OpenPGP-based Financial Instruments and Dispute Arbitration

Daniel A. Nagy[1] and Nadzeya V. Shakel[2]

[1] Eötvös Lóránd University, Faculty of Science
Department of Computer Science,
ELTECRYPT Research Group,
Pázmány Péter sétány 1/C
H-1117 Budapest, HUNGARY
nagydani@epointsystem.org

[2] Belarusian State University, Faculty of International Relations
Department of Private and European Law,
Akademicheskaya ul., 25-602
220030 Minsk, BELARUS
nshakel@gmail.com

Abstract. In this paper, we present some guidelines for implementing various financial instruments for the purposes of credit and payment, including protocols for commercial transactions, dispute resolution, and establishing credit reputation. We strive to employ only widely used, standardized cryptography and keep the proposed procedures as simple as possible on the conceptual level. Also, we want all the documents to resemble their paper-based counterparts as closely as possible and be readable by humans, while also facilitating automated processing by computers. The presented results are being actively implemented within the ePoint System framework.

1 Introduction

Electronic commerce is currently severely hampered by the lack of reliable financial and legal services matching the speed and convenience of on-line transactions. The security level of online contracts and payments leaves much to be desired; when contracts are typically made by filling out and submitting web forms (with no customer copy beyond an easily forgeable confirmation email) and payment authorization is done by entering one's credit card details, all involved parties are highly vulnerable to fraud. In case of such fraud, especially in an international setting, legal proceedings are prohibitively slow and expensive and fraught with inconsistent rulings due to the lack of reliable evidence.

The problems resulting from the lack of common jurisdiction, ill-equipped central authorities and impracticality of coercive enforcement of contracts are nothing new; international trade has always been beset by such problems. Over time, a number of efficient techniques, both legal and financial, has evolved to deal with them. The body of laws and customs for international trade, commonly

known as *Lex Mercatoria*, provides us with both inspiration and guidance for designing a set of on-line protocols for overcoming the above described difficulties in electronic commerce. In this paper, we describe some core techniques and procedures concerning financial instruments used for payment and credit that rely as much as possible on the existing infrastructure.

OpenPGP[1] is the IETF standard inspired by Phil Zimmerman's PGP program that, among other things, describes digitally signed documents and facilities for peer-to-peer certification of public keys. Over time, a distributed, decentralized, massively redundant network of so-called Public Key Servers (PKS) has been established, based on Mark Horowitz's web- and email-based protocol (HKP[3]). At the time of writing, the peer-to-peer certification facility and the PKS network is used solely for establishing bindings between public keys and identities and the trustworthiness of participants in such matters, forming the so-called PGP Web of Trust. However, as shown in this paper, this infrastructure can be leveraged for the purpose of the more general task of reputation tracking. In particular, for recording and disseminating arbitrator decisions and other information affecting credit reputation.

2 Compliance without coercion

The Internet inherited essential elements of design, such as redundancy and decentralization, from an ARPA project aimed at maintaining network operations during a nuclear conflict. These features, compounded by problems of jurisdiction in increasingly complex, multinational business structures render coercive enforcement of national law problematic and unreliable for on-line business.

By contrast, *Lex Mercatoria* is a set of customs, rules and usages that are widely applied in international trade. This phenomenon became especially important in international commercial arbitration.

Parties choose international arbitration because national courts can not satisfy the growing demands of commerce, e.g., need for speed and lower formality level in dispute resolution (see, e.g. [5], [6], [12]). Similarly, they want to avoid the application of national rules. Thus, *Lex Mercatoria* as an a-national body of private customary law is used in international commercial arbitration, if the parties or arbitrators choose so [4]. This process is further promoted by the fact that even if the award is based on *Lex Mercatoria*, it is still recognized and enforced in the majority of the countries.

Lex Mercatoria does also fulfill a very important preventive function. Autonomous commercial law can regulate merchant conduct without the coercive assistance of state governments. Businessmen are encouraged to comply with *Lex Mercatoria*, so that disputes do not arise. This is guaranteed through 'black lists', withdrawal of membership rights, forfeiture of bonds and similar dangers to the commercial reputation [11].

In this paper, we describe similar mechanisms that are applicable to electronic commerce, based on already standardized and widely deployed solutions. Our goal is to design procedures that can be easily understood by the Internet-

using public. For instance, we would like to avoid relying on "exotic cryptography" that is conceptually difficult to grasp, such as blinded signatures [13], Byzantine agreement [14], two-party secret exchange [15], etc. Instead, we rely on third parties that require only very limited trust (e.g. PKS servers, time stampers, etc.). Also, we often forfeit the ability to prevent fraud by making it infeasible; instead, we deter it by reactive security measures made possible by strong evidence in the spirit of *Lex Mercatoria*.

Unfortunately, *Lex Mercatoria* is often not applicable directly to electronic commerce, because many of its implicit assumptions break down on the Internet. Also, in many cases, contemporary telecommunications allow for short-cuts and considerable improvements in efficiency over customary practices. In the next section, we shall explore the most important differences between the legal aspects of traditional and on-line commerce.

3 Differences Between Paper-based and Electronic Evidence

3.1 Irreversible Operations: Leaving Marks vs. Revealing Secrets

Any kind of evidence results from some kind of alteration that is difficult to reverse, caused by the action that needs to be evidenced. The quality of evidence can be measured by comparing the expenses (not necessarily monetary) required for forging said evidence to the benefits of forgery.

Traditionally, documentary evidence is the result of marking paper with ink. Once the paper is marked, it is very difficult to remove these marks as if they have never been there and it is often also difficult to make an exact duplicate of the unmarked document. With electronic documents, this is not the case; any change to a document can be reversed with minimal effort, precisely by the way of keeping an exact duplicate of the unmarked version, which is practically free.

This is a major problem. Take, for example, the endorsement of a cheque. Once a cheque is endorsed with the name of the new beneficiary and the signature of the old beneficiary on its flip side, the old beneficiary cannot cash the cheque; in order to do so, he would need to steal it back from the new beneficiary and remove the endorsement, both of which are very costly. However, adding the name of the new beneficiary and any kind of digital signature to an electronic cheque does not prevent the old beneficiary from cashing a copy of the unendorsed version or endorsing it to someone else; this kind of fraud is known as "double spending" in financial cryptography. This problem alone renders large parts of *Lex Mercatoria* inapplicable to electronic transactions, at least directly.

Instead, in the digital world, the irreversible operation is revealing information that was not previously known [16]. It is very costly to force someone to forget a piece of information and it is even more problematic to completely erase something from the public records. In Section 4, we describe in detail several methods for dealing with digital negotiable financial instruments by revealing secrets where paper-based procedures would require making marks on them.

In general, we include cryptographic challenges (for example, the value a one-way hash function calculated over a secret) in the document. Once a proof of knowledge of this secret (in most cases, the secret itself) is revealed, the document is irreversibly altered. For example, instead of stamping "PAID" on an invoice, one can reveal a secret corresponding to a hash value included in said invoice (at least to the paying party). Thus, the paying party will have very strong documentary evidence; a receipt of payment.

3.2 Confidentiality: Envelopes vs. Encryption

In traditional commerce, the confidentiality of correspondence is typically protected by tamper-evident (i.e. sealed) envelopes. This is a reactive measure designed to deter breaches of confidentiality by the postal service or anyone else. However, it is not possible for the recipient to obtain the message without opening the envelope.

Encryption (especially public key encryption), which has been the primary purpose of PGP, while in many ways analogous to putting documents into a sealed envelope, still merits some remarks. For example, the creator of an encrypted message may or may not be able to prove to a third party (i.e. the arbitrator) beyond doubt that the stated recipient can indeed decipher a PGP-encrypted message. In many cases, however it is impossible to verify. This is in sharp contrast with envelopes, which the stated recipient can always open.

3.3 Integrity: Envelopes vs. Hashes

Another purpose of tamper-evident envelopes is to protect the integrity of a message; if the seal is not broken, the content of the envelope can be assumed, with a high level of confidence, not to have been altered since the act of sealing.

The integrity of digital documents can be evidenced by the corresponding hash value or a valid digital signature (which itself is often calculated from the hash value). There are other cryptographic techniques used for integrity protection (e.g. MAC - message authentication codes), but they are not very useful for the purposes of third-party arbitration and thus are not discussed here any further.

OpenPGP provides facilities for the so-called MDC (modification detection code, see Section 5.14. of [1]), which protects the integrity of encrypted messages against those who cannot decrypt them but may attempt to alter the encrypted version.

Static digital documents such as appendices to contracts or a body of applicable rules are best referenced by their hash values. Such references also evidence the chronological order in which these documents were created.

3.4 Authenticity: Signatures and Stamps

Digital signatures are often assumed to be analogous, in the legal sense, with hand-written signatures (see, e.g. [7]). Unfortunately, this is a very inaccurate

assumption, seriously hampering the adoption of digital signatures in electronic commerce.

The first and most important difference is that digital signatures are made by computers on behalf of signatories, not by signatories themselves. This means that non-repudiation should be judged against the possibility of adversaries taking control of someone's computer. In fact, digital signatures are, in this respect, more similar to seals and stamps in that the machinery used for their creation can be stolen or copied. Of course, it still makes sense to treat digital signatures as legally binding evidence of intent, not least because this approach would provide users of such signatures with a strong incentive to guard their private keys and signing machinery.

Another important difference is their reversibility, as explained above. Once a paper document has been signed with ink, the unsigned document ceases to exist. Not so with digital signatures! One can always obtain a perfect unsigned copy by simply stripping off the signature. This difference has profound consequences for electronic commerce, requiring substantial changes to traditional procedures beyond simply replacing ink signatures on paper documents with their digital counterparts on electronic documents. Most of the presented research was motivated by this realization.

3.5 Digital Contracts

To achieve the contract formation several conditions need to be fulfilled; these conditions are different in various jurisdictions. In the field of electronic commerce means are to be found to eliminate doubts as to the question on the existence of the contract. However, digital contracts still retain the main characteristics of non-electronic ones; thus, a brief explanation of the existing systems is needed.

The common law standard for contract formation has three requirements: offer, acceptance and consideration. Offer is a promise to enter into the contract on a certain terms upon acceptance (statement or other conduct demonstrating assent). The criterion of consideration means that both parties to a contract must bring something to the bargain. The mailbox rule is of importance here, as it provides that the contract is formed when the letter of acceptance is placed in the mailbox.

The common law is even more liberal in the USA, were a contract for the sale of good may be made "in any manner sufficient to show agreement" (2-204(1) UCC [8]). This means that issues like undefined timing, open terms, etc. are non-relevant, and contract is nonetheless formed. The scholars claim that common law criteria (offer, acceptance and consideration) are still important, but they are proved merely by showing whether words and/or actions of the parties recognize the existence of the agreement [18].

Another approach, generally accepted in civil law, requires only offer and acceptance. Offer should be sufficiently definite; generally it means that it should indicate goods and make it possible to determine the quantity and the price. The basic test is whether the offer indicates the intention of the offerer to be

bound in case of acceptance. Contract is formed when acceptance is actually communicated to the offerer.

Thus, to avoid all the complications caused by these differences, it is absolutely necessary to explicitly state in the contracts the requirements for offer and acceptance. In order for contracts to stand up in arbitration, we may extend the UCC requirement for acceptance to be made "in any manner sufficient to show agreement to a *third party*".

Precisely because of the very real danger of malicious parties tricking unsuspecting computer users (or their computers) into signing something without their consent, it is prudent of arbitration to require consideration in contracts, because doing so would render such attacks more difficult and less lucrative. In short, promises to do something without any reciprocal benefit to the person making the promise are not to be considered valid because of the substantial risk that such promises have been obtained by fraudulent means.

4 Digital Representations of Debt and Credit Reputation

4.1 General Negotiable Financial Instrument

Traditionally, negotiable instrument is generally defined as a transferable, signed document that unconditionally promises to pay the bearer a sum of money at a future date or on demand. Negotiable instruments are commonly used in business transactions to finance the movement of goods and to secure and distribute loans. Examples include cheques, bills of exchange, and promissory notes. All of them have statutory requirements that define their main elements, and these should be strictly fulfilled. It is also important to emphasize that there is a number of similar financial instruments, such as letters of credit that are treated separately by law and custom, which, nevertheless, can be represented digitally in a very similar way.

We propose representing negotiable financial instruments as PGP-clearsigned plain text documents (see Section 7. of [1]) that are both readable by humans and easily parsable by computers. Whenever possible, they should follow the customary form of corresponding financial instruments and should be easily recognizable as such.

Additionally, they must include a cryptographic challenge corresponding to a secret known to the bearer of the instrument. Endorsements must include a proof of knowledge of this secret (typically, the secret itself) and a new challenge corresponding to a secret known to the new bearer. Technically, revealing such a secret invalidates the instrument; endorsements are, in fact, back-to-back instruments carrying the same promise. The exact legal interpretation will hopefully emerge from future precedents.

It is possible to turn these instruments into smart contracts [17], that are automatically processed by suitable machinery. One of the earliest general instrument of this kind is the Ricardian Contract [20] developed by Ian Grigg and others at Systemics Ltd. We believe that this approach has some very important

benefits over expressing smart contracts in universal programming languages (even specialized ones, such as E [21]), such as limiting the possibility of obfuscation and being generally readable to non-programmers.

4.2 General Reputation Record

Reputation records are to be implemented as OpenPGP signatures (version 4) directly on the public key of the subject (tag 0x1F, see Section 5.2.1. of [1]), containing all the additional information in notation sub-packets. This way, they can be disseminated using the existing PKS infrastructure, by simply uploading the signed public key to any of the interconnected public key servers.

Since these records are inherently signed, users of the system are free to choose which ones to trust based on who issued them. All the techniques that have been developed (and already implemented) for judging the reliability of statements about the identities corresponding to public keys can be directly applied to statements about their creditworthiness.

Payment, within this context, often means the exchange of one form of debt into a more liquid form of debt. If all the involved debt is represented according to this proposal, dispute resolution becomes easier, faster and cheaper.

In the next section, we will explore some typical cases involving the issuing of such records.

5 Case Studies

5.1 Dramatis Personæ

In our case studies, we invoke the usual cast of characters in financial cryptography:

Alice, Bob, Carol and Dave: Participants in commercial transactions.
Ivan: The issuer of the currency used in transactions.
Justin: The arbitrator of disputes.
Trent: A trusted third party helping to perform various protocols.

5.2 Cash (Banknote)

This is special, simpler case of promissory note, which explained in a separate case in its general form. Cash-like payment has already been discussed in detail in [16].

A cash-like instrument (which we call "certificate of value") is a clearsigned document signed by Ivan that includes a serial number, a timestamp, the value, a reference to Ivan's public key, a hash value corresponding to a secret known to the bearer and the reason for issuance (typically the secret corresponding to an older certificate, which was invalidated by issuing this one). It also contains the promise of Ivan which he makes issuing this note. Upon request, Ivan also provides timestamped status reports with the latest serial number issued.

In this paper, we present two simple payment scenarios (Alice pays Bob), with and without invoice. Both scenarios begin with Alice knowing some secret a for which Ivan has already published a corresponding certificate containing $H(a)$ where H is a cryptographic hash function.

a) Simple payment without evidence

Alice simply sends a through some reasonably secure channel to Bob.

Bob may then choose to exchange a for some other secret b sending an exchange request to Ivan, containing a and $H(b)$. If he does so, Alice no longer has the option to reverse the payment.

This simple payment is very easy and convenient (it can be performed in a very low-tech setting), but it produces insufficient evidence. Thus, arbitration cannot help with disputes arising from such payments, which are therefore only suitable for low-value transactions, similarly to coin-operated vending machines.

b) Payment with evidence

In this case, Alice first orders some service (or good) X from Bob. Depending on the case, this may or may not be an offer to buy it.

Then Bob responds with an invoice which includes $H(b)$, b being a secret known to Bob. It may also include a deadline by which Alice is required to make the payment in order to receive X.

If the transaction is such that the order by Alice already constitutes an offer then Bob should send this invoice by certified mail. The operator of the messaging service (Trent) provides a signed receipt for the encrypted message (that contains the invoice), which Bob should save. He should also save the session key by which this message was encrypted.

If Alice fails to make the payment, despite having made a binding offer, Bob should submit the following evidence to Justin supporting his claim:

i. the order signed by Alice
ii. the encrypted invoice sent by Bob in response
iii. the receipt by Trent
iv. the symmetric session key with which Justin can decrypt ii.
v. a status report by Ivan timestamped after the payment deadline

If Justin can verify Bob's claim, all of the above should be included in the ruling condemning Alice for not following up on the order.

If Alice pays the invoice, then the new certificate of value signed by Ivan and the original invoice signed by Bob constitute a receipt. Both should have the same $H(b)$ included. If Bob fails to deliver X, Alice should send these to Justin as evidence supporting her claim.

Justin then asks Bob to provide evidence for delivering X to Alice. The nature of this evidence, of course, depends on the nature of X.

5.3 Promissory Note

A promissory note is very similar to certificates of value as described above, except that in general they may include additional information such as maturity

and expiry dates, circumstances of repayment, etc. When the promissory note is redeemed, the corresponding secret must be revealed to the issuer of the note (in a signed, certified message executing the instrument).

Chains of endorsements may be signed and published by a trusted timestamping service (Trent). In this case, before accepting an endorsed promissory note, one can check whether or not double-spending has occurred.

In the absence of Trent's timestamping service, double spending (or double endorsement) can only be established after the fact, when damage has already occurred. However, Justin can still be presented with sufficient evidence to find out who double-spent (or, more precisely, double-endorsed) a promissory note.

Although Justin can immediately find out who the fraudulent party was, when presented with two different executions of the same note, it still makes sense to keep the custom of (implicitly or explicitly) guaranteeing previous endorsements from *Lex Mercatoria*, because it would provide the users of such instruments with the right incentives to verify the reputation of their counterparties, thus distributing the effort of verification and enforcement.

For example, Bob endorses Alice's promissory note both to Carol and to Dave. Carol has no problem getting her cash from Alice, but Dave's request would be refused. Instead of money, Dave would receive Bob's endorsement with Carol indicated as beneficiary, which he is free to attach to Bob's public key as a direct signature proving that Bob is a fraud. Additionally (or alternatively), he can sue Bob for compensation, with submitting both endorsements and the original promissory note as evidence.

In another example, Bob endorses Alice's promissory note to Carol in exchange for some service rendered to Bob, but Alice fails to honor her obligation to pay. Carol, in this case, should sue Bob for compensation and it is Bob's task to recoup his losses from Alice.

Promissory notes are in many ways inferior to drafts described below. Their only benefit is that they depend less on the availability of third parties such as Ivan, Trent or Justin. Their biggest disadvantage is that their processing is automated to a much lesser degree.

5.4 Draft

A draft is an order signed by the drawer (Alice) inviting the drawee (Ivan) to pay the beneficiary (Bob) a given amount of money (in Ivan's notes) on demand after a given maturity date. The payment is done by issuing a certificate of value with a cryptographic challenge also included in the draft. Optionally, one can include an expiry date and other information within the draft. Importantly, drafts must conform to templates provided by the drawee in order to be processed. Also, because processing drafts depends on the availability of Ivan's server, it is practical to follow eUCP's recommendation (Article *e5*, Section *e* of [10]) of extending expiry dates by multiples of 24 hours to the next working day following the expiry date, if Ivan's server is unavailable.

The only reference to the beneficiary is the cryptographic challenge. Thus, beneficiaries can be (and are expected often to remain) anonymous. The drawer,

however, is always identified by a public key fingerprint. Thus, publishing a draft does not violate Bob's privacy, but provides Alice with additional incentives to repay it (since anyone can thus see Alice's outstanding debt).

Once published (by Ivan), drafts automatically become negotiable. Technically, upon receiving a draft for publication, Ivan would emit a special issue of notes that are backed by Alice's draft and can only be merged among themselves. Upon maturity, they can be exchanged for notes representing Ivan's debt, provided that Alice holds sufficient funds in Ivan's obligations (which are thus redeemed). It is Bob's choice whether or not to turn Alice's draft into tradeable debt.

Thus, drafts can be executed either directly, by presenting them for the first time to Ivan after maturity or by first turning them into tradeable debt as described above and then, upon maturity, executing in part or in full. Thus, unlike promissory notes, drafts are perfectly safe from double-spending.

In either case, if Alice does not have sufficient funds at the time of executing her draft to cover the request, Ivan would calculate a signature directly on Alice's public key, indicating the reason for bouncing the draft (not sufficient funds) and the message executing the draft (or parts of the debt that it represents). Bob is then free to publish Alice's signed key on a PKS in order to affect her reputation in a negative way.

Of course, Bob can also turn to Justin, in case the bounced payment by draft was part of a more complex transaction, which failed because of Alice's failure to maintain sufficient funds on her account.

In addition to above described unconditional drafts, one can also implement conditional drafts that depend on further documentary evidence to execute successfully. Such conditions are defined by the supplied documents' template, the signer (if any) and simple conditions on its fields such as EQUAL TO X, HASHES TO X, LESS THAN X or GREATER THAN X (the latter two only meaningful for numerical values of X). Conditions may be encrypted with Ivan's, Alice's and Bob's public keys, and possibly others. For example, it may be also decipherable to Justin, though of course, it is sufficient to provide Justin with the correct session key so that he can decipher the condition when the parties turn to him for resolving their dispute.

For example, Alice wants to borrow money from Bob in Ivan's notes. Thus, she sends Bob a draft that he can execute after the maturity date only if he pays Alice within 24 hours. The supplementary document is defined, in this case, as follows: it must use Ivan's template for certificates of value, it must be signed by Ivan, it's value field must be EQUAL TO the amount that Alice wants to borrow, it's date field must be LESS THAN 24 hours from now and it's cryptographic challenge must be EQUAL TO something provided by Alice.

5.5 Cheque

A cheque is technically identical to a draft but used for the purposes of payment rather than credit. It is typically characterized by a maturity date at most a few seconds after issuance.

5.6 Letter of Credit

Letters of credit are similar to certificates of value, except that they contain conditions like those described in conditional drafts and can be exchanged only if Ivan is presented with the corresponding documentation. Those executing Letters of Credit may ask Ivan to encrypt the presented documentation with a number of public keys before publishing. Just like in the case of conditional drafts, the provisions of eUCP for expiry extension due to server unavailability apply. It is important to note, however, that complying with all of eUCP is difficult and often impractical, because that would require forfeiting the desired feature of fully automated processing. This may actually be one of the primary reasons for the very limited use of eUCP, despite the wide acceptance of UCP [9].

The simplest letter of credit is the so-called ripped certificate of value. The only condition is that the holder presents an additional secret that hashes to a given value. The name is due to the fact that this digital instrument works analogously to a banknote ripped in two; one half is handed over with the order, the other – upon delivery. In this case, Ivan acts as an escrow agent. Below follows an example:

- Alice asks Bob to bring her a bottle of milk
- Bob invoices Alice for a given amount in Ivan's notes, promising a bottle of milk in exchange
- Alice pays the invoice, but attaches an additional condition, namely that Bob presents the pre-image of a given hash value $H(a)$.

At this point, Alice has already lost the money, but Bob has not obtained it, so he has an additional incentive to bring Alice milk, even if he does not care about his reputation.

- Bob brings Alice a bottle of milk

At this point, Alice has no reason not to reveal a to Bob, because she would not gain anything by not doing so.

A more complicated letter of credit would involve Trent, operating a carrier service.

- Alice asks Bob to send her a thousand bottles of milk
- Bob invoices Alice for a given amount in Ivan's notes, promising a thousand bottles of milk in exchange
- Alice pays the invoice, but attaches an additional condition, requiring a bill of landing signed by Trent, the carrier, about a thousand bottles of milk delivered to Alice.

At this point, Alice has already lost the money and all control over the payment. If Bob indeed ships the milk using Trent's services, he gets the money.

6 Arbitration

So far, we have only described how transacting parties gather sufficient evidence and in what cases do they turn to arbitration. In this section, we outline the arbitration protocol, with Alice being the claimant, Bob the respondent and Justin the arbitrator.

First, Alice sends a claim against Bob to Justin, *including* evidence supporting her claim. The statement of claim also contains a specific value and a cryptographic challenge, like invoices described in Section 5.2. It is important that the statement of claim actually includes all the supporting evidence, not just references it by hash value, because only this way can it be demonstrated that whoever processed the claim was also able to access the evidence. We propose the use of PGP/MIME format [2] for the submission.

After receiving it, Justin invoices Alice for the arbitration fee. This invoice refers to Alice's statement of claim by hash value.

Justin's method of determining the arbitration fee has profound consequences. Too high fees may limit the usefulness of the service and may result in attempts at using arbitration clauses in contracts to shield liability. Too low fees may result in an increased number of bogus claims. Discussing the effects of the arbitration fee and comparing various methods of determining such fees is outside of this paper's scope.

Once the fee is paid, Justin notifies Bob, presenting him with Alice's claim and the supporting evidence. This is done automatically, without human intervention.

Bob, at this point, has four options:

1. He can *settle* by paying Alice the claimed amount; this would be evidenced by Ivan's certificate of value containing the same cryptographic challenge and value as Alice's statement of claim.
2. He can *contest* Alice's claim. At this point, he should also present Justin with evidence proving Alice's claim wrongful. Justin acknowledges receiving Bob's documents in a signed receipt, referring to each document and Alice's statement of claim by hash value.
3. Bob may also *demur* at Alice's claim. This means that Bob is not contesting any of the factual statements, but informs Justin that in his view they do not imply that Bob should pay anything to Alice. It is the formal way of saying "so what?". The demurrer is a document signed by Bob referring to Alice's statement of claim by hash value. It is important to emphasize that the demurrer is neither an admission nor a denial of the factual statements in Alice's claim. Justin acknowledges receiving Bob's demurrer in a signed receipt with the corresponding hash value.
4. Bob may *do nothing* within the time frame allotted for responding to Alice's claim.

The consequence of the first choice is that the case is closed. Clearly, from Justin's point of view, this is the most desirable outcome, as he ends up pocketing the arbitration fee, without using human resources.

In the second case, Justin proceeds with evaluating the available evidence. Depending on its nature, the process can be automated to some extent. In some cases it can be even fully automated. If Alice's claim does not stand up, both Alice and Bob get notified about the case being closed. If Justin finds Bob in the wrong, then Bob is invoiced for damages and arbitration. If he fails to pay this invoice on time, then Alice shall receive a demerit signature of Justin on Bob's key, which she is free to upload to the PKS network.

In the third case, Justin decides on the demurrer assuming that the factual statements in Alice's claim are true. Otherwise, however, the demurrer is *not* an admission of those facts by Bob. If the demurrer is sustained, both parties receive a signed statement to this effect from Justin and the case is closed. If not, the case proceeds as if Bob decided to do nothing.

The reason for using the largely obsolete demurrer is that using it results in possibly crucial evidence for other arbitration procedures connected to the one in question, such as appeals or disputes further up the endorsement chain of some negotiable instrument.

The consequences of the fourth choice (doing nothing) also depend on the particular case. In general, Bob should not be encouraged to delay arbitration by doing nothing, but on the other hand Bob should be protected from harassment. Just like in the case of Justin's fees, this topic merits more discussion, which, however, lies outside of the scope of this paper.

7 Conclusions

We have presented a framework for implementing various financial instruments using standardized cryptography that closely resemble their paper-based counterparts. A server program that processes such instruments is described in detail in Janis Schuller's thesis [19]. This piece of software will be the basis for the reference implementation of the protocols and data formats described in this paper.

We have also proposed a basic protocol for arbitration that is designed to provide rapid and cost-effective justice for electronic commerce using OpenPGP-based electronic contracting, financial instruments and reputation tracking. Currently, the protocol is not implemented, but we are hoping to start development soon and release the resulting software under an open source licence at `ePointSystem.org`.

8 Acknowledgements

The authors would like to thank Mihály Bárász, Ian Grigg, Ágnes Koltay, Nick Szabo and Janis Schuller for inspiration, encouragement and fruitful discussions.

References

1. Jon Callas, Lutz Donnerhacke, Hal Finney, David Shaw, Rodney Thayer: *OpenPGP Message Format.* RFC2440bis-22, IETF, (2007)
2. Michael Elkins, et al.: *MIME Security with OpenPGP.* RFC3156, IETF, (2001)
3. Marc Horowitz: *A PGP Public Key Server.* Master's Thesis, MIT, (1997)
4. Ole Lando: *The Lex Mercatoria in International Commercial Arbitration.* The Int'l and Comparative Law Quarterly, Vol. 34, No. 4 (1985), pp. 747-768
5. Tibor Varady, John J. Barcelo III, Arthur T. von Mehren: *International commercial arbitration. A transnational perspective.* Second edition. West Group, (2003)
6. Alan Redfern, Martin Hunter, Nigel Blackaby, Constantine Partasides: *Law & practice of International Commercial Arbitration.* Fourth edition. Sweet & Maxwell, (2004)
7. *Electronic Signatures in Global and National Commerce (ESIGN) Act.* U. S. Federal Trade Commission, Bureau of Consumer Protection and Department of Commerce, National Telecommunications and Information Administration, (2001)
8. *Uniform Commercial Code.* The American Law Institute, (2001)
9. *Uniform Customs and Practice for Documentary Credits* (UCP 600) International Chamber of Commerce, (2007)
10. *Supplement to UCP 600 for Electronic Presentation* (eUCP V1.1) International Chamber of Commerce, (2007)
11. Klaus Peter Berger: *The Creeping Codification of the Lex Mercatoria.* Kluwer Law International, (1999)
12. Klaus Peter Berger: *Private Dispute Resolution in International Business.* Negotiation, Mediation, Arbitration. Kluwer Law International, (2006)
13. David Chaum: *Blind signatures for untraceable payments.* Advances in Cryptology - Crypto '82, Springer-Verlag (1983), pp. 199-203
14. Danny Dolev, H. Raymond Strong: *Byzantine Agreements.* Proceedings of COMPCON83, San Francisco, (1983), pp. 77-81
15. Silvio Micali: *Simultaneous electronic transactions.* US Patent 5,666,420 (1997)
16. Daniel A. Nagy: *On Digital Cash-Like Payment Systems.* Proceedings of the 2nd Int'l Conf. on E-Business and Telecom. Networks, ICETE, (2005). pp. 66-73
17. Nick Szabo: *Smart Contracts* Online essay at `http://szabo.best.vwh.net/smart.contracts.html`
18. William Long: *Contract Formation Under Article II* Online essay at `http://www.drbilllong.com/Sales/FormationI.html`
19. Janis Schuller: *Designing and Implementing a System for Digital Cash* Master's Thesis, University of Bremen, (2007)
20. Ian Grigg: *The Ricardian Contract* Proceedings of IEEE Workshop on Electronic Contracting, (2004) pp 2531
21. The *E* Language Online references at `http://erights.org/elang`