Intrinsic Limitations of Digital Signatures and How to Cope With Them*

Ueli Maurer

Department of Computer Science
ETH Zurich
CH-8092 Zurich, Switzerland,
maurer@inf.ethz.ch

Abstract. Digital signatures are a core enabling technology for the automation and digitization of business and government processes. Despite the slow progress in their use for non-repudiation services, there is little doubt that in a few years digital signatures will be a key mechanism in digital business applications.
A fundamental intrinsic problem with digital signatures is that they are not linked to any event in the real world, even if enhanced with time stamps and other confirmation information. It is inherently impossible to determine when, where, how, and by whom a digital string was generated. A user takes the abstract risk to be liable for a signature generated without his consent, for instance because of a security problem in the system, a flaw or ambiguity in the user interface, a flaw in the cryptographic mechanism, fraud or errors in the certification process, or any other of many possible reasons.
The goals of this paper are to discuss the role and limitation of digital signatures and to propose digital declarations as a simple new concept for coping with these limitations. The user signs, in addition to the digital document, the recording of a conscious act related to the document, thereby confirming his consent. Some possible embodiments are the digital recording of the user's voice, an image, or a video stream.
Like a conventional signature, a digital declaration assures that the signer is guaranteed to be aware of whether and what he agreed to and signed, which is essential to make a denial meaningful and thus possible. Digital declarations can also provide a substantial additional level of security. Moreover, they can improve user acceptance by lowering the psychological barrier for committing to a public key, allow illiterate people to participate in e-commerce, facilitate the adoption of signature legislation, and substantially reduce the technical security requirements and hence the overall systems cost.

1 Introduction

Perhaps the main paradigm shift of the emerging information society is that digital information, like software, digital multi-media content, or digital signa-

* This paper appeared in Proceedings of 6th Int. Conf. on Information Security (ISC '03), C. Boyd and W. Mao (eds.), Lecture Notes in Computer Science, Springer-Verlag, vol. 2851, pp. 180–192, 2003.

tures, are becoming a key ingredient of business and government processes and, more generally, of many activities in the society at large. The full consequences of this paradigm shift seem far from well-understood and remain to be seen, but without doubt they will be far-reaching.

1.1 Digital Signatures as Evidence: Promises and Obstacles

In view of the continuing automation and digitization of many business processes, the transmission, storage, and verification of physical evidence, like signed contracts, presents a major problem. In contrast to physical evidence, digital evidence (like digital signatures, certificates, and time stamps) is easy to transmit, archive, and search. Moreover, digital evidence is generally unambiguous because its verification corresponds simply to the evaluation of a well-defined mathematical predicate (e.g. the signature verification predicate relative to a given public key). For these reasons, digital signatures promise to provide an elegant solution to the non-repudiation problem in the digitally operating economy.

Furthermore, due to the conjectured security of the underlying cryptographic mechanisms, digital signatures also promise substantially higher security compared to conventional signatures, and hence fewer disputes and simpler dispute resolution.

Despite the promises, in the context of non-repudiation services digital signatures are currently used only in isolated applications. We are still far from an internationally operational framework and infrastructure. Some of the obstacles are (temporary) technological problems (e.g. integrating PKI-technology into smart-cards and mobile devices), the lack of internationally applicable laws, the lack of standardization, the lack of viable business models for fostering the creation of a global PKI, problems with the integration into business processes, and, last but not least, the abstractness and complexity of the subject matter, resulting in slow user acceptance.

A different but related obstacle is the intrinsic problem with digital evidence, which is the subject of this paper.

1.2 Goals and Outline of the Paper

In this paper we discuss the fundamental intrinsic problem with purely digital evidence, like a digital signature, that it is not linked to any event in the real world. It is inherently impossible to determine when, where, how, and by whom a digital string was generated. Digital declarations are proposed as a cost-effective pragmatic solution.

Legislation is discussed in this paper only at an abstract and generic level, without referring to the various national approaches and their similarities and differences. Current legislation is not our primary concern as future legislation will adapt to new research results and business practices, including those proposed here.

Throughout the paper one should keep in mind that the main purpose of collecting evidence is not to resolve disputes, but to avoid them in the first

place, by deterring misbehavior. Actual disputes are the rare exception and the technical and legal procedures must therefore be pragmatic, simple and as light-weight as possible, but sufficiently well-defined to enable actual dispute resolution if needed.

In Section 2 we discuss the role of conventional signatures in the context of the non-repudiation of a contract. In Section 3 we analyze the process of entering a contract, for collecting evidence, and for resolving a dispute, at an abstract level. In Section 4 we discuss the use of digital signatures as digital evidence and the intrinsic limitations, and in Section 5 we present digital declarations as a solution to the described problems. Section 6 provides a concluding discussion of some main points.

2 On the Role of Conventional Signatures

As a motivation for this paper, it is instructive to discuss the role of conventional hand-written signatures and why they are so useful in practice. despite the fact that their technical security is generally quite low. Conventional signatures are a pragmatic and flexible mechanism. For obvious reasons, they are generally not applicable for on-line transactions, but understanding their usefulness and value in a conventional setting can help us better understand the corresponding issues in the context of digital transactions.

An idealized (but of course naïve) view of the use of conventional signatures can be described as follows. A user's signature is well-defined, for instance by a master copy he has deposited. In case of a dispute, a signature allegedly issued by the user can be compared to his master signature. If one assumes that forged signatures can be recognized, then a signature is convincing evidence for the person's consent to the signed document.

In practice, however, things are quite different from this idealized view. First, most people's hand-written signatures are not very difficult to forge for a dedicated forger. In fact, some signatures like those often used by illiterates (e.g. "xx") can trivially be forged. Second, in most settings (except for example in a bilateral business relationship with a bank), a person's master signature is neither deposited nor defined. Third, a person could use a signature different from the master copy in order to be able to later repudiate it. To avoid this last problem, the other party would have to have on-line access to the signer's master signature.

Therefore the value of a hand-written signature is not primarily that it is difficult to forge, but rather that it creates a situation in which a person *knows* whether or not he or she signed, thus guaranteeing his *awareness* of performing a conscious and willful act, as discussed in more detail in Section 3. Similarly, forging a signature also requires a conscious act.

Due to this guaranteed awareness, the denial of having signed a document is a precise and meaningful claim, equivalent to the (serious) claim that the signature is forged. Requesting the alleged signer to testify takes a conscious denial to an even more serious level. The importance of a typical contract would

not justify perjury. This is a main reason why there are only rare disputes about *who* signed a document. Most actual disputes are about the interpretation of the content of a contract, a problem we can ignore in this paper.

The described view on conventional signatures is in sharp contrast to what digital signature achieve. The existence of a digital signature does not imply the guaranteed awareness of the alleged signer of the act which caused the signature generation. A signature could have been computed by a virus, because of another security problem, a flaw or ambiguity in the user interface, a flaw in the cryptographic mechanism, fraud or errors in the certification process, or any other of many possible reasons. Therefore a signer cannot meaningfully deny that a signature was generated by him, even if the probability of the potential problems listed above can be reduced by (expensive) security technology. Rather, a denial is equivalent to the quite useless claim that the user is not aware of having issued a signature.

3 Contracts and Evidence

In this section we discuss, at an abstract level, contract signing, non-repudiation, the role of evidence and witnesses, and the reason why guaranteed signer awareness is important. Evidence is used in this section as a general term, and the special case of digital evidence is discussed in Section 4.

3.1 Entering a Contract

A basic act in business and other contexts is to enter an agreement, often called a contract, between two (or more) entities. Such an agreement requires the clear mutual understanding of all relevant parameters, in particular the terms and conditions. An agreement is valid only if both parties entered it. It is generally understood that a contract has been entered by a user or entity only if he or she (or an authorized representative) performed a well-defined conscious and willful act, for instance by shaking hands and/or by signing a paper document.

In order to prepare for a possible future dispute, each party to a contract wants to keep sufficient evidence for the fact that the other party performed the relevant act confirming agreement to the contract. This is a symmetric goal, although the evidence gathered by each party may be different. Here we consider only one side of the symmetric problem[1]: How can an entity V obtain sufficient evidence E that the other party U entered the contract C, i.e., that U performed an act A which confirms agreement to C. A typical example, relevant in this paper, is a user U who orders a product or service (for instance a banking transaction) on-line from company V.

One can distinguish three types of evidence: physical evidence, statements by witnesses, and digital evidence. A typical example of physical evidence is a signed

[1] We leave out of consideration the theoretically interesting, but in many practical settings not very relevant fair-exchange problem, namely that the evidence should be exchanged simultaneously, with no party gaining a temporary advantage.

paper document. A typical example of digital evidence is a digital signature. The role and limitations of digital signatures will be discussed in Section 4.

3.2 Basic Requirements

At an abstract level, the two basic requirements for a procedure for U to enter a contract C with V are as follows.

- **Feasibility.** It is feasible for U to perform an act A, resulting in evidence E, which V accepts as sufficient to convince a judge if necessary.[2]
- **Unforgeability (security).** The risk that convincing evidence E (for the claim that U performed an act A confirming agreement to C) is generated without U's consent is small enough to be acceptable for U.

These two requirements are inherently conflicting. As in most other contexts, there is a trade-off between feasibility and security. As a coarse classification, one can perhaps distinguish the following three levels of unforgeability of evidence:

- Lowest level: Forging the evidence may be easy but requires a dedicated (e.g. legally prohibited) act of forgery, i.e., it cannot be generated accidentally. An example is a handwritten signature which in many cases is quite easy to forge, but a forgery requires a conscious act.
- Medium level: Forging the evidence is technically non-trivial, though perhaps possible for a dedicated powerful forger. An example might be a video showing a person performing a certain act.
- Highest level: Forging the evidence is virtually impossible. An example is perhaps the signature and testimony by a notary.

For most applications it is infeasible to achieve the highest level. But even the lowest level can be sufficient for a pragmatic solution, as the use of conventional signatures illustrates.

3.3 Witnesses and Guaranteed Signer Awareness

It is often too expensive or infeasible to generate evidence that is by itself sufficiently convincing. For example, a signed contract alone, if denied by one party, is usually not sufficient evidence (see the discussion in Section 2). This is why witnesses are needed to resolve disputes, at least as a last resort when the evidence and the parties' statements remain conflicting.

However, for most types of contracts (e.g. an on-line transaction) it is impossible, too expensive, or impractical to arrange for an external witness to be present when U performs act A (e.g. clicks "OK"). In this case, the only reasonable alternative for resolving a dispute is to let U and/or V testify as witnesses.

[2] For example, in an e-commerce context, feasibility requires that the customer U need not physically meet the seller V.

This significantly reduces the chance of false statements because perjury is considered a significant crime and punished severely. For most contracts, perjury is not worth the risk of being so convicted.

But using an involved party U as a witness is useful only if it is guaranteed that he or she *can* indeed testify, i.e., if there is a clear (preferably yes/no) question which he can definitely answer and which, under the assumption that it is answered correctly, would resolve the dispute. This requires that U is guaranteed to be aware of the correct answer because then answers like "I don't know" or "I am not sure" are unacceptable and can reasonably be held against him. Guaranteed awareness assures that in a dispute, one of the parties is necessarily *consciously* lying, and hence makes a request to testify meaningful. This fact prevents false denials in the first place, avoiding the need for actual dispute resolution.

4 Digital Evidence and its Limitations

4.1 Non-Repudiation Based on Digital Signatures: A Common View

In simplified terms, a quite common view of how digital signatures could be used for non-repudiation services is as follows. Each user commits to a public key, i.e., declares liability for documents of certain types correctly signed relative to his public key.[3] A public-key certificate issued by a trusted certification authority (CA) can be used as evidence for this commitment. Certificates (or public keys) can be revoked if the need arises, for instance when the private key is lost or leaked. If the public key has not expired nor been revoked at the time of signing, then the user is liable for the signed contract.

This requires the ability to determine whether a signature was generated prior to a certain time. For this purpose, one can ask a trusted time stamping service to issue a time stamp. For example, a time stamp on a document (in this case a signature) is a signature by the time stamping authority on the document together with the time when the time stamp was issued. Hence it is, like the signature itself, purely digital information. More generally, the entire evidence resulting from a digital signature process, including certificates, time stamps and other possible confirmation information like certificate validation messages, is purely digital.

4.2 Definition and Discussion of Digital Evidence

The entire digital evidence relevant in a given context can be thought of (and represented as) a single bitstring s, even if it consists of several parts (e.g. a digital signature, certificates, time stamps, and certificate validation information).

[3] A user's commitment to a public key would typically involve signing a paper document, which in addition to the public key can also specify an expiration date, an upper bound on the value of a transaction, or other limitations of liability. These parameters must be correctly reflected in the certificate.

The verification of such digital evidence s corresponds to the evaluation of a Boolean predicate

$$v : \{0,1\}^* \to \{\textsc{True}, \textsc{False}\}$$

and is hence unambiguous. The predicate v summarizes the entire verification computation that needs to be performed, including the verification of the signature, the certificates, the time stamp, etc. A string s is accepted if and only if $v(s) = \textsc{True}$.

Conceptually, to be committed to a signature public key means to be committed to such a predicate $v : \{0,1\}^* \to \{\textsc{True}, \textsc{False}\}$. If somebody manages to produce a bitstring s for which $v(s) = \textsc{True}$, then the committed user is liable for whatever s is evidence for. We call this the *digital liability exposure* of a user, meaning that the mere appearance of a bitstring s, independently of how, when, and where it was generated, makes the difference whether or not the user is liable. The fundamental intrinsic problem with purely digital evidence is that it is not linked to any event in the real world. This point deserves some further discussion.

One might be tempted to argue that a time stamp guarantees when the evidence was generated. But the time stamp is itself digital and as such not related to time. A time stamp should be interpreted as providing an additional level of security, since forging a time stamp (and the signature) can be assumed to be more difficult than forging the actual signature alone. More precisely, the time stamping authority can be seen as the user's delegate, with high security standards, trusted (by him) to issue a time stamp (and hence cause liability) only with the correct time. But obviously, if somebody manages to forge the signature and the time stamp, plus the other possible parts of s required to yield $v(s) = \textsc{True}$, then the user *is* liable.

This view may still seem to be somewhat odd, as the circumstances of how s was generated really do seems to matter. For example, one could try to argue that the digital evidence s is needed only as evidence, possibly together with other (physical) evidence, to conclude that the user performed a well-defined act (i.e., clicked "OK") on the user interface, and that it is this act which implies liability, not the digital evidence. But the core question is whether or not the digital evidence *can* make the difference between liable and not liable. If it never can, because a decision is always ultimately based on other evidence, then it is useless and should not be applied in the first place. If it can make a difference, which is indeed the case in any envisioned scenario for using digital signatures, then the above arguments apply, namely that the mere appearance of a bitstring s satisfying $v(s) = \textsc{True}$ implies liability.

This is a problem one needs to address. There is a trade-off between the usefulness of digital evidence on one hand and the digital liability exposure on the other hand. Digital evidence that is relevant only in rare cases is not useless and would not justify the investments into the necessary infrastructure.

4.3 The User's Abstract Risk

As recognized by legislators, the use of digital signatures is problematic because of the described digital liability exposure. The owner of a public key is forced to take the substantial and abstract risk to be liable for signatures generated without his consent.

What happens when indeed a digital signature shows up for which the user has absolutely no explanation? There are many reasons why this could happen. Some are discussed below.

1. The secret key could have leaked to a third party, for instance due to a security problem in the system or a timing or power attack on the user's smart-card.
2. The signature could have been generated by the user's system, but without his consent, for instance due to a virus or other malicious software component on the system with the inserted smart-card. The virus could either
   a) call the smart-card without the user being aware, or
   b) display a contract different from that actually signed.
3. The signature could have been generated by the user's system, without any influence from an outsider or a virus, but nevertheless without the user's consent and awareness. This could happen for instance if
   a) the user interface is not sufficiently clear about which action (e.g. clicking "OK") initiates the signature generation,
   b) the user does not carefully follow all the required steps, perhaps because he does not understand the complex matter, or
   c) another person is using the user's system or secure signature device.

   Another possibility is that the user simply forgot that he actually completed a transaction.
4. The cryptographic signature function might be broken, meaning that somebody has found a way to either compute a user's private key from his public key, or to generate signatures for a given public key without knowing the secret key.[4]
5. The certificate could be false, for instance because of a criminal CA employee or because the CA's private key is compromised.

When a user is confronted with a signature (for his public key) for which he has no explanation, the user has no clue which of the above reasons applies. Therefore he cannot even meaningfully deny a digital signature.

[4] Current proposals for digital signature schemes depend on the assumed computational hardness of a very specific mathematical problem, for instance factoring large integers. It is conceivable that a fast algorithm for solving this problem will be discovered. Even worse, such a discovery might not necessarily be reported to the public.

4.4 The Envisaged Solution for the Digital Evidence Dilemma

As discussed above, no matter how a system is designed and how legislation is set up, *purely digital evidence does imply liability*. The envisaged approach to solving this dilemma, followed in certain legislations, is as follows. In order for digital signatures to be legally binding, both the technical infrastructure and the processes must satisfy very high security standards so that it appears virtually impossible that a signature is generated without the user's consent. Some of the requirements are:

1. Very high security standards for the CA's technical infrastructure, processes, and personnel supervision and recruitment.
2. High security margins in the choice of the cryptographic security parameters. Possibly use of several signature schemes in parallel.
3. The user interface is required to be highly unambiguous, essentially excluding any misunderstandings by the user.[5]
4. The user's private key is stored in a very secure device, without possibility to extract it.[6] Signatures are generated in the device. Because of the described virus attack, the device should ideally have its own input and output mechanisms, for instance a keyboard (at least a confirmation button) and a display.
5. The security of a device could be increased further by a biometric identification mechanism, allowing only the designated user to activate the device.

There is an obvious trade-off between the achieved level of security on one hand and the cost and practicality on the other hand. Moreover, even if the technical security is carried to an extreme (and impractical) level, it is impossible to eliminate all sources of uncertainty. For instance, no such solution can prevent a disaster in case the cryptographic signature scheme were broken.

5 Digital Declarations: A Pragmatic Approach

5.1 The Awareness Issue

As described above, a digital signature, even if time-stamped or otherwise confirmed, cannot imply that a user agreed to a certain document. Even worse, it does not even imply that the user is aware of the fact that the document was signed, let alone of its content. This is in sharp contrast to hand-written signatures, as described in Section 2. The user is forced to be aware of the act of signing, and since one is supposed not to sign a document without reading it, it is also reasonable to conclude that he is aware of the content.

A previously proposed technique for addressing the awareness problem is to ask a user to type a certain word or text on the keyboard. The correctness of the

[5] However, this also requires more advanced skills on the user's part.

[6] Smart-cards may actually not be sufficiently secure.

typed character sequence is checked before activating the signature generation. However, this solution does not solve the problems described in Section 4.3. All it can guarantee is that, provided the entire system is working correctly, a user will not accidentally perform the act required to activate the signature generation. Thus it solves only problems 3a) and 3b) of the list in Section 4.3, but it does by no means prove that he performed the act. Similarly, biometric identification technology can only solve problem 3c).

5.2 Digital Declarations

We propose a new solution to address the full list of problems stated in Section 4.3. The user performs some act related to the relevant contract, and this act is recorded digitally and combined with characteristic information of the digital document. This is called a *digital declaration*. In a typical implementation, the digital declaration can be signed together with the actual digital document. It can also be time-stamped.

Digital declarations can be embodied in many different ways. As an example, a user ordering a product on-line might be asked to speak a certain sentence referring to the product, the price, and the date of purchase.[7] As another possibility, the willful act could be documented by a digital image, a video sequence, or by any other recording device possibly invented in the future. Future implantation technology can open another host of possible applications.

Digital declarations can be an essential feature of future digital transaction systems. Some of the reasons are:

- guaranteed user awareness,
- higher deterrence of misbehavior, hence fewer disputes,
- improved security compared to conventional signatures,
- lower cost[8] due to reduced technical security requirements,
- improved user acceptance of digital signature technology, and
- usability by moderately educated people.

Let us expand on some of these points.

5.3 A Discussion of Digital Declarations

A digital declaration guarantees a user's awareness, the most crucial property of conventional signatures. Therefore a user can, in case of a dispute, request

[7] It should be pointed out that digital declarations are different from current standard practices like the recording of phone conversations in the context of brokerage services. The digital declaration is recorded by the user's device and typically signed together with the digital document.

[8] There is no cost for extra hardware as one would the recording hardware of the same device that people are using for other purposes, for example a next-generation mobile phone.

the digital declaration to be presented, say in court. Like for a hand-written signature, the user has the possibility to deny the digital declaration. When confronted with the declaration (e.g. the speech signal) he knows precisely whether or not it is forged. Hence a denial is equivalent to the claim that the declaration is forged, bringing such a claim to the same (serious) level as the claim that a particular conventional signature is forged. A user can therefore meaningfully be forced to testify. The refusal to deny the digital declaration can reasonably be taken as evidence against the user. This fact is not only essential in a dispute, it helps prevent fraudulent denials in the first place.

Most types of digital declarations (like a voice recording) are non-trivial (though not impossible) to forge and offer considerably improved security compared to, say, conventional signatures. Future recording technologies may even be much harder to forge. But digital declarations make of course sense even if they are considered only moderately hard or even easy to forge, as long as a forgery requires a dedicated act. Moreover, they would typically be used together with digital signatures.

It is quite possible that some future e-commerce solutions will involve human sales representatives, for various reasons, including the potentially improved sales efficiency and the costumers' need to obtain specific advice. In such a case, documenting part of the human interaction in the signed contract, i.e., using digital declarations, is a very natural possibility.

A digital declaration makes sense even if it is not checked by the recipient, for instance by a human operator. In fact, in the context of e-commerce, it may not even be possible to completely verify a declaration because the person whose voice or image is recorded need not yet be known to the on-line shop. Even in such a case, the digital declaration makes sense if customers can generally be assumed to be honest at the time of the order but must be deterred from later repudiating the transaction.

User acceptance is a key issue in e-commerce. Digital declarations lower the psychological barrier for using digital signature technology for non-repudiation services. One knows that if worse comes to worst one could request a digital declaration to be presented, with the possibility of denying it. It is impossible to give such an assurance with the currently envisaged use of digital signatures.

Yet another advantage of digital declarations is that they are very intuitive and hence can be used by a substantially larger, moderately educated user community.

Perhaps the most important reason for using digital declarations is that they can allow to establish a reasonable compromise between cost effectiveness, user friendliness, security, and legal issues. For the envisaged use of digital signature technology, sufficiently secure hardware may be too expensive for cost-sensitive large-scale applications. It can be expected that legislation will be adapted to new technical solutions, and digital declarations are closer to a conventional legal understanding. The commercial success of a new technology (e.g. digital signatures) is often determined not by the technology itself but by the cost, the

user friendliness, and the adequacy of the underlying business model. Digital declaration can change this model.

6 Concluding Remarks

A basic dilemma in digital signature legislation (more generally digital evidence legislation) is to specify what constitutes a user's commitment to a digitally signed contract. Is it the *existence* (more precisely, the presentation) of the digital signature on the contract, or is it the user's act (interacting with some user interface) which initiates the computation of the signature? It cannot be both.

Both viewpoints are problematic. In the first approach, there is not even a chance for the user to argue, when confronted with a valid signature, that he did not sign. However, as was argued in this paper, the fact that purely digital evidence *does* imply liability is unavoidable. Otherwise digital signatures would be useless. This is true even if digital declarations are used in connection with digital signatures, but in this case the digital signature is less important as it matters primarily when the digital declaration is ambiguous.

In the second approach, where it is the *act* that counts, the digital signature is only supporting evidence for the fact that the user performed the relevant act. In this case it is relevant which other evidence is accepted in a dispute. There is a dilemma: Either a user has no reasonable and fair chance of denying a signature he has not issued (because the signature generation process is supposed to be so secure that errors can virtually be excluded), or the usefulness of digital signatures is severely limited because the recipient of a signature bears the risk of a later denial, which he cannot influence. This dilemma is intrinsic. The only viable solution appear to be digital declarations, as described in this paper.

To make an example, suppose one would allow a user to deny a digital signature because he provably had no access to his signature device at the time of signing. Moreover, it may even be evident that nobody else had access to the device, perhaps because it is known to have been destroyed at the time the signature was generated, or because the device's biometric identification mechanism is known (and testified by the experts) to be totally secure. If both claims are correct, this implies that the signature could not have been generated in the device. However, accepting such reasoning would be unfair towards the recipient of the signature as he has no way to check these facts. It would open the door for fraudulent denials and would undermine the envisaged advantages of using digital signatures. For example, some witnesses could confirm that the device was destroyed before the signature in dispute was generated.

In practice, technology is always used in a pragmatic balance between security on one side and cost-efficiency and convenience on the other side, often giving security actually a lower priority. This is often justified by the underlying business model which determines who takes the risk in case of a security problem. A prime example are credit card transactions which are quite insecure from a technical viewpoint, but the business model still seems to work, despite quite massive fraud. What this paper calls for is a pragmatic solution in the area

of non-repudiation of on-line transactions. It seems that the security demands by legislation and other players may have been too high in the past, and this is probably one of the reasons for the slow adoption of digital signatures and public-key infrastructures in practice. There is definitely room for finding a more pragmatic and cost-efficient balance.

It was unavoidable to make simplifications in this paper, especially with respect to legislation and how the legal system works. Many subtle aspects were ignored, some of which the author may not be aware of.

The paper contains no references because any specific selection would appear to be arbitrary. However, we refer the interested reader to two classical books [1, 2] on security technology.

The views on digital signatures presented in this paper also lead to a new interpretation of the role of certification authorities, time stamping authorities, certificate expiration, certificate revocation, and many other aspects of a public-key infrastructure. For example, a certificate could be interpreted as the digital statement by the CA that it (the CA) holds physical evidence (a signed document) of the user's commitment, which it could present if the need arises. In this view, the CA can be seen as the signature recipient's delegate, and the certificate owner need not even trust the CA because the certificate alone, without the physical evidence, implies no liability. These ideas will be presented in a separate paper.

References

1. A.J. Menezes, P.C. van Oorschot und S.A. Vanstone, Handbook of Applied Cryptography, Boca Raton: CRC Press, 1997.
2. B. Schneier, *Applied Cryptography*, Wiley, 2nd edition, 1996.