheme is used) the debtor bank has to make a judgement based on the circumstances of the disputed collection. If the electronic mandate solution used to issue the mandate provided for a strong level of authentication the likelihood of an unauthorised transaction is considerably lower and the debtor bank would have to provide additional proofs in case they would like to claim a refund from the

[14] Recommendations for the security of internet payments, January 2013: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

[15] "7.6: All payment schemes should promote the implementation of strong customer authentication by introducing a liability regime for the participating PSPs in and across all European markets"

[16] Assessment guide for the security of internet payments, February 2014, http://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf

[17] "7.1.3 If no PSP is involved in the issuance or amendment of electronic direct debit mandates, the creditor's PSP could encourage merchants to implement a procedure using strong customer authentication."

[18] Article 66: "…For payments via a distance communication where the payment service provider does not require strong customer authentication, the payer shall only bear any financial consequences where having acted fraudulently. Should the payee or the payment service provider of the payee fail to accept strong customer authentication, they shall refund the financial damage caused to the payer's payment service provider."

creditor bank. Otherwise, i.e. if the electronic mandate solution used by the creditor provided a weak customer authentication the Rulebooks should more explicitly support the debtor bank to get a refund from the creditor bank. The details of how such rules are formulated should be left to the SDD scheme owner, as long as they stay within the current (PSD) and future (PSD2, once approved) legal framework. **This approach could provide a solution acceptable to all stakeholders over the short term** and at the same time sustain incentives for stakeholders to migrate towards solutions with stronger customer authentication over the longer term.

In addition **the attention of the Commission should be drawn to the lack of fully supportive EU legal background for cross-border authorisation of payment transactions** via electronic signatures. In general it would be favoured if national legal regimes would be adapted if they are not supportive – or even are perceived to constitute a legal barrier – for cross-border use of electronic methods of authorisation for payment transactions.

Notwithstanding the short term improvements to the clarity on the 'burden of proof' in scheme rules, with **a view to medium or long-term prospects** there is a need to ensure further market integration on electronic mandate solutions at the EU level. This can only be achieved if truly pan-European solutions or fully interoperable national solutions emerge and will be taken up by stakeholders. To assess the current state of play and identify barriers to integration in the field a workstream should be set up to analyse the issue and come up with recommendations.

Annex: EU level regulation of electronic authentication via electronic signatures

Current regulation and market situation

Electronic signatures have been regulated at the EU level since 2000 via Directive 1999/93/EC. This Directive provides the definitions of electronic signatures and stipulates basic and technical requirements for them. It also provides a framework for cross-border acceptance, but does not enforce a full harmonisation (most notably it does not make acceptance of electronic signatures mandatory) leaving the option to member states to define their own national requirements on the validity or legal effect of different forms of authentications for contracts and other documents.

Both the existing Directive 1999/93/EC and the upcoming Regulation replacing it define three categories of electronic signatures:

i. The first one is the simplest form of '**electronic signature**' and is given a wide meaning. It refers to "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". It can be as simple as signing an email message with a person's name or using a PIN-code. To be a signature, the authentication must relate to data and not only be used as a method for entity authentication.

ii. The second form of electronic signature is the '**advanced electronic signature**'. This form of signature has to meet the following requirement defined in the Directive: "it is uniquely linked to the signatory, it is capable of identifying the signatory, it is created using means that the signatory can maintain under his sole control and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable". In practice, this definition refers mainly to electronic signatures based on a public key infrastructure (PKI).

iii. The third form of electronic is referred to as a '**qualified electronic signature'**. It consists of an advanced electronic signature based on a qualified certificate (detailed requirements of which are defined in the Annexes of the Directive and of the upcoming Regulation) and created by a secure-signature-creation device (requirements of which are also defined in detail in both legal texts).

All three forms of electronic signatures are admissible as evidence in legal proceedings, however, member states are only obliged at the EU level to grant the same power of evidence as hand-written signatures to qualified electronic signatures from the above three categories.

Despite the clear merits of the Directive in practice not much happened since 2000 in the actual use of qualified electronic signatures in the EU and no noticeable cross-border integration took place. In practice, given the complexity and costs involved in complying with the requirements to produce qualified electronic signatures, very few stakeholders make use of such a signatures in electronic banking and most private individuals do not have a qualified certificate or the device needed to produce such qualified electronic signatures. Furthermore, cross-border use of such signatures virtually does not

exist, which is not only due to the lack of supply and demand, but also to differing national legal requirements.

The upcoming change in EU law on electronic signatures

The EU Commission reacted to the lack of practical integration and proliferation of electronic signatures in 2012 by launching a proposal for a Regulation to replace the Directive. This Regulation has not yet been adopted but –given political agreements – it is expected to enter into force by the summer of 2014. The proposed Regulation largely builds on the existing Directive, but elaborates on several services closely linked to electronic signatures (e.g. time stamping, electronic seals for corporates, validation of signatures, archiving, etc.). It also proposes more transparency on existing electronic signature schemes and provides more detailed rules on the supervision of related service providers. It also strengthens rules on multilateral acceptance of e-ID schemes used primarily in e-government services. However, it does not strengthen requirements (as compared to the existing Directive) to national legal regimes related to the acceptance and validity of electronic signatures for private services. This means that it cannot be reasonably expected that significant improvements will stem solely from the above change in EU rules in the field (market) of electronic authentication methods used for electronic banking.