A Dual Consent Approach for *x*-payments

Ron J. Berndsen* and Daaf van Oudheusden*

18 April 2012

Abstract

In this paper we develop an approach for *x*-payments. An *x*-payment is a payment between a remote debtor and creditor established by using any channel (hence the *x*) to move funds between the debtor account and the creditor account. We address two related issues: one on the debtor side and the other on the creditor side. Firstly, the issue of access to bank accounts of debtors where the problem is who may have access to such accounts and under which conditions. Secondly, the issue of time-critical payment guarantees to creditors (merchants) which is the area where nowadays most of the innovations in retail payments take place. The dual consent approach reconciles both issues by allowing various degrees of access to bank accounts by third parties and a varying quality of the payment guarantee to the merchant based on the degree of assurance from the debtor's bank for an appropriate fee. It is proposed in this paper to use the dual consent approach to regulate the class of *x*-payments in the retail payment sphere.

Key words: retail payments, payment guarantee, *x*-payments, dual consent approach, overlay payment service, access to bank accounts.

1 Introduction

In recent years we observe a couple of trends in retail payments and internet banking which enable customers to use their bank accounts to pay in a multiplicity of ways in a world where risks seem to be rising.

Firstly, the innovation trend is mostly visible in a greater choice for consumers and merchants in the way they send and receive payments. Compared to a decade ago, it is now possible to pay remotely using mobile devices or apps, access your bank account and make payments out of it through internet banking. Consumers may also use electronic money, but the appetite for such pay-before or pre-funded payment methods seems limited as the bulk of remote payments is executed in pay-now (debit card) or pay-later mode (credit card).

* De Nederlandsche Bank, Amsterdam, The Netherlands, e-mail: ron.berndsen@dnb.nl and daaf.van.oudheusden@dnb.nl.
The authors would like to thank colleagues of DNB, members of the Payment and Settlement Systems Committee and others of the ECB for their useful comments on an earlier version. The views expressed here do not necessarily represent the views of De Nederlandsche Bank. The first author is also affiliated with Tilburg University.

The second relevant trend is buying goods and services at web shops over the internet. Often buyer and seller do not know each other. It is crucial for the merchant that the time and effort spent by the customer at effectuating the payment is as minimal as possible. If it takes too long or if it is too cumbersome, the potential customer will mouse-click to the next web shop. The need for the merchant is to have a fast and simple way to establish that the customer will pay.

The third trend is that risks in the financial sector and internet usage are increasing or at least perceived as such by customers. This is a result of the financial crises in recent years including the realistic possibility of bankruptcies of banks and the increasing evidence of cyber crime related to retail payments such as skimming of magnetic stripe payment cards or phishing attacks with the aim of obtaining credentials for internet banking access. One counter measure for the latter phenomenon is to regularly inform and educate the public at large to keep such credentials secret at all times and use these only in well-defined circumstances on the website of your own bank. However, it is also recognized that it is not reasonable to ask customers of a bank to protect their PC or mobile device against all threats present on the insecure internet.

2 The *x*-payment

When consumers are doing business together and a buyer is purchasing an item from a seller, the buyer has to pay the seller to receive the item. The item can be something tangible, a service or even a piece of software. In a brick and mortar shop the payment process can be easy; the buyer pays the seller with cash and the seller gives the item to the buyer: payment versus delivery. Or the buyer uses another way of payment based on a payment scheme that is accepted by the seller as a payment.[1]

But as mentioned in the previous section the way items are sought and bought is changing. The buyer is now surfing on the internet to look for the item she wants and for the price she likes. And finally when the buyer found the item she was looking for and wants to buy, she has to pay for it.

[1] Examples of such payment schemes are payment card schemes, credit transfer schemes and direct debit schemes.

We use the well known four-corner retail payment model to describe the payment process involved (see Figure 1).

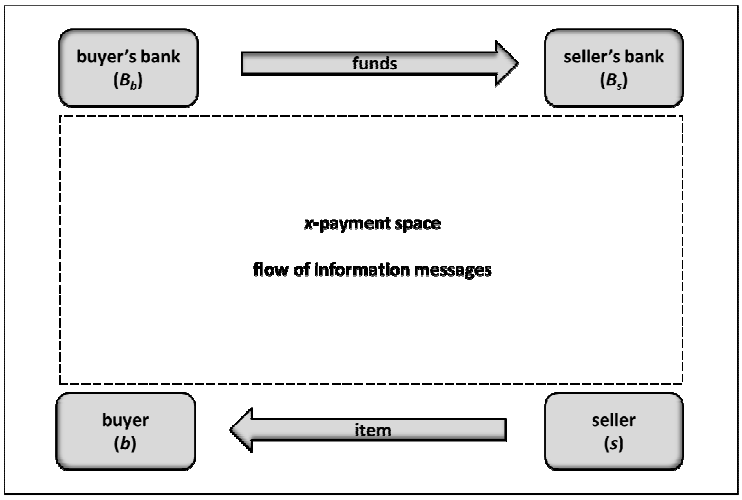

Figure 1: the *x*-payment space in the four-corner model

The buyer keeps her funds on a payment account with her bank and the seller has a payment account with his bank. The transfer of the funds from the account of the buyer to the account of the seller (the payment) is processed through the existing banking, clearing and settlement systems. These payment processes are well described elsewhere and are out of scope of this paper. On the other side the item is send by the seller to the buyer; although this can be an interesting process in relation to payment versus delivery, it is not considered in this paper.

Instead, the focus of this paper is the flow of information messages necessary to initiate the payment transaction up to the point where the actual transfer of funds takes place. This information flow can be through any channel, it can even be oral, but the focus here is on information flows through IT systems and networks like closed terminal networks or the open internet. Some practical examples are card payments, electronic payments, mobile payments, micro payments and overlay payments.

To capture this broad notion we introduce the term *x*-payment:[2]

> *An* x*-payment is the flow of information messages between a remote buyer and seller established through any channel, scheme or mechanism (hence the* x*) to eventually move funds from the buyer's account to the seller's account.*

The combined result of the three trends mentioned above can be translated into the following basic assumptions of the various economic agents which play a role in the retail payment chain. First, customers do not want to split their liquidity over many different accounts or money schemes and the account where they receive their main source of income and pay out most of their expenses is typically held at a bank with covered deposit insurance. Second, in this remote case merchants do not necessarily want to receive the actual funds in real-time; what they need is a real-time, instant payment guarantee from a third party (as the customer may be a first-time buyer for that merchant) that the merchant trusts, so that the item can be shipped right away (straight-through processing to the extent possible). Third, banks need to protect and manage the bank accounts of customers and may be liable for damage. Hence they need to control and authorize any payment order for actually debiting the account. Fourth, third party service providers facilitate customers, merchants and banks in various ways by acting as an intermediary.

In the rest of this paper we formulate the *x*-payment problem and develop general notions for access to bank accounts and payment guarantees. We then impose a solution (called dual consent) which pairs a certain degree of assurance from the bank of the debtor with a certain quality of the payment guarantee such that there are always two agents giving consent. We conclude this paper with the proposal that the dual consent approach could be used as a basis to regulate *x*-payments.

[2] See Berndsen (2011); note that the scope is wide in order to incorporate future innovations, i.e. $x = \{c, e, m, \mu, o, ...\}$.

3 The *x*-payment problem

In this section we formulate the *x*-payment problem. Suppose there are two economic agents *b* and *s* who are remote, possibly haven't done transactions with each other before, but want to transact now. In particular, buyer *b* wants to buy a good or service (henceforth called item) at a price *p* from seller *s*. As they are remote there is no direct, face-to-face contact possible. This problem arises typically in an e-commerce situation where the buyer found an item that she wants to buy on a website (from *s*).

Buyer and seller want to control principal risk in this transaction. Principal risk is here defined as the risk of delivering one side of the transaction while not getting the other side at all. This implies a loss of an amount equivalent to *p*; for *b* it is the loss of funds (an amount of money *p*) and for *s* it is the loss of the item and the gross profit margin (together worth *p*).

From the seller's side it is important that *b* is serviced as fast as possible before *b* decides to move to a competitor of *s* on the internet. Ideally *s* wants to ship the item immediately. In order to do so *s* needs some guarantee that *b* is going to pay the amount *p (*either now or at some point in the future). Depending on the amount *p* the quality of the guarantee may vary. For low *p* the guarantee could be of low quality but for higher *p* the guarantee should be more robust. As soon as *s* gets the requested quality of payment guarantee he can ship the item off to *b*.

Furthermore, *b* prefers to manage all her payments from one account at her bank (B_b) because on this account she receives her main income and she wants to observe her liquidity position in a glance. Viewed from *b*'s perspective the bank account balance represents her main (liquid) financial assets so she wants it protected well, under a deposit guarantee scheme.[3]

All this implies that there is a need for trust in the *x*-payment in the general case where there is no prior chain of trust from the buyer to the seller via their banks. Trust in payment systems is based on a combination of security measures, contractual relationship between parties and transparency of the process. By definition there exists a trust relation between the buyer and her bank and respectively between the seller and his bank. Trust in the payment processes between the banks is covered by

[3] The distinction between a current account and a savings account is neglected here because only the current account can be used for payments; other accounts are not relevant here.

mutual agreements for clearing and settlement systems. Even more trust is gained by regulation of parties, supported by supervision and oversight on these parties. The focus of this paper is the general case where the buyer and the seller are remote and possibly have not done business before; in which case there is no existing trust relation between them. When the buyer and seller use a payment scheme for the payment, the scheme provides the trust necessary for the payment transaction and hence for the business. But when they use one of the new innovative payment products offered by new parties which are not participating in a payment scheme, there will be no a priori trust relation.

Let *G* represent a guarantor who provides this trust by delivering a payment guarantee to *s*. By definition *G* is distinct from *b* and *s* and plays the role of a non-account holding payment service provider.[4] We allow the guarantee to vary between the two extremes of a guarantee with no quality to maximum quality. The former case is no payment guarantee at all (of *G*), the latter corresponds to a completed payment i.e. *s* has been informed that the funds are credited to his bank account (held at bank B_s) with finality so principally the funds could be reused by *s* to make a new payment. Between these two extremes there is the normal notion of a guarantee i.e. *G* provides for a certain level of guarantee towards the seller that either the buyer will eventually pay or – if not – that *G* itself must provide for the funds.

Furthermore it is assumed that the payment guarantee can be provided by *G* in (near) real-time to *s* so shipment of the item bought by *b* takes place directly after receipt of the guarantee. There is no prior assumption about the timing sequence regarding the moment of payment and the moment the item arrives at *b*.

G, being a non-account holding payment service provider, needs to get an assurance for the payment from an account holding payment service provider *B*, normally the bank of *b*, i.e. B_b. We allow the assurance to vary between the two extremes from no assurance to maximum assurance. The former case is no information at all (to *G*), the latter corresponds to a completed payment i.e. *b* has been informed that the funds are debited from her bank account (held at bank B_b) with finality so principally the funds cannot any longer be used by *b* to make a new payment. Between these two

[4] However without loss of generality a payment service provider with a license can also perform the function of guarantor (e.g. $G = B_s$)

extremes there is the normal notion of an assurance i.e. *G* can translate the received assurance from the bank of the buyer into a payment guarantee for the merchant. Furthermore it is assumed that the assurance can be received by *G* in (near) real time.

The *x*-payment problem can now be stated as follows:

> *How can for x-payments a guarantor obtain assurance from the bank of the buyer and generate a payment guarantee for the seller such that the transaction between the buyer and the seller can be agreed in real-time and with sufficient trust while the integrity of the bank balance of the buyer is preserved?*

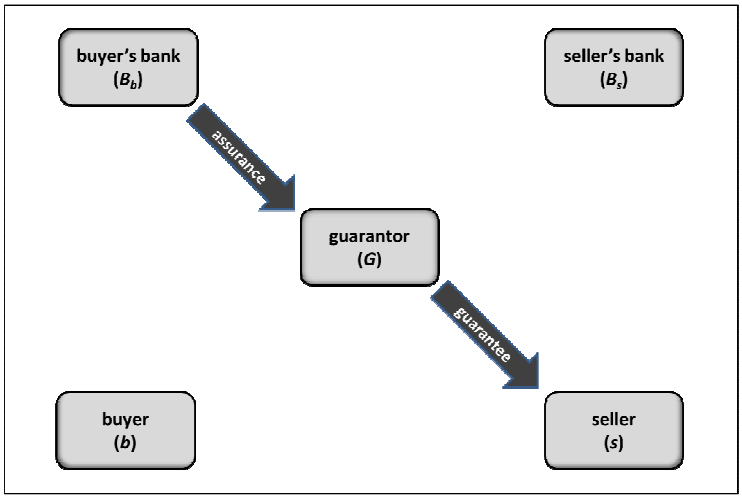

Figure 2: the *x*-payment problem

In Figure 2 the *x*-payment problem is depicted with a separate guarantor role *G* added to the standard four-corner model. The two arrows show the basic flow of information that is needed by *G* respectively assurance from B_b and guarantee to *s*. *G* translates the received assurance from the bank of the buyer into a payment guarantee for the merchant. This is the subject of sections 4 and 5.

4 Varying degrees of access to bank accounts

In this section we look deeper into the issue of access to a bank account. We take as a basic premise that the balance on the bank account can operationally only be changed (debited or credited) by the bank (account servicer) i.e. the bank on behalf and with consent of the customer (account owner).[5] In other words, the actual transfer of value in or out of the account is the exclusive competence of the bank. This operational form of access to bank accounts is however not the main focus of this paper. With access to bank accounts we mean *access to information* on the present status of an account. On request of the guarantor the bank provides an assurance for the (future) payment based on the status of the account. We distinguish six different degrees of assurance (denoted by a) ranging from 0 to 5 (integers), increasing in the level of assurance:

$a = 0$: b is not known as an account owner of bank B_b

$a = 1$: b is an account owner of bank B_b (identification)

$a = 2$: b is the legitimate account owner of the account (authentication)

$a = 3$: b has a credit at B_b equal to the amount of p (verification)

$a = 4$: b's account is blocked for an amount of p (reservation)

$a = 5$: the payment from b's account at B_b is settled (final settlement)

Note that b has access to her bank account B_b at levels $a = 1$ through 5 by definition. Assurance level $a = 1$ only confirms that b has an account at B_b. An example (outside the realm of *x*-payments*)* for assurance level $a = 2$ is the authentication of citizens who want or need to use e-government. In some countries this authentication comes from the relationship between a bank and that citizen. Case $a = 3$ can be interpreted as the verification for a provisional credit transfer. It is then known in real-time (i.e. at the time of making the request) whether there are enough funds or credits in bank account B_b for the payment of the amount p. For the case $a = 4$ the buyer's bank B_b will reserve the amount p on the account of b; and awaits further payment instructions to transfer the funds. In the case $a = 5$ bank B_b has transferred the funds and received confirmation of the final clearing and

[5] Definitions from ISO 20022; see ISO (2004-2009)

settlement. The latter case will take more time and G is probably not receiving $a = 5$ in real-time. Finally $a = 0$ can also be interpreted as the default value.

The economic agent requesting access to bank account of b at B_b can obviously be the bank itself (B_b) or b the customer of the bank whose balance is on the account. However, central in our case is the introduction of third-party access to the bank account by an economic agent G (the guarantor) who is able to get the information of a certain degree a (over the integer interval [0,…,5]). This implies that access to bank accounts in the sense as defined above is assumed to be open to interested intermediaries G, but subject to certain conditions outlined in section 6.

5 Payment guarantee with varying quality

In this section we define the quality of a payment guarantee g. First we need to define who provides the guarantee to whom. We take as a basic premise that it is the merchant or seller s who requests the payment guarantee g from the payment guarantee provider G. It is good to note that the payment guarantee need not to come from the bank but is provided by the payment guarantor G based on the assurance a the guarantor receives from the bank of the buyer B_b. In case the bank of the seller B_s acts as the guarantor G the guarantee to s can even be stronger then based on a alone, especially when clearing and settlement has taken place and the payment transaction is final or when the payment transaction is an on us transaction within the bank (where $B_s = B_b$).

We allow for a varying quality of the payment guarantee g. To that end we distinguish the following qualities with g ranging from 0 to 4 (integers):

$g = 0$: No guarantee at all (merchant takes principal risk)

$g = 1$: Guarantee of the existence of a bank-relationship of b with B_b

$g = 2$: Guarantee that a (future) payment equal to p is expected (authorisation)

$g = 3$: The amount p is guaranteed by guarantor G (guarantor takes principal risk)

$g = 4$: The amount p is settled and available to the merchant on the merchant's bank account B_b (customer takes principal risk)

In the two extremes, there is either no guarantee ($g = 0$) or the money has already been settled (with finality) and transferred to the account of the merchant ($g = 4$). This guarantee may be based on information gathered from accessing the bank account of *b* or on some other information. For $g = 1$ the guarantee is only based on the fact that *b* has an account at B_b, while for $g = 2$ the guarantor *G* has received enough assurance from B_b that the (future) payment of *p* can be expected. With $g = 3$ we have the case that *G* takes up the liability of providing a guarantee to the merchant. Finally $g = 0$ can also be interpreted as the default value.

It is assumed that the merchant is charged a fee for obtaining a guarantee and that *G* also pays a fee to the bank for accessing the bank account. The here envisioned fees are either a small fee per transaction in the order of eurocents or a small flat processing fee and may be dependent on the degree of assurance and guarantee. The reason for this assumption is that the information obtained by accessing a bank account has an economic value and can be bought and sold. Recent initiatives such as the introduction of overlay payment services worldwide are a clear indication of the positive economic value of the payment guarantee. The business case for an economic agent which is only providing the pure guarantor function *G* is then the positive difference between the fees collected from merchants and the fees paid to banks to gain access to B_b.

6 Dual consent approach

In this section we combine the notions developed in the two previous sections into one approach as a solution to the *x*-payment problem, as formulated in section 3. In a stylized way, the approach consists of the following chronological steps:

[1] At any time: *b* wants to buy an item with price *p* from *s* and have it shipped right away;

[2] *s* asks for a guarantee with quality *g* from a payment guarantor *G* (in real time);

[3] *G* obtains consent to access *b*'s bank account (or has obtained prior consent) from

   i. buyer *b* and

   ii. bank B_b;

[4] On the basis of [3] *G* obtains from *b*'s bank assurance *a* (in real time) and converts the

information of *a* into a payment guarantee *g*;

[5] *G* provides *s* with one of the following outcomes:

a. There is a real-time guarantee with quality *g* sufficient for *s* to ship the item to *b* (success)

b. Something goes wrong[6], there is no or insufficient guarantee and *s* will most likely not ship the item (failure).

Core of this procedure which basically converts a level of assurance *a* into a quality of guarantee *g* is step [3] which describes the dual consent (see Figure 3).

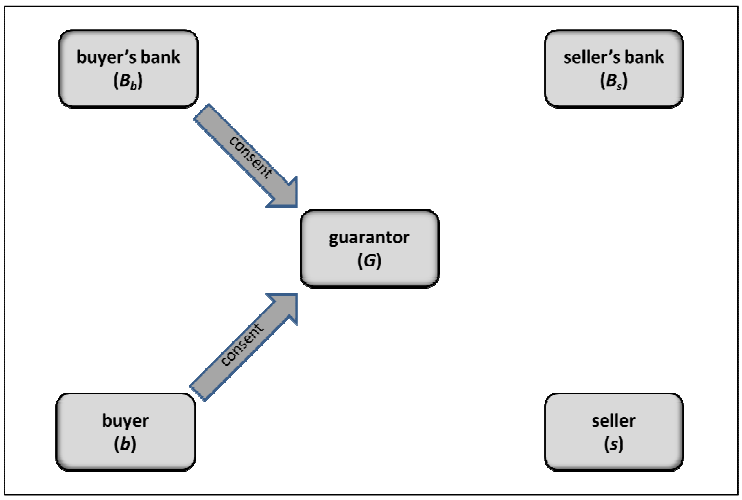

Figure 3: dual consent

The dual consent is thus a consent of *b* to *G* **and** a consent of B_b to *G* in order to permit *G* to access the bank account of *b* and obtain assurance *a*.

The rational for the requirement that *G* should have both consents, is based on the notion that *G* is not a priori participating in a chain of trust, like in a payment scheme. On the contrary, *G* is a new and innovative party in *x*-payment, with no prior relations with the buyer or the banks. There are two conflicting interests that need to be balanced. On the one hand, there is the integrity of the bank account in the interest of the bank and the customer, which calls for well controlled bank account access because the bank needs to know that the person who wants to pay out of that bank account is

[6] Either a failure to get *a* from B_b (default $a = 0$) or a failure to get *g* from *G* (default $g = 0$).

indeed the authentic debtor. On the other hand, there is consumer sovereignty in the interest of the consumer who wants to buy anywhere (in Europe or even worldwide) on a remote basis not hindered by a limited acceptance of a certain payment method, which calls for open bank access.

In Figure 3 it is shown that the guarantor obtains a dual consent from *b* and B_b in a "parallel" fashion (and gains access to *b*'s bank account (not shown in Figure 3)). On the basis of the dual consent *G* gives a guarantee to *s* and *s* ships the item to *b*. There are other configurations which would also be acceptable as a dual consent. For example, if the buyer gives consent to B_b who in turn gives consent to *G* (in that case the dual consent follows a consecutive "in series" pattern). Furthermore it seems logical to limit the requirement of a dual consent to cases where *G* would give guarantees with $g > 0$.

For the sake of clarity if the function of guarantor *G* is performed by the bank of the seller B_s then simpler cases than the general case arise as follows:

1) $G = B_s$, which simplifies the general case to the standard four corner model where the merchant's bank provides the guarantee to *s* (this configuration is shown in Figure 5).
2) $G = B_s = B_b$ in which the flow of information simplifies to the equivalence of an on us (in-house) credit transfer (this configuration is shown in Figure 8).

In Table 1 an example of a possible conversion from *a* to *g* in step [4] is given.

Assurance *a*	**Guarantee *g***
0	**0**
1	**1**
2-3	**2**
3-4	**3**
5	**4**

Table1: conversion of *a* to *g*

As visualised in Figure 4 the dual consent approach furthermore consists of two dimensions: an IT dimension and a contractual dimension.

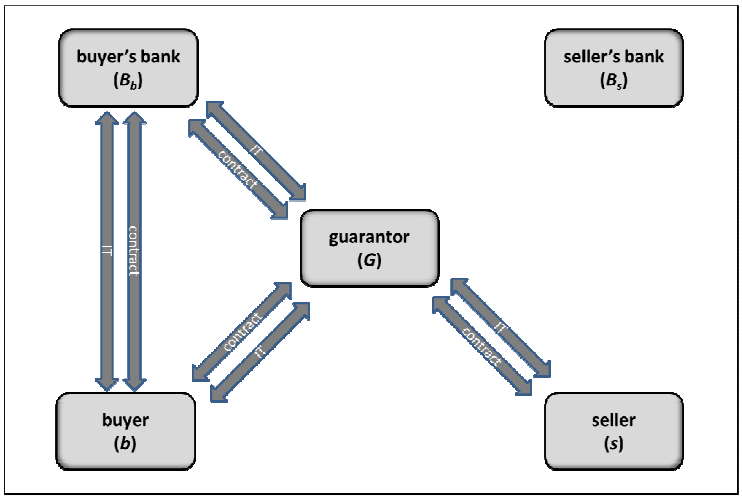

Figure 4: dual consent in two dimensions

The IT dimension comes down to a secure IT connection with sufficient encryption and two-way authentication. This is especially important when all communication runs over the insecure internet, but it is also relevant for other data communication facilities. Because a payment transaction will be based on these flows of information messages, it is obvious that the integrity (and confidentiality) of these information flows, including the authenticity of the end-points, must be secured. Also the systems of all participants that are used in the information flows for the *x*-payments must be secured against attacks.

The contractual dimension should be an agreement about the liabilities and fees concerned. As a minimum it should be agreed which party is liable in case of claims or incidents and which fees are applicable in both scenarios (success and failure); but also issues like governance, audit trails and fraud detection must be agreed. Obviously there will be an existing contractual arrangement between *b* en B_b, which should cover basic requirements from inter alia the Directive on Payment Services (PSD)[7]. Another important observation is that the seller's bank B_s has no direct role in the *x*-payment; therefore the existing contractual agreement between *s* and B_s is not relevant here. But we do expect a contractual agreement between *s* and *G* to exist.

[7] Such as Article 56 Obligations of the payment service user in relation to payment instruments; see PSD (2007).

7 Application of dual consent to existing and future *x*-payments

In general *b* can choose from a set of different payment methods to pay *s*. These methods may differ in risk profile and fee structure for both sides. In Table 2 some currently available payment methods are listed. It shows at the point in time when the transaction is agreed whether or not third-party access to a bank account is needed and which quality of payment guarantee *g* is given to *s*. Furthermore, we analysed the extent a payment method complies with the two additional dimensions mentioned in section 6 (IT and contractual) and consequently whether it is consistent with our dual consent approach.

Payment Method	**Assurance *a***	**Guarantee *g***	**IT dimension**	**Contractual dimension**	**Dual consent**
e-banking	3 / 4	3	yes	yes	yes ($G = B_s$)
overlay payment service[8]	3 / 4	3	no	no	no
on-line banking e-payment (OBeP)[9]	3 / 4	3	yes	yes	yes
on us payment[10]	5	4	yes	yes	yes ($G = B_s = B_b$)
Proposal dual consent future innovations in x-payments	*a > 0*	*g > 0*	yes	yes	yes

Table 2: Application of dual consent to selected payment methods

[8] See Sofort Banking (2011) and DNB (2009).
[9] Examples are e-payment schemes, e.g. eps, giropay, iDeal and the proposed scheme Mybank; see EBA Clearing (2011).
[10] Examples of on us payments are PayPal and e-money.

The e-banking payment method is visualised in Figure 5. An e-banking payment typically initiates a credit transfer into the banking systems. However, this method also covers the initiation of a direct debit by the seller into the payment systems when the buyer has previously submitted an e-mandate.

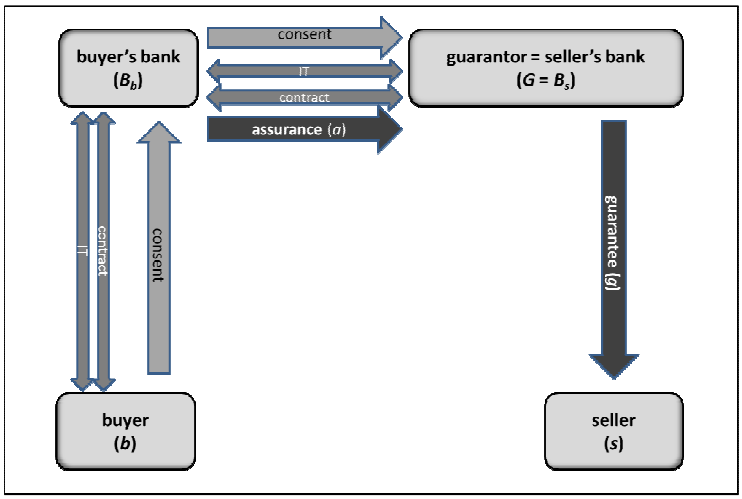

Figure 5: e-banking

Figure 6 shows the current overlay payment method. Note that the overlay payment service (OPS) acting as *G* does not obtain consent of *b* and B_b, because the contractual dimensions with *b* and B_b are missing. Although *G* has IT-connections with *b* and B_b, these connections do not comply with the IT dimensions as described in section 6.

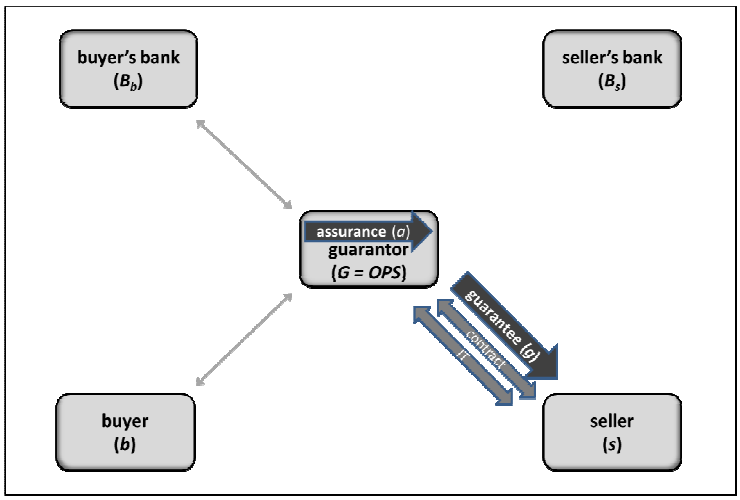

Figure 6: overlay payment service (OPS)

Figure 7 presents the on-line banking e-payments method. In this case the consent of *b* is delivered to *G* via B_b ("in series"). The IT-connection between *G* and *b* is not relevant here for the dual consent approach.

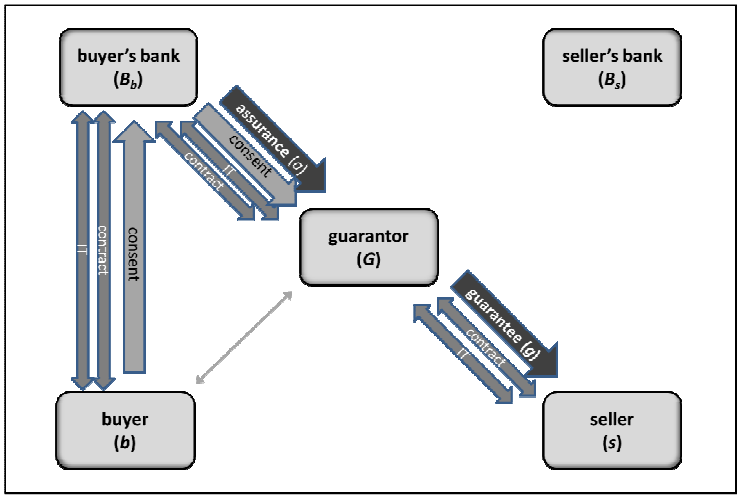

Figure 7: on-line banking e-payments (OBeP)

Figure 8 shows the on us payment method. In practice this method converts to a three-party payment model.

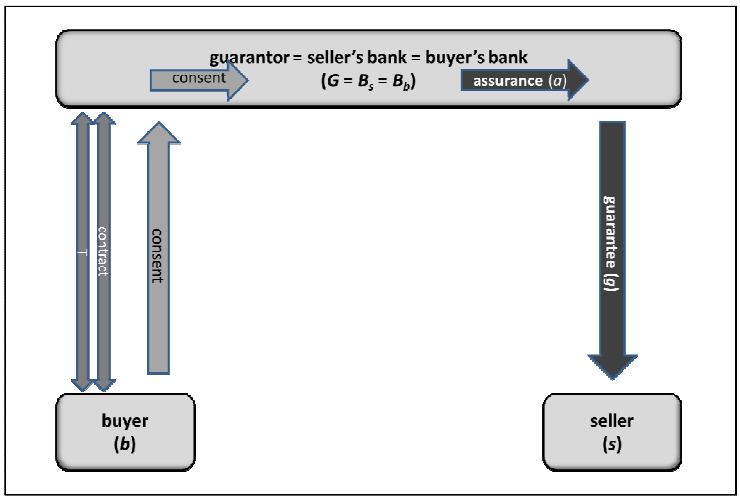

Figure 8: on us payments

Finally the proposed dual consent payment method is represented in the Figure 9.

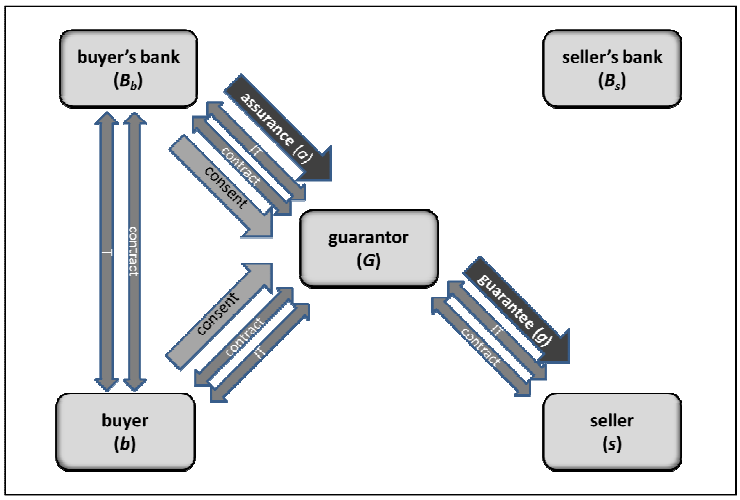

Figure 9: dual consent *x*-payments

8 Concluding remarks

From a regulatory standpoint there are at least two interests that should be balanced. On the one hand the safety and protection of bank accounts. This is the duty and responsibility of the bank which is mostly liable in case of damage, e.g. as a result of cyber crime. On the other hand, we see a lot of innovations in the retail landscape. These are on-going but still in an early stage, mostly fragmented and surely not SEPA compliant yet. This calls for a wide acceptance of various payment channels (here collectively called *x*-payments) across Europe or even worldwide where it is not in the interest of consumers to use a large number of payment instruments in order to do e-commerce activities.

The dual consent approach outlined in this paper is intended to lay down as a first step some minimal regulatory requirements for accessing bank accounts, providing assurance and payment guarantee (combined in one guarantor function) such that a large variety of payment methods can be accommodated. The rational underlying the dual concept approach is that it is not feasible for consumers to have a priori trust in the third party accessing their account.

The concept of the dual consent approach is fully scalable. It will be feasible for small and medium implementations with modest transaction fees in the order of eurocents per transaction. For

bigger implementations on a European scale we expect the approach to migrate to a full blown dual consent scheme for *x*-payments, with low transaction fees based on high usage.

In addition, the dual consent approach should be viewed as a minimum. As the various payment methods will differ in risk profile and usage, extra requirements could be necessary as there are many ways to combine a level of assurance with a certain quality of guarantee. This is an area for future research.

9 Literature

Berndsen (2011), E-Money regulation versus innovation: perspectives from Europe, Presentation at the e-money World Council meeting in Amsterdam, 23 March 2011.

DNB (2009), De Nederlandsche Bank's position on overlay payment services, press release, 15 October 2009, www.dnb.nl.

EBA Clearing (2011), Blueprint for a Pan-European E-Service Solution, June 2011.

ISO (2004-2009), International Organization for Standardization, ISO 20022 - Financial Services - Universal financial industry message scheme.

PSD (2007), Payment Services Directive, 2007/64/EC.

Sofort Banking (2011), Presentation for Preparatory Workshop SEPA Council, Frankfurt, 18 October 2011.