RZ 3232 (#93278) 05/22/00
Computer Science/Mathematics 31 pages

Research Report

Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity

Birgit Pfitzmann[1], Michael Waidner[2], Andreas Pfitzmann[3]

[1] Universität des Saarlandes, Saarbrücken
pfitzmann@cs.uni-sb.de

[2] IBM Zurich Research Laboratory, Rüschlikon
wmi@zurich.ibm.com

[3] Technische Universität Dresden, Dresden
pfitza@inf.tu-dresden.de

Research Division
Almaden · Austin · Beijing · Delhi · Haifa · T.J. Watson · Tokyo · Zurich

Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity*

Birgit Pfitzmann[†], Michael Waidner[‡], Andreas Pfitzmann[§]

This text is translated from the German article *"Rechtssicherheit trotz Anonymität in offenen digitalen Systemen,"* which was published more than 10 years ago: first in 1987 in *Computer und Recht Vol. 3 No. 10–12*, and with some revisions in 1990 in *Datenschutz und Datensicherung (DuD) Vol. 14 No. 5&6.* The translation is based on the 1990 version.

The text was written for an audience interested in computer science and law, i.e., not primarily for the IT security expert. In those days the assumed technical basis for electronic commerce was "ISDN." Today's readers may read "the Internet" instead.

The text is an unedited translation.

Abstract

The growing importance of conducting legal transactions over open digital systems creates new requirements for these systems. They have to be designed in such a way that the users remain anonymous to one another and their activities cannot be observed by uninvolved parties. At the same time, the systems have to guarantee the necessary legal certainty for the transactions being carried out. It will be demonstrated (Section 1) that legal regulation alone is not sufficient to ensure that these requirements are dependably met.

For this reason, known technical methods and new proposals from the field of information technology are presented as a complement to legal regulation. On the one hand, these proposals guarantee unobservability and anonymity when using the system (Section 2) and, on the other hand, they provide sufficient legal certainty for the conduct of typical business processes over the open system without sacrificing anonymity (Section 3). Due to their particular importance, two issues are presented in more detail: two methods to prevent fraud during the exchange of values between anonymous parties (e.g., an information service offered in exchange for payment) (Section 4), and an anonymous digital payment system and variants of it (Section 5). The paper concludes with an overview of open problems and a practical evaluation of the issues (Section 6).

*This article was written while all authors were with the University of Karlsruhe, Institut für Rechnerentwurf und Fehlertoleranz, Germany.

[†]Universität des Saarlandes, Fachbereich Informatik, pfitzmann@cs.uni-sb.de

[‡]IBM Zurich Research Lab, wmi@zurich.ibm.com

[§]Technische Universität Dresden, Fakultät Informatik, pfitza@inf.tu-dresden.de

1 Introduction

The German PTT's introduction of new communication systems, ISDN (Integrated Services Digital Network), will lay the foundation for the introduction of *open digital systems.* Initially, it will only unify the narrow-band communication services, such as telephone, telex, teletex, etc. Later, however, all broad-band communication services, such as television and long distance visual-audio communication, will be united and offered to users via a few "multifunctional" devices [69, 70, 71]. An open digital system should be potentially available to all users of ISDN and it should offer special services. Possible services include pure information services (as successors to teletex) making special data bases available to their users, the dissemination of POS terminals, and "electronic marketplaces," which allow users to offer and order goods, transfer money, in short, enable users *to conduct a variety of legal transactions* [66, 76].

This transfer of everyday business to a digital environment will essentially create two problems:

For one, the current regulations applying to legal transactions generally assume that living human beings, of flesh and blood, make declarations of intent in an unforgeable manner, e.g., by means of signed documents, and that the submission of these documents can be confirmed by equally human counterparts. In an open digital system the person is represented by his computer and, moreover, the computer does not create signed physical documents, but only digitally encoded information which can be arbitrarily copied. Furthermore it is more likely that a machine, rather than a person, will be able to witness that this information has been created. For instance, the machine might be a PTT computer that transmitted the information via ISDN to the recipient, and the information could represent a legally binding order for goods.

Evidently, time-honoured standards, in particular statutory regulations and conventions about what should be accepted as evidence, do not take the new conditions related to digital systems into account and will have to be adjusted in order to achieve legal certainty. In this adjustment, care has to be taken that the regulations continue to fulfil the same purposes as before. For example, omitting signatures as in teletex clearly fails to achieve this, because the technical system has to offer an equivalent for signatures which provides unforgeable evidence that a particular user is the originator of a particular message [63].

On the other hand, the use of open digital systems makes the user much more transparent than was previously the case.

For instance, the business partner usually obtains much more precise information about what interests the customer if he offers an encyclopaedia service, rather than selling the entire encyclopaedia, or by offering pay TV in place of broadcasting television programs. Similarly, entirely new business partners come up, e.g., the providers of special information systems, that can draw conclusions about their customers.

In addition, in many business transactions more partners will be involved than before. For instance, banks will be involved in every payment via ISDN when certain digital payment systems are used (see Section 5) and in virtually every purchase when POS terminals are used, even if the goods have not been ordered via ISDN. This applies in particular to partners such as the PTT in its role as a distributor of teletex where, due to its mediator function, it is involved in a variety of different transactions made by the same user.

In addition to the business partners who necessarily obtain certain information, it is also possible for fully uninvolved parties to obtain information about the user by observing the open system, or the ISDN used for communication. Observers may be the service provider, e.g., the PTT or the provider of value-added services, the software or hardware manufacturer by means of Trojan horses, or other parties by tapping lines.

As the obtained information is already in digital form, all these parties can arbitrarily store it, evaluate it more efficiently than in the past, and compare it to information obtained by other parties.

The opportunities for obtaining information apply, of course, not only to selected individual users, whose personal rights are legally restricted by the G10 law. Many of the possible observers have the opportunity to collect data about a large number or, in fact, all users of a system. As a result, there is an opportunity for mass surveillance. (This is distinct from conventional surveillance techniques like wire tapping, which continue to exist, but which are only feasible for individual surveillance due to the effort involved.)

It is reasonable to question whether a system that seriously endangers the personal rights of the general public is compatible with our constitution, in particular if one considers the right to informational self-determination as expressed in the national census judgment by the Federal Constitutional Court [16].

Both problems mentioned, on the one hand the adaptation of applicable standards to the new environment and the design of systems in such a way that legal certainty is provided and, on the other hand, the protection of personal rights, have to be resolved before a system is allowed to be put into use. The goal of this article is to show that both problems together can be resolved for open digital systems and to present approaches which are suitable for actual use.

2 Anonymity

2.1 Anonymity According to the Law

The first approach at achieving open systems which do not endanger the personal rights of their users and cannot be misused for mass surveillance is to legally prohibit the processes necessary for surveillance. This has been done, if not to the necessary extent, in the data protection laws and through the telecommunication secrecy regulations.

These processes essentially consist of data collection on the part of non-participants, e.g., the PTT, and the undesirable processing or passing on of the collected data by participants.

If such processes are possible, legal prohibition comes up against two principle limitations:

Due to the ease of copying and processing data, the enforcement of such a ban is difficult. Data, even if obtained legally, is not changed when processed, with the result that constant monitoring of the data would have be carried out. Even a single gap in this monitoring process can result in data being passed on unnoticed. Once there is a copy outside the legal sphere, it is virtually uncontrollable.

Even when an unauthorised transfer of data is detected (or precisely if it is), irreparable damage may already have occurred, e.g., if a user's personal data have been published.

It can be argued that it is justifiable to place a certain amount of trust in some uninvolved and involved parties to a business transaction: the PTT, in the role of ISDN provider, would certainly not observe its customers, and one could also scarcely deny that banks at least intend to handle their customers' data in a trustworthy manner.

Unfortunately, potentially interested observers and business partners cannot be restricted to this circle alone. For instance, it is not currently possible for the PTT to guarantee that the ISDN software and hardware it uses are free of covert system components (so-called Trojan horses, see [62, 75]), which pass on sensitive information to the manufacturer, e.g., by means of the frequent maintenance required by systems of this size. It is equally impossible for a bank to guarantee this of its computer centre. Nor can one guarantee that normal wire tapping will not be used, or that employees will treat data confidentially. For mass surveillance, however, wire tapping presents less of a threat, and so do employees if suitable organisational structures are in force.

Hence a purely legal solution to the problem is impossible. It is therefore necessary to try to prevent the undesirable collection and processing of data by additional technical measures. This requirement also arises when the Federal Data Protection Law (and appendix, [41]), is appropriately applied to open digital systems.

2.2 Technical Measures for the Protection of Data

If one wanted to implement technical data protection centrally, that is through the system provider or by placing him under public supervision, the system administration would have to be done by so-called secure devices, which never output certain data. However, such central devices are so complex that is impossible to check them thoroughly for Trojan horses with state-of-the-art methods. The checks would also have to be repeated after each maintenance measure. Last but not least, the technical reliability of a central device which has to react to actual as well as suspected attacks on its integrity by destroying at least its sensitive data, would be minimal.

Hence even technical measures cannot fully resolve the problem of the arbitrary copying and processing of data once it has been collected. A technical guarantee can, however, be provided that no unnecessary data can be collected. To achieve this, the technical data protection measures must essentially be carried out by the user himself.

Such a strategy would be preferable even if all the technical problems mentioned above had been resolved, because it is the only one where individual citizens can monitor the measures themselves. This is important because, according to good common sense and the rational behind the decision of the Federal Constitutional Court in respect of the Census of December 1983 ([16], Page 272), not only should

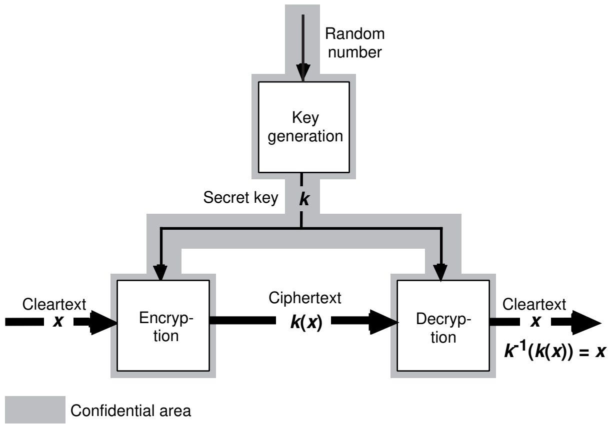

Figure 1: Symmetric Encryption System

citizens be secure and unobserved, but they should also feel that they are. In addition, decentralised implementation makes it more difficult for the state to make a rapid and unpublicised change in the data protection regulations.

The same principles which underlie the following measures for data protection also apply to the measures for achieving legal certainty presented later: Both should essentially be carried out by the user himself and not by a system provider.

For the implementation of all of these measures, however, the user may take advantage of computer support. There are sufficiently small and inexpensive computers for these purposes, e.g., PCs which are only slightly more expensive than terminals which are, in any case, necessary for participation in an open system. It is also possible to manufacture these devices reliably and to monitor them publicly, so that every user can at least be certain that his computer will not act against his will and, in particular, not contain a Trojan horse which reveals data about him without his permission. In the following, actions of the user himself and of his computer will usually not be distinguished.

2.2.1 Unobservability Towards Uninvolved Parties

A fully uninvolved observer of a transaction, e.g., an eavesdropper or the PTT, need not and should not obtain any information: the transaction should be *unobservable* for him. Ideally, he should not even be able to find out that a transaction is taking place, or at least not between what parties.

If a transaction is implemented purely by the exchange of messages via a communication system, e.g., ISDN—as we generally assume—the use of a suitable *encryption system* and an *anonymous network* is sufficient for this.

2.2.1.1 Encryption Systems. Encrypting data by using an encryption system should guarantee that the contents of a transmitted message are only available to the owners of a certain key. (A good and well-founded introduction to encryption systems can be found, for example, in [34, 45, 12, 31].)

In respect of the permissible and feasible distribution of these keys, one distinguishes *symmetric* and *asymmetric* encryption systems. The former is often called conventional cryptography and the latter public-key cryptography.

In a symmetric encryption system (Fig. 1), to which all classical encryption systems belong, the communication between two partners is secured by means of both parties possessing a common key, which is used both to encrypt and to decrypt.

Hence a key is not assigned to a particular user, but to a particular communication relationship. In order to commence a communication relationship securely, the partners have to have agreed on a common key. In open digital systems, this has to take place within the system itself because one cannot assume that the partners have previously been in direct contact with one another. There are essentially two approaches for solving this key distribution problem.

The classical solution provides for a key distribution centre, which is external to the system. Each user exchanges a key with this centre before participating in system activities. Upon request, this centre generates a key for a communication relationship and distributes it to the future communication partners

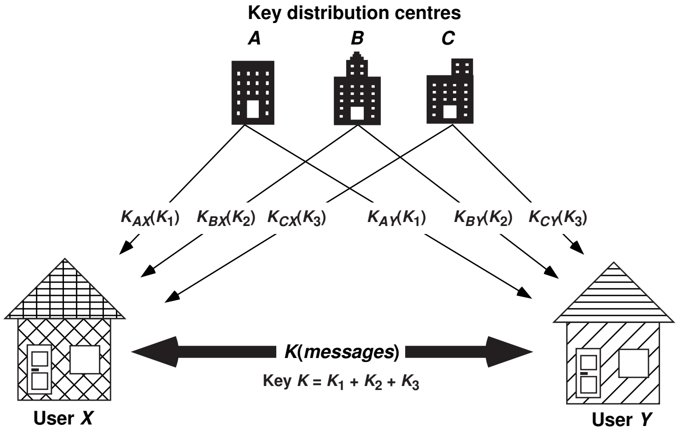

Figure 2: Key Distribution in a Symmetric Encryption System

in a confidential and authenticated manner using the key which has been agreed with the respective users [31].

Such a centre has the potential to decrypt all messages which are sent because it knows all the keys. Hence this simple solution is unacceptable for purposes of data protection, at least for open systems. A way around this is to use several independent key distribution centres, each of which generates a key and distributes it to both communication partners (Fig. 2). The communication partners then use a key which consists of the sum of all the keys distributed. Thus all the key distribution centres would have to collude in order to calculate this sum and monitor the communication.

The second approach uses an asymmetric encryption system for the distribution of keys, as described below.

The best-known modern symmetric encryption system is DES (Data Encryption Standard [35]), which was defined and published as an intermediary solution (until a better one has been standardised) by the NBS (National Bureau of Standards–the American Standards Authority for the federal government). Its security has not been proven, but to date it has withstood all (known) attempts to break it. Fast hardware and software implementations are available (20 Mbit/s [1, 4, 47, 12] on a chip, or with an Apple Macintosh IIci (MC 68030, 25 Mhz) 715 kbit/s [3, 55]. Hence, in combination with an asymmetric encryption system for the distribution of secret keys (hybrid encryption), it would be possible to make standard use of this in ISDN.

Applying the principle employed by DES and changing partial functions and using longer keys, it is possible to construct a number of symmetric encryption systems which could be implemented easily. Their security would not have been proven either, but it would be much less doubtful than with DES [3, 55].

In addition, there are also symmetric encryption systems with provable security:

The Vernam cipher (one-time pad, [73]) conceals the message contents perfectly, i.e., an attacker obtains no information whatsoever. However, due to the high key distribution overhead (a "new" key bit is required for every message bit), it is only suitable for special applications.

Some symmetric systems are "cryptographically" secure, i.e., breaking them would imply solving a basic problem that has been thoroughly investigated and is generally believed to be hard [77, 50]. A typical basic problem is the calculation of the prime factors of a given number. Factoring numbers which are made up of very large prime factors is, to date, virtually impossible [49], although mathematicians have been working on this for a long time. It has not, however, been possible to prove the infeasibility of this basic problem (or that of the others which have been used). The encryption speed of cryptographically secure symmetric systems is comparable to that of the following asymmetric systems.

The idea of asymmetric encryption systems (Fig. 3) was first published in 1976 [36]. It solves the key distribution problem in a surprisingly simple way: Instead of using a single key to encrypt and decrypt, this function is distributed over a key pair c and d. Key d is intended only for decrypting and must, of course, be kept secret; thus is also called the private key. In contrast, key c is intended only for encrypting and should not enable decrypting. Thus it can be made public and is also called the public key. In particular, there must not be any realistic possibility of deriving an unknown d from the corresponding c.

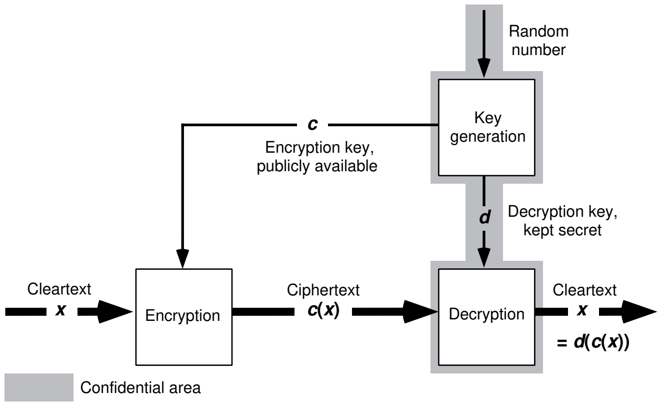

Figure 3: Asymmetric Encryption System

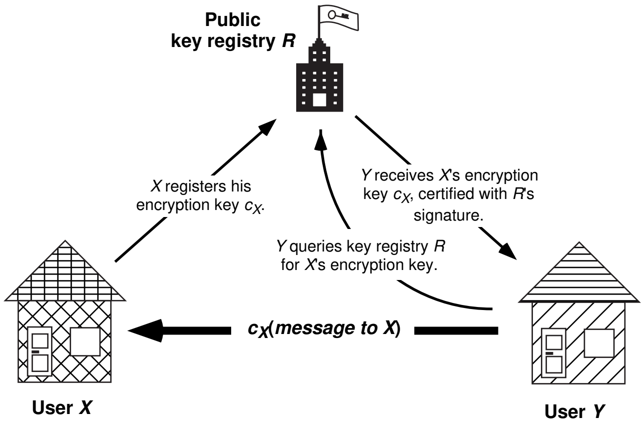

Figure 4: Key Distribution in an Asymmetric Encryption System

In theory d could, of course, always be determined by trying out all possible keys because only the correct d would correctly decrypt all messages encrypted with c. Hence there have to be so many possibilities that this approach has no realistic chance of succeeding.

In addition, in order to prevent anyone from guessing short standard messages and testing them with the public key, messages must have more than one form of encryption. This can be achieved by padding the message with a randomly selected sequence of characters before it is encrypted, or by using an encryption system which is already non-deterministically encrypting (probabilistic encryption [42, 9]).

In contrast to the difficulty of determining d from c, generating an arbitrary pair of a corresponding c and d has to be simple because the owner of the key pair has to do this at the onset.

By means of an asymmetric encryption system it is possible to assign a key or, more precisely, a key pair (c, d) to an individual user, rather than to a communication relationship. In addition, the user can generate this key pair himself. Should a person wish to communicate securely with this user, he simply has to obtain this user's public encryption key c. This can be achieved either by asking the communication partner openly, whereby problems of authentication arise [46, 67], or by means of central registers which are protected against manipulation (Fig. 4). The administrators of these register now no longer have an opportunity to obtain the contents of encrypted messages as a result of knowing the public keys.

In 1978, RSA, the first and, to date, best-known asymmetric encryption system (encryption, decryption and key generation) was published [68].

To date, the security of RSA has not been proven. It is generally conjectured that decrypting, given only the public key, is as difficult as determining the prime factors of a given number. Individual messages can, however, be decrypted by means of active attacks [33]. By combining RSA with an appropriate redundancy predicate (e.g., [60]), the risk of active attacks can be virtually eliminated. The security of these combinations, however, has not yet been proven either. Hardware implementations of RSA achieve encryption rates of 200 kbit/s (with a modulus of 660 bit, [72]). Software implementations are much slower (e.g., 57 bit/s on an IBM PC (intel 8088, 4,77 Mhz) [12] Page 31).

There are asymmetric encryption systems whose security against passive attacks has been proven to be as difficult as factoring [42, 9]. There is, however, (as yet) no asymmetric encryption system which has been proven to be secure against active attacks. (For the supposedly provable system sketched in [8], a proof of security has not yet been found [5].)

The use of an asymmetric encryption system such as RSA plus a redundancy predicate, either for the actual encryption or only to exchange a secret key of a faster symmetric encryption system at the onset of a business relationship, can, in our opinion, sufficiently guarantee that the contents of messages are kept secret from uninvolved parties.

For this reason the standardisation of an asymmetric encryption system for the exchange of keys, as well as a fast symmetric encryption system for en- and decrypting user data, is urgently required if ISDN is to be an *open* system. Otherwise, data protection (just as data security) will only be achievable within *closed* user groups which have agreed on an encryption system.

This problem is anything but new, but remains an unresolved organisational problem. At the national and international level there were attempts to standardise RSA and DES, but they have been abandoned [85]. Instead, the ISO has merely provided an opportunity to register arbitrary encryption systems (by means of describing their interfaces). An evaluation of the registered encryption systems is not planned ([31], Page 347).

It is to be hoped that the continuing lack of standards will at least encourage the German PTT, in its role as the provider of ISDN, to standardise appropriate publicly validated encryption systems.

2.2.1.2 Anonymous Networks. An anonymous network guarantees its users that neither the sender nor the recipient of a message can be determined without his cooperation, not even by the provider of the communication system (which is the major difficulty) or the communication partner. Since the known concepts for anonymous networks and their practicality is discussed in detail elsewhere [61, 59], and because for the following it is only important to be aware of their existence, we will not go into more detail here.

2.2.2 Anonymity Towards Involved Parties

It is clearly impractical to require that a transaction cannot be observed by a party to the transaction. To prevent the opportunity for collecting unnecessary personal data, the goal here is rather to conceal the identity of the user from his partners as far as possible, i.e., to keep him *anonymous.*

There are three criteria for determining the strength of anonymity.

The first is the *attacker model.* It describes from which partners the user should be anonymous and if this anonymity continues to exist if several partners, or also uninvolved parties, combine their information. A particularly important question is whether special authorities can reveal the identity of the one business partner at the request of another, should a dispute arise. Wherever possible this should be avoided because if a few authorities together can revoke anonymity, they have an overly strong position of power, and if a large number is needed (in an extreme case the entire user population), the revocation will be unreliable.

Secondly, given a particular attacker, one can ask among *how many possible actors* the party actually taking action is hidden. If possible, in open systems all users should be potential actors in any particular action. There can, however, be practical limitations due to the performance of an anonymous network [61, 59]. Then a party who submits a certain statement may be hidden among a large number of users, but not all, if his business partner and the network provider co-operate. Care must be taken that the number of possible actors is so large that the damage which would be incurred by an individual user, as a result of deanonymization, cannot simply be inflicted upon all possible actors, without the party causing the damage experiencing a greater disadvantage than advantage as a result [52]. For example, if a customer of a publisher of anti-constitutional material is revealed to be among a group of 10 persons, the constitutional loyalty of all 10 might be questioned and they might all have problems getting jobs in certain areas.

Thirdly, anonymity cannot only be considered in respect of isolated actions. Attention must also be paid to the extent to which a specific attacker can form a relationship between a number of transactions, or parts of a transaction, i.e., *link* these actions. In concrete terms, such linking of actions usually means that the partner knows that the same person has carried out two actions. For the purposes of data protection, linkability has to be kept to a minimum. However, for purposes of legal certainty,

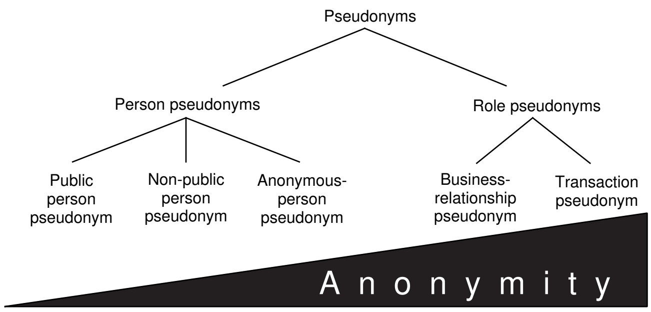

Figure 5: Classification of pseudonyms according to their linkability to a person

linkability is sometimes desirable, in particular between parts of the same transaction or, e.g., in repeated communication with a bank for purposes of authentication.

The strength of the anonymity of a user is not only determined by the characteristics which the partner automatically learns about user, e.g., the type of transaction and the time at which it is made, but, above all, by specially provided identifiers, such as identification numbers or digital signatures (see 3.1.2.1), so-called *pseudonyms.*

Fig. 5 shows a rough, but for practical purposes sufficient, classification of pseudonyms according to the strength of anonymity they achieve.

A pseudonym is called a person pseudonym if its owner uses it for a wide variety of business relationships over a long period of time and, as a result, it represents a substitute for his name. In respect of the opportunities for linking the pseudonym to the person, three basic types of person pseudonym can be distinguished.

If one considers the point in time when a person pseudonym is first used, then for a public person pseudonym, the assignment to a person is, at least in principle, generally known (e.g., telephone numbers). For private person pseudonyms this assignment is only known in very few places (e.g., account numbers, if used without the name, or unlisted telephone numbers). For anonymous personal pseudonyms the assignment is only known to the user himself. When person pseudonyms are used, an observer continuously gathers personal information, with the result that after some time the owner of a private or anonymous person pseudonym can be deanonymized. Every person pseudonym is, therefore, a potential identifier of a person.

Role pseudonyms, in contrast to person pseudonyms, are not assigned to a person, but only to the role a person is currently playing. Hence they avoid this disadvantage. Business-relationship pseudonyms are role pseudonyms used for many transactions, e.g., an account number which is used for all entries for one account. In contrast, transaction pseudonyms are used for only one transaction, e.g., the reference (box number) used for an anonymous advertisement. If role pseudonyms are used, different partners cannot simply link information gathered about one user by the pseudonyms, but at most by a correlation of the times where actions occur, the sums of money involved, etc. Nevertheless an intensively used business-relationship pseudonyms incurs the danger that the partner obtains enough information about the user for deanonymization. From the point of view of data protection, transaction pseudonyms should therefore be used whenever possible.

In the following, we write $p_R^S(X,t)$ for the pseudonym that person X uses in transaction t, where it plays role R (e.g., "customer") towards another person who plays role S (e.g., "service provider"). We omit indices and arguments in cases where they do not matter, e.g., the transaction identifier for business-relationship pseudonyms.

As already mentioned in 2.2.1.2, communication between partners who are anonymous to each other to this extent is readily achievable using an anonymous network, because messages can be sent without sender information and received using any number of pseudonyms which do not (as other addresses do) describe the physical location of the user, or the user himself. Neither will anonymity interfere with the use of an encryption system, because the keys of an asymmetric encryption system, which are used either to encrypt or for the exchange of keys for a symmetric system, can also be assigned to pseudonyms, rather than to identifiable users.

Having shown in this section that anonymity is necessary and technically feasible for verifiable data protection in open digital systems, the following sections will discuss how the desired legal certainty can be achieved without having to abandon anonymity, for example, during authentication.

3 Legal Certainty for Business Processes with Protection of Anonymity

In this section we investigate generally how business processes can be designed in order to achieve legal certainty without sacrificing anonymity. The current legal situation will, however, not be examined in detail (see [63, 29, 48, 64]).

We will proceed in the order in which a legally binding business transaction is conducted, including possible dispute handling. Much of the following also applies to non-anonymous business processes in open digital systems: There, too, one has to assume that at the onset, the business partners neither know each other personally nor can they identify themselves in the usual fashion. Thus anonymity (but not necessarily unobservability) is given at least at the beginning.

3.1 Declarations of Intent

3.1.1 Anonymous Submission and Receipt of Statement

The opportunity to submit and receive legally relevant statements (declarations of intent in German law) anonymously is already provided by an anonymous network.

If corresponding statements are to be issued and it is desirable that either all involved parties sign, or none (which is not the case for most transactions envisioned for open systems), this can be regarded as a complete business sequence for the exchange of signed statements and be dealt with in the same way as the exchange of goods for money, which is later described in more detail. If desired, special contract signing protocols [6, 38] can be used which permit a nearly simultaneous exchange of the statements, without requiring the services of a third party. Such contract signing protocols, however, incur a substantial communication overhead.

3.1.2 Authentication of Statements

Frequently, the person submitting a statement has to provide evidence of his right to make such a submission. *Digital signatures* are the main tool for doing this via a communication system [34, 2, 43, 12].

3.1.2.1 Digital Signatures. In legally binding transactions over open digital systems, so-called digital signatures are to replace hand-written signatures for providing assurance that a certain statement originates from a certain person (or group of persons), identified by a pseudonym.

The basic requirements for a digital signature are, therefore:

1. that no one apart from the owner of a pseudonym should be capable of attaching the signature which belongs to this pseudonym to a document, and
2. that anyone who wishes to do so can check if the signature which belongs to a certain pseudonym has been attached to a certain statement.

The first requirement solely refers to the intention of the user: Clearly, in a purely digital system it is impossible to hinder a user from permitting another user to act using his pseudonym. This is similar to the opportunity, which exists today, for a person to place any number of blank signatures at someone else's disposal. It can only result in damage to the user himself, due to the fact that signed statements produced in this fashion will be attributed to the owner of the pseudonym.

The simple approach of trusting the uniqueness of the pseudonym and attaching it to the statement like a customary signature does not, unfortunately, fulfil the requirements outlined above. Anyone who has received one signed statement from a user could copy the attached digital pseudonym to as many additional statements as he liked. Attaching a digitalised copy of a hand-written signature to authenticate statements, which is currently being discussed, must also be viewed as an inadequate approach. The digital version could easily be separated from the statement and copied, even if it had been written diagonally across the statement in the paper version. (The thoughts from [48] cannot be applied here because they combine facsimile signatures with special paper forms, as is done for bank notes, which cannot be sent in digital form. In addition, already with the current standard of copying technology, the printing on such forms is no more secure than a hand-written signature; at the most the structure of the paper, or something similar, may be.)

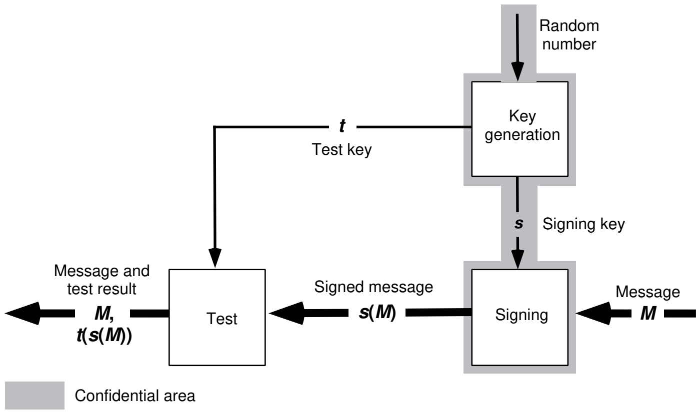

Figure 6: Signature System

For this reason, even in the non-anonymous case, one needs a digital pseudonym which differs from the name (a public personal pseudonym). This is one of the reasons for treating this case as a special case of anonymity.

A *digital signature* system (Fig. 6) solves the problem mentioned above. Such a system assigns each pseudonym a special function pair (s, t). The signing function s serves to sign a message and is only known to the owner of the pseudonym, whereas the test predicate t serves to verify that the message has been signed with s. The test predicate can be publicly known. In particular, the signature system can always be selected in such a way that the test predicate t and the message M can be derived from the signed message $s(M)$.

If the implementation of the signature system allows it, the test predicate t (i.e. its description) would be used as the pseudonym [20].

In practice, this description of the test predicate consists purely of a kind of key, just as in encryption systems. The key is used in an otherwise generally known test function, which needs to be standardised so that every signature can be tested with little effort.

Let us mention again (see 2.2) that for complexity reasons, the user must use a computer to test and, above all, to sign messages. As this computer contains the secret signing function, it is even more important now than in the case of anonymity that the computer is completely controlled by the user. This includes both identification of the legitimate user by the computer and that the communication between the user and his computer takes place without any intervention of devices which are not under the control of the user.

Currently, password mechanisms (PIN, personal identification number) are used to enable a computer to identify the legitimate user. In the future, the additional use of biometric data, e.g., the user's fingerprint, for identification is conceivable. This would scarcely make identification more reliable or more secure (apart from persons who cannot remember a PIN or who write it on the smartcard), because fingerprints can also be imitated. However, in normal use, it would prevent more than one person (e.g., a family) from using the same signature, which prevents a signed message from being attributed to a single individual.

If the access to an open system is also to take place outside the user's home, the computer needs to be portable and have its own keyboard and display, i.e. more like a small pocket calculator than today's smartcards.

A simple and well-known signature system can be obtained by using the asymmetric encryption system RSA (see 2.2.1.1):

Here the user's encryption function c, which may be publicly known, is used as the test predicate. Applying the decryption function d to a given message counts as signing. No one other than the owner of the pseudonym can sign, because, if he has created the key pair himself, he is the only person who knows d. RSA has the attractive characteristic that first applying the decryption function and then the encryption function to a message (i.e. the reverse of what is needed for message secrecy) yields the original message again. Thus anyone can test if a statement has been signed by the owner of a particular pseudonym by encrypting the "decrypted" statement with c and checking if this yields the correct statement. As the security of RSA has not been proven, the security of the signature system based on RSA is equally unproved.

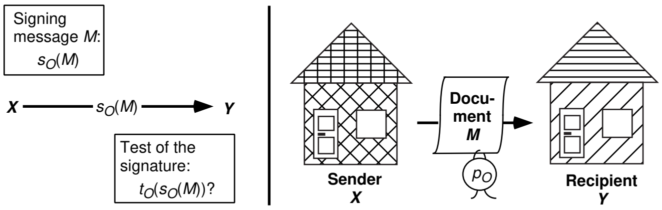

Figure 7: Transfer of a signed message from X to Y; functional notation left, graphical representation right.

An alternative to RSA which can be recommended is the GMR signature system [43]. This system, which is similarly efficient to RSA, has the advantage that it has been proven to be cryptographically secure against the strongest conceivable attacks (adaptive active attacks). Breaking it is equivalent to factoring a given number which has two large prime factors of a certain type. The GMR system is somewhat more complex than the RSA system.

Wherever possible, the GMR signature system should be used in preference to RSA.

Fig. 7 shows the transfer of a signed message from user X to user Y, where X is using the pseudonym p_O (for "originator"). The left half shows a functional notation, the right half a graphical representation, in which the message is illustrated as a document and the signature as a seal. This representation is used throughout the remainder of this paper.

For some applications it is useful to require additional characteristics from digital signature systems:

The receiver of a message which has, e.g., been signed using GMR, can show it to all other participants and convince them of the authenticity of the message. The signatory has no control over the passing on of his signature. This deficiency is compensated for by *undeniable signatures* (which are in fact signatures which cannot be shown to others) [18]. In order to convince other participants that a signature is genuine, the apparent signatory has to be questioned. He cannot deny signatures which have, in fact, been generated by him.

With a significant amount of effort, every signature system (just as every asymmetric encryption system) can be broken. In customary signature systems the signatory bears this risk. By using *fail-stop signatures* [82, 83, 58, 7, 10], this risk can be transferred to the recipient: If a signature has been forged, the apparent signatory can prove this to all other parties.

A further variant, *blind signatures,* which is actually needed in the following, will be described in 3.1.2.2.

So-called *digital identification systems* should not be confused with digital signature systems. Whereas the recipient of a signed message can prove the signature (and thus possibly the authenticity of a statement) to third parties, an identification system only allows the recipient to identify the sender as possessing a certain pseudonym at the point in time when the message was sent [86, 11, 40, 74].

For simplicity the sender will enclose a pseudonym (which has probably been specially created) with the statement, or encrypt the statement with the key of a symmetric encryption system which is only known to him and the recipient. Once the statement has been received, however, a third party can no longer check the authenticity of the statement (as already mentioned above). Hence for reasons of legal certainty, digital identification systems appear to be unsuitable for authenticating declarations of intent.

3.1.2.2 Forms of Authentication. Depending on where the authorisation for submitting the statement comes from, one can distinguish between *self-authentication* and *external authentication.*

Self-authentication takes place when the person submitting a statement refers to a statement which has already been submitted by him, e.g., the final order of goods after a binding offer has been requested.

In this situation the person sending the message wants to indicate that both messages originate from the same person. This represents a desired link between different messages; it can be achieved by the originator of the message using the same digital pseudonym for both messages and sealing them with the digital signature belonging to this pseudonym. In classical systems one would in any case have used the same name and the same signature for all transactions and, possibly, in order to facilitate the linking of the various statements related to one business process, may also have used an additional identification number.

External authentication takes place when the person submitting the message has received authorisation to submit from others.

In this case he needs a document, like a certificate or a declaration of credit worthiness, which states that the holder of a certain pseudonym is authorised to submit certain statements. He attaches this document to the statements. In addition, he has to sign the statement with the signature belonging to this pseudonym.

It is possible for the originator of a such a document to be in his turn authenticated by additional documents.

If further measures are not taken, this enables the authenticating third parties, e.g., banks if they have to provide a payment guarantee for each purchase, to derive unintended links in collaboration with the recipients of the message.

This can be prevented by the use of *convertible credentials* [22]. They allow the credentials required for the submission of a message to be issued under another pseudonym than the one used for the submission of the statement.

For this, the received credentials must be convertible into credentials referring to the currently used pseudonym. On one hand, no one should be able to establish the relation between the pseudonyms used without permission of the person issuing the statement. On the other hand, the person should only be able to convert the credentials received to his own pseudonyms and not to those of his friends.

A system for the conversion of credentials, based on RSA, was first proposed in 1985 [23, 27]. In this system, all possible credentials (e.g., those of a bank) have to be assigned to a certain RSA signing function. If a credential is to be issued for a pseudonym, this simply means that the pseudonym is signed with the signing function belonging to the credential. This means, of course, that the credentials which are possible have to be considerably generalised.

If it is sufficient for each credential to be converted once, the system allows the pseudonym to which the credential will be converted to be chosen such that it can be used for signatures [25]. If one wishes to use a credential more than once and, for this purpose, to convert it more than once, this is also possible. The pseudonyms to which the converted credentials refer are, however, then unsuitable for signing. As a result, the converted credentials may only be used in an identification system.

Whereas the anonymity of the system is perfect (in an information-theoretical sense), the security is, at best, as high as that of RSA.

The special signature system from [18] can be used in a similar way, bearing in mind that it has not been proven either.

A system for convertible credentials that is provably secure in the cryptographic sense, based on an arbitrary cryptographically secure signature system, was proposed in [30]. However, for efficiency reasons it cannot be used in practice.

If RSA were broken, but other secure asymmetric encryption and signature systems were still available, the following scheme, based on the anonymous network described in ([20], Page 86), could be used: Assume there are n users who each wish to receive the same credential on the pseudonyms $p_1, \ldots, p_n$. The organisation issuing this credential checks whether all users are entitled to receive the credential (i.e., if they already possess it on another pseudonym which has to be presented to the organisation). If yes, the organisation allows them to anonymously publish exactly one message each in random order, namely the corresponding pseudonym, on an anonymous network which is exclusively used for this purpose (logically constructed on the basis of an existing physical system). Thus the communication system guarantees that no one can ascertain who contributed which pseudonym. Now the organisation signs all the published pseudonyms.

Any signature system can be used here. The scheme conceals user X only with the level of security of the anonymous network used, and only among the n users who received the credential at the same time. In contrast, convertible credentials hide user X with information-theoretic security among all other users who received the same credential until the point in time where he uses it.

Another idea for preventing undesired linkability due to external authentication is based on the assumption that *tamper-resistant secure devices* exist. In such a device user authorisation can be entered and also deleted again, for example by communication with other secure devices. On request, the secure device can confirm an authorisation which has been entered by means of a digital signature, which can be checked throughout the system.

In contrast to the computers referred to so far (see 2.2, 3.1.2.1) this device has to provide a function based on secret data, e.g., the keys of a cryptographic system, which must also remain hidden from its user. Otherwise, the user could alter the credentials in the device, or construct a similar device which would appear correct to other users and secure devices, but would contain more credentials or different ones.

However, it must still be possible for the user who "operates" it to control the functions of the device. Hence the device should be in the physical possession of the user, as explained in 2.2. This is also typically assumed in the literature [65, 24, 32, 66].

The existence of devices which simultaneously fulfil both of these requirements is highly questionable. The user can manipulate and observe the device in any number of ways, in particular while it is in operation. Even extremely expensive or time-consuming measures could be worthwhile due to the fact that the successful corruption of a device would enable the production of a large number of copies. Each time information is processed within the device, energy is transported. To prevent this transportation of energy from being measured (e.g., via electromagnetic emissions), the device has to be sufficiently well shielded. As a user can also attempt to investigate his device by means of destructive measurement, a secure device must also recognise if its protection mechanism is being attacked from outside. In such a case (and also if its functionality is affected by an internal error), the secure device has to immediately render itself unusable, i.e. delete its secret information.

This establishes a race between the constructors of secure devices and those of measuring technology, which it is unlikely either will win in the long run.

Nonetheless, in practice, smartcards are currently being used as secure devices. Possible applications for these are as an authorisation for use, e.g., of data bases or public telephone booths (in this case the authorisation is initially restricted to n number of uses and is decremented by each use). They are also being proposed for use in digital payment systems (see Section 5.5).

In our opinion devices which have to be secure against their user should be used as rarely as possible.

3.2 Other Actions

To make it worthwhile to submit and receive statements in a business transaction anonymously, the other actions needed in the transaction must also provide anonymity.

If such an action also consists of sending information over the communication system, e.g., the delivery of information from a data base as a good, the anonymity is already ensured by the underlying anonymous network.

In an open system it should also be possible to transfer money digitally; possibly in the form of a sequence of declarations of intent (see Section 5).

This already concludes the list of the most important actions required to conduct legal transactions over open networks.

If a part of the transaction is not conducted by means of the communication system, the unobservability cannot be preserved entirely, and sometimes this is not even desired. In the following we therefore restrict ourselves to declarations and actions conducted by means of the communication system.

3.3 Guaranteeing Evidence

Building on the possibilities for authentication described in 3.1, we must now investigate ways to guarantee enough evidence to prove the submission and the receipt of a declaration of intent.

Just as in 3.1, in comparison to the non-anonymous case no essentially new problems arise.

This investigation can be organised according to two criteria:

On the one hand the goal of providing evidence can be considered. This goal can be to prove the submission or the receipt of a statement, but it can also be the opposite, i.e. to prove that a statement has not been sent or received.

The second goal, however, is achieved simply by comprehensively achieving the first. A statement for which no verifiable evidence of submission or receipt can be produced can then be considered as not sent or received. For this reason, the second goal will not be explicitly pursued in the following.

On the other hand one can consider which party is interested in providing the proof, the sender or the recipient.

Frequently, the fact that a statement has been submitted is advantageous to only one of the two parties. Hence only this party is interested in obtaining proof and is the only one who has to collect evidence.

For the recipient of a statement this proof is simple if the statement has the character of a document, i.e. carries a digital signature. In this case, presentation of the statement provides sufficient evidence that the possessor of the digital pseudonym which belongs to the signature has submitted this statement.

In many cases, it is not necessary that the sender of a statement has to collect evidence that he has submitted the statement, or even that it arrived at the recipient, even if this fact is advantageous to him.

If the exact time of the submission is unimportant, it is sufficient for the statement to be repeated the moment its transmission is doubted, if necessary in court. This is the case for the type of everyday transactions which are to be conducted over open networks. Equally, it is not necessary for the sender to gather evidence that he delivered information serving as a good or the messages belonging to a transfer of digital money: in contrast to the distributor of material goods or paper documents, the sender can save the information. The recipient clearly does not gain any benefit from a double delivery. The second delivery simply represents a copy of the first and the recipient could just as easily have created such a copy himself.

If it is nevertheless necessary to prove the receipt, the possibilities are similar to those for non-anonymous statements.

One possibility is to require a signed receipt. It is easy to prove that this receipt has been received (see above). If the person who sent the information does not receive the expected receipt within a prescribed period of time it must be possible, in an emergency, to obtain it by means of legal pressure, or for a court to provide a substitute. For these disputed statements, one also needs the following alternative.

This second possibility is to set up so-called bulletin boards in the open system. These would have to be checked at regular intervals by the potential recipients of statements that require proof of delivery. As a computer could take over this task of checking the bulletin boards, it can be assumed that this method would be no more time consuming than the daily emptying of the mailbox.

The fact that a statement for a user who uses the pseudonym p_E was displayed on a bulletin board can then be substantiated by witnesses. In order to ensure that the witnesses do not discover the contents of the statement, the statement has to be encrypted with a key known to the recipient of the statement. If one assumes that the pseudonym p_E of the recipient is linked in a verifiable way to a key c_E in an asymmetric encryption system (e.g., by means of a public-key directory, or by using c_E itself as a pseudonym) the sender can prove that the message was received by the person using the pseudonym p_E by presenting the pseudonym p_E and the decrypted message. It is most convenient to use a public facility, such as the PTT, as a witness. It should regularly, e.g., daily, publish and sign a list of all the submitted encrypted messages. This ensures that the witness is accountable and that the recipient does not lose anonymity.

3.4 Investigation Procedures

Should a situation arise in which one of the involved parties questions the legitimacy of the current state, the basis of this doubt has to be investigated. The user who instigates this procedure does not have to reveal his identity. Instead, it is sufficient initially to establish if the person who owns a particular pseudonym has, in fact, been deceived.

Deanonymizing all the anonymous parties who might be involved in advance should certainly be avoided (this could result in misuse). Hence one must be take into account that it is not possible to force all parties to take part in the investigation. For this reason, all necessary evidence must be in the possession of those users whose participation in the investigation is ensured. This includes the party who instigated the procedure and all non-anonymous participants, e.g., notaries, but also anonymous participants if they might incur damages by not taking part. For example, an anonymous data base which is accused of having accepted money, but having failed to deliver satisfactory information, could be forced to reveal the answer it sent, if, otherwise, it would be assumed that it had sent nothing at all, with the result that it would be convicted. (For assurance that this is actually a threat see 3.5. Also note that it is possible in an anonymous network to issue this summons to the data base securely under its pseudonym.)

3.5 Regulation of Damages

If a violation occurs, it must be rectified in the same way that a legal condition which has been violated is compulsorily re-established today.

In general, this is achieved by intervention in the financial resources of a user. Hence he should have sufficient financial reserves for this purpose, the relationship between the claims being made and these financial reserves should be clear, and access to this money, or the special portion of it to which the claims are related, should be possible.

Whether or not it is possible from the onset to ensure that the user possesses sufficient financial reserves is not dependent on the anonymity, but rather on fundamental considerations regarding the legal transaction in question and is not always guaranteed today either.

The fulfillment of the remaining requirements is the main difference between anonymous and non-anonymous systems:

If anonymity is not desired, the relationship can be established using names (and additional information which provides clear identification). This means that management of financial resources and the collection of evidence can be organised completely independently. All financial resources are in the possession of named persons and all evidence is linked to persons also known by name.

If anonymity is to be provided this independence is lost. This does not mean that there is no longer an opportunity for regulating damages, but rather, that the transaction processes become more complicated. At the very point where the evidence is secured, attention has to be paid to the relationship to the financial resources which may need to be accessed.

For this reason the investigation of the components of a transaction process made in this chapter 3 do not automatically result in finished protocols for the entire transaction process, but only in building blocks, which still have to be skillfully combined.

Which individual regulations are required depends, above all, on who is to be bound by the legal transaction, to whom, and for how long.

If the request for the regulation of damages arises as a result of, for example, a large credit, a prerequisite for the guarantee that financial resources be accessible is always the prior transfer of securities in the form of material goods, e.g., a piece of land. By using the credential mechanism (see 3.1.2) this can also be carried out anonymously: A land registry office provides a credential confirming the value of a piece of land and makes a record that the piece of land has been used as a financial guarantee. Transactions of this dimension are, however, untypical for open systems.

Low-value transactions for the purchase of goods, in particular of information, will probably be much more typical. Here a person binds himself to pay a certain small sum of money within a short time after the delivery of the good. Due to its importance for open digital systems, and in order to illustrate an example of a complete transaction process, the purchase of a good for a small sum will be presented in a separate section (Section 4).

With two exceptions, the provision of a service, e.g., managing an electronic mailbox, can be treated like a sequence of many small purchase transactions. The management of a mailbox could, for example, always be cashed up when the user wanted to empty the mailbox. Transfer of the contents corresponds to the delivery of a good.

The two exceptions are those services which must be used in order to carry out a transaction at all over an open network, i.e. the transport of information through the anonymous network and the supply and management of money by means of an anonymous digital payment system.

The communication system can either be paid for in a lump sum, or by enclosing money (digital "postage stamps") with each message [56]. In the first instance, non-paying users of a communication system can be excluded, in the second instance, messages which have not been paid for will not be transported further.

As the supplier of the communication system is not anonymous (in general the PTT), intentional damages caused to a user by the communication system would have to be settled outside the system, in court, as is the case today.

The services of the anonymous digital payment system could be managed in the same way. The banks themselves could collect the required fees directly and, if necessary, the customers could take proceedings against the banks (the latter could be done anonymously via the communication system).

4 Fair Exchange of Values

From the standpoint of legal certainty, classical cash purchases in shops could be implemented with full anonymity because the proximity of the business partners ensures that either both the goods and the money are exchanged, or neither. In this case (leaving aside retrospective complaints), a claim for damages is never necessary.

One cannot assume that there will be a similarly simultaneous exchange of goods and money over a communication system. Certain business partners will always temporarily have an advantage. Hence, if they break off the communication at an appropriate point in time, claims on them may still exist which must be enforced.

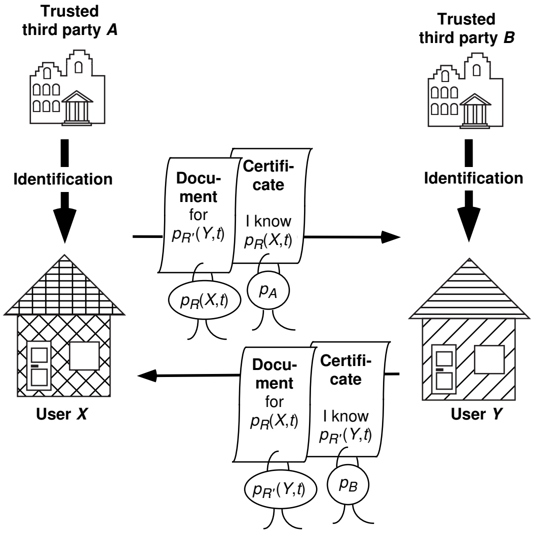

Figure 8:

The following two sections describe two concepts for ensuring the enforceability of claims. We prefer the second.

4.1 Third Parties Guarantee that Identity can be Revealed

The first concept guarantees that the identity of the debtor can be revealed if he or she wish to dispute the assignment of damages. Then, just as in the non-anonymous case, the entire assets of the debtor are available.

Technically this deanonymization is made possible by the parties to the transaction showing a special form of external authentication: Each of them provides proof of identity to a non-anonymous third party, who seems trustworthy to all. This third party issues a certificate to the person, or his business partner, that he can identify the owner of a particular pseudonym if necessary (non-public person pseudonym, see 2.2.2).

One third party [44] or a chain of third parties [20] can be used to provide this authentication. The principle is illustrated in Fig. 8 for one third party (but possibly different third parties for different users). Let X and Y be the users and A and B the non-anonymous authorities who can identify X and Y, respectively, and let

- $p_R(X,t)$ be the pseudonym which X wishes to use in a business transaction t with Y,
- $p_{R'}(Y,t)$ the pseudonym which Y wishes to use in this business transaction (but in another role than X),
- p_A and p_B the public person pseudonyms of A and B, respectively.

The fact that A can verify the identity of X is guaranteed by requiring X to have his pseudonym $p_R(X,t)$ signed by A before he can use it. In the same way Y has his pseudonym $p_{R'}(Y,t)$ signed by B. In order to ensure that when A reveals the identity of a previously anonymous person it is always the correct person, X has to sign a statement "the pseudonym $p_R(X,t)$ belongs to X" with his usual hand-written signature or, more securely, with a digital signature belonging to a public person pseudonym, and give this to A before he receives his certificate from A. If the third party is trusted not only in respect of anonymity, but also legal certainty, the use of an identification system (see 3.1.2.1) will be sufficient here, e.g., it would be possible to identify X by his fingerprint. The same process applies to B.

If X and Y present their signed pseudonyms, that is pseudonyms which have been verified by A and B, before they carry out a legal transaction with each other, both know that should fraud occur, X can be identified by A, and Y by B.

In the course of the business process, it might arise that X complains to B that his business partner has broken off a communication relationship, although he should have completed it. For this, X attaches messages from Y which have been signed with $p_{R'}(Y,t)$ and prove to B that a communication relationship existed. B asks Y to continue, and from this point on, all messages from Y to X must be sent via B. If Y refuses, his identity is revealed by B and an investigation is conducted according to the customary procedures for the non-anonymous case.

If X accuses the other falsely, by withholding the remainder of the statements in the sequence, the worst which can happen is that Y has to resend the remainder of the information. As it will be sent via B this time, X can no longer pretend that he has not received all of the statements.

The same applies if Y complains to A.

The advantages (+) and disadvantages (–) of this solution are:

– Who should ensure that A and B do not reveal the identity of X or Y unless they are entitled to do so? In respect of data protection, therefore, A and B have to be absolutely trustworthy, whereas in respect of security against fraud, this is not necessary because they cannot falsify the assignment of persons to pseudonyms.

– X or Y may cause damages which remain unsettled. For example, X could order a service from Y and also receive it, although he does not possess the necessary funds to pay for it. Revealing the identity of X will not result in payment of the damages incurred by Y.

– For efficiency, one would typically use person pseudonyms for $p_R(X,t)$ and $p_{R'}(Y,t)$, which can lead to a gradual loss of anonymity as described in 2.2.2.

+ If person pseudonyms are used, A and B need not intervene in the individual transactions of X or Y.

A way to divide the ability to deanonymize among a number of third parties is described in ([20] Page 86). With the procedure described there, the owner of the pseudonym which has been given to the partner can only be identified through co-operation of all third parties. Extensions of this scheme, in order to tolerate the loss of function of some authorities, are described in [57].

Although the anonymity is increased by using several third parties, deanonymization still has the disadvantage that it does not guarantee that sufficient capital is available.

4.2 Trustee Ensures Fairness for the Anonymous Partners

In order to ensure that no unrecoverable damages can occur there is a very simple procedure, which furthermore works without deanonymization: The money is deposited with a non-anonymous trustee so that claims can only arise with respect to the trustee [56, pages 29–33] [78, 79]. The actual business partners can then remain completely anonymous to each other, as well as to the trustee. Because the trustee is not anonymous, proceedings can be taken against him in the customary manner if he abuses the trust placed in him, without the actual business partners having to give up their full anonymity.

Rather than exchanging money and goods directly with each other, all the involved parties give the trustee information regarding the amount of money or the nature of the goods (information) which they wish to receive, and then the money and the goods. The exchange must take place in precisely this order, because if the trustee receives the goods, but not the money, he cannot compensate the supplier for his damages. The trustee checks if what he has received fulfils the expectations of the partners. Depending on the result of this check, he either passes on what he has received, or aborts the transaction.

In order to complete transactions quickly, this trustee must be part of the open digital system. It could be the PTT, which currently undertakes similar tasks for certain transactions carried out using teletex.

Returning to the users X and Y, where X is the customer and Y the supplier of a good (in the form of information), this idea can be put into concrete terms as shown in Fig. 9. In the figure, the numbers of the documents indicate the order of the appropriate statements. The following notation is used:

- $p_C(X,t)$ is X's pseudonym as customer in transaction t,
- $p_S(Y,t)$ is Y's pseudonym as the supplier in transaction t, and
- p_T is the public person pseudonym of the non-anonymous trustee.

The illustration of the money transfer is greatly simplified because money can, of course, not simply be represented as a single message or statement—otherwise, it could be duplicated by copying (see Section 5).

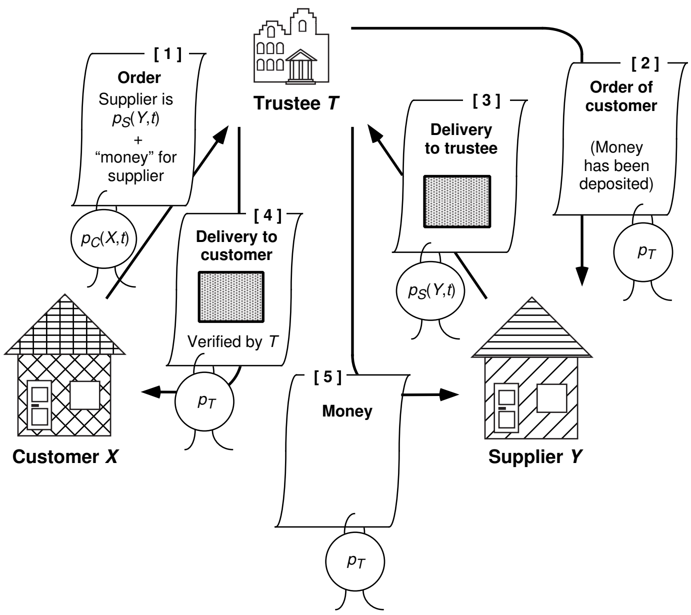

Figure 9:

As explained in Section 3.3, it is not necessary in any of the actions, i.e., the deposit and transfer or refund of payment, and the deposit and transfer of the goods, that the person who acts collects evidence of the action. Receipt of the order (first by the trustee and then by the service provider) can simply be proved by presenting the document.

For the purposes of data protection this concept should be given preference, but it has one disadvantage. It requires that the trustee make certain checks regarding the goods. He is not always capable of doing this or, for reasons of data protection, should not be able to do it.

To reduce the impact of this disadvantage, X and Y can agree on a reclamation period during which the trustee T withholds the money he has received, but not the goods. In this way, the trustee only has to ensure the "genuineness" of the money he has received, but need not check the goods, and therefore need not receive any information about them.

During the reclamation period, if customer X is not satisfied with the goods, because, for instance, an inquiry has been incorrectly answered, he can instruct the trustee not to transfer the money and is then compelled to prove that the goods were indeed defective.

If one can ensure that the court, which may need to be consulted, will work quickly enough, it will not be possible for X to cause any large damages to Y by a reclamation, for instance, a loss of interest on the money.

If X and Y wish to conduct a transaction of "goods against goods," they have to divide it into two transactions of "goods for money," in order to maintain the sequence "money before goods" for each exchange.

The trustee solution with these extensions can be evaluated as follows:

− The trustee always has to be actively involved in the transaction.

+ It is not necessary for any party directly involved in the transaction to trust the trustee, because both parties involved in the transaction monitor the trustee and can take legal action against any mistakes or attempted fraud. The existence of sufficient evidence is ensured and enforcement of a claim against a trustee can be ensured just as in a non-anonymous case.

+ All claims made by X on Y, or Y on X can be satisfied by recourse to the values which have been deposited with T.

+ Those directly involved in the transaction can use transaction pseudonyms without any additional effort.

+ The anonymity of those directly involved in the transaction is fully ensured.

If the service provider, a newspaper publisher for instance, does not wish to be anonymous, he could, of course, also serve as the trustee. In this case the form of the transaction would resemble one where the purchaser pays at the same time he orders and, if the service provider cannot or will not deliver, he has to return the money.

All the concepts introduced here have left one open problem: how money can be represented and transferred anonymously in a digital system. This will be treated in the following section.

5 Anonymous Digital Payment Systems

A payment system should serve its users by securely transferring money.

In terms independent from a concrete payment system, money is nothing more than a collection of rights which is defined in a purely quantitative terms. In order to consider the security and anonymity of payment systems, it is therefore not necessary to define what exactly is the money in them, or where exactly it is located. Therefore, in the following only rights will be referred to.

In particular, it is of no importance for the security within a payment system whether these rights are based on a positive balance or a limited credit, although, of course, a credit must be sufficiently covered outside the payment system.

A payment system is secure if:

- a user can transfer the rights which he received,
- he only loses a right if he intends to surrender it,
- in the case that a user unambiguously designates another as the recipient of a payment, only this recipient can obtain the right,
- if necessary, the user can prove to a third party that a transfer has been made (receipt problem) and
- even if they co-operate, the users cannot increase their rights (i.e., money).

If one does not (only) rely on the good intentions of the users, when a right is used in the form of a transfer, that right must be proved. As only payment systems in which the entire transfer is carried out by exchanging digital messages (in general via a communication system) are considered here, and as digital messages can be copied as often as one likes, but the rights must cease to exist once the transfer has been completed, proof by a document alone is not sufficient. Hence a witness who can guarantee the current validity of the right is required.

For the witness to be able to fulfil this task he must be aware of every use which is made of a right which he is supposed to witness. As a result, even if the recipient of a payment trusts the payer, it cannot be possible for the right to be transferred without confirmation by the witness.

In Sections 5.1 to 5.4 it is assumed that the users do not wish to place full trust in these witnesses in respect of data protection or security.

If full trust is placed in the witness, for instance because the witness is a secure device in the form of an electronic wallet, the problems are simplified considerably. This will be discussed in more detail in 5.5.

A payment system which is not secure in the sense described above, but functions completely without active witnesses is described in Section 5.6.

5.1 Basic Scheme for Secure and Anonymous Digital Payments

In the following, we discuss how a secure and anonymous digital payment system with witnesses can be implemented.

For this purpose it is assumed that user X wishes to transfer a right to another user Y of the payment system, and a witness B (for bank) confirms this transfer. For simplicity, it is assumed that there is only one witness. This sole witness should be liable for false confirmations, i.e. if new rights to money occur as a result of his falsely witnessing a transaction, he must make this money available. If he refuses to confirm existing rights, the person affected by this can prove this to an objective third party (e.g., a court). This is achieved by choosing a non-anonymous witness with sufficient financial resources. To a certain extent, the witness assumes the role of a bank in customary cashless payment systems.

One can assume that the payer X and the recipient Y already know each other by certain pseudonyms (see 2.2.2). These pseudonyms are pre-determined outside the payment system and are assumed to be sensitive, i.e., must be protected (typically role pseudonyms, e.g., a customer number and the name of a service provider). Equally pre-determined is the pseudonym of the witness, which, however, must not be anonymous (public person pseudonym). In addition, within the payment system it is pre-determined by prior payments under which pseudonym X can identify himself to the witness B as the possessor of the rights he wishes to transfer. Therefore let

- $p_P(X,t)$ be the pseudonym under which the payer X in the transfer t is known to the recipient;
- $p_R(Y,t)$ be the pseudonym under which the recipient Y in the transfer t is known to the payer;
- p_B be the pseudonym used for many payments by the witness B;
- $p_P^B(X,t)$ be the pseudonym under which the payer X in the transfer t is known to the witness B.

Under these assumptions, one obtains the following protocol for the transfer t of the right from X to Y, analogous to today's money transfers:

[1] *Choice of pseudonym.* Y selects a pseudonym $p_R^B(Y,t)$ by which he wishes to be known to the witness B as the recipient of the right in the transfer t, and he informs X that he wishes to receive the right under this pseudonym. Correspondingly, X informs Y of the pseudonym $p_P^B(X,t)$ under which he wishes to transfer the right. The necessary statements are authenticated with $p_R(Y,t)$ and $p_P(X,t)$, respectively.

[2] *Payer's transfer order.* X gives the witness B an order to transfer the right to $p_R^B(Y,t)$. This order is signed with $p_P^B(X,t)$. As external authentication X attaches a certificate which says that $p_P^B(X,t)$ is entitled to the right which is to be transferred; this is signed by B himself with p_B. As every transfer has to be confirmed by B, it is possible for B to check whether $p_P^B(X,t)$ still has the certified right or has already transferred it.

[3] *Certificate by the witness.* The witness B confirms to X and Y the transfer of the right from $p_P^B(X,t)$ to $p_R^B(Y,t)$; he addresses them under these pseudonyms.

[4] *Receipt for the payer.* The recipient Y sends X a receipt which only indicates $p_P^B(X,t)$ and $p_R(Y,t)$ and is authenticated with $p_R(Y,t)$, and which confirms the receipt of the right.

If Y refuses to issue the receipt (which, in general, cannot be prevented because Y is anonymous), X can use the certificate of the transfer by B (from [3]) together with the confirmation from Y that he wished to receive the right under this new pseudonym $p_R^B(Y,t)$ (from [1]) as a substitute receipt.

It is exactly this opportunity which distinguishes the receipt problem from the general value exchange problem where it is not possible for a third party, for instance a trustee, to produce a substitute of either of the exchange objects.

[5] *Certificate for the recipient.* The payer X sends Y a confirmation of the transfer which only indicates $p_P(X,t)$ and $p_R(Y,t)$ and is authenticated with $p_P(X,t)$.

If necessary, Y can also use the certificate by B (from [3]) together with the confirmation from X (from [1]) that he wanted to transfer the right to Y as proof that he has received the right from $p_P(X,t)$.

[6] *Converting the certificate.* Y will want to use the certificate from B produced for $p_R^B(Y,t)$ that he has received the right in Step [2] of a future transfer t'. In order to prevent linkability and a resulting loss of anonymity, $p_R^B(Y,t)$ should not be used as $p_P^B(Y,t')$ there.

By using the convertible credentials referred to in 3.1.2.2 it is possible for Y to convert the certificate to a new pseudonym. For this purpose, however, in Step [1] of the transfer Y must already have chosen the future pseudonym $p_P^B(Y,t')$ and from this formed a $p_R^B(Y,t)$ suitable for conversion.

The protocol is illustrated in Fig. 10, in which the authentication is once again illustrated by a seal.

As the certificate from [6] that a right has been received is used in a future transfer to transfer the same right, i.e. the same sum of money, it is appropriate in this payment system that there is a fixed

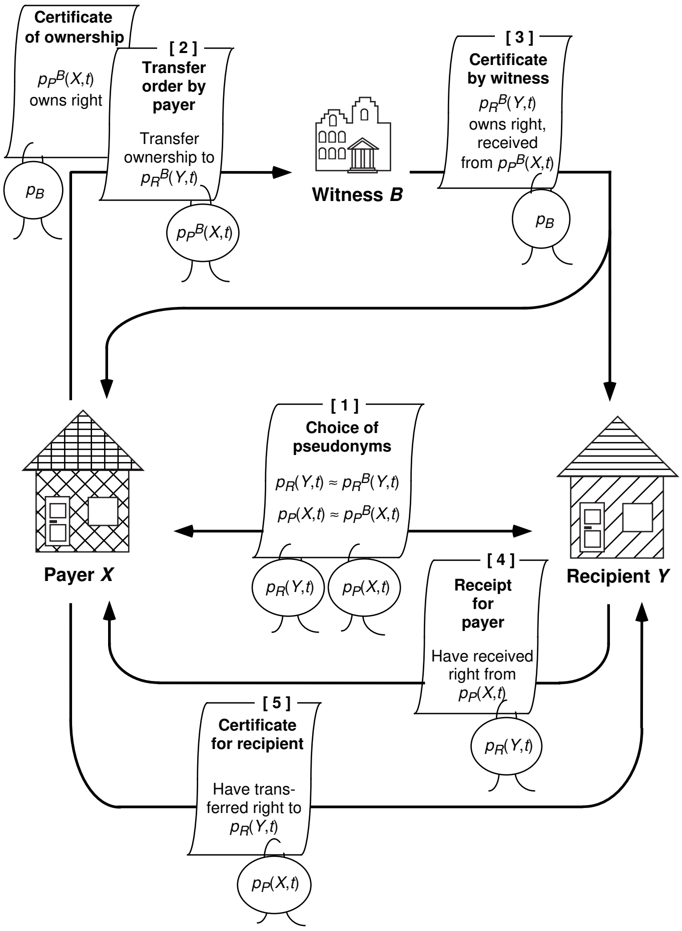
Certificate of ownership
$p_P{}^B(X,t)$ owns right
p_B
[2] Transfer order by payer
Transfer ownership to $p_R{}^B(Y,t)$
$p_P{}^B(X,t)$
Witness *B*
[3] Certificate by witness
$p_R{}^B(Y,t)$ owns right, received from $p_P{}^B(X,t)$
p_B
[1] Choice of pseudonyms
$p_R(Y,t) \approx p_R{}^B(Y,t)$
$p_P(X,t) \approx p_P{}^B(X,t)$
$p_R(Y,t)$
$p_P(X,t)$
Payer *X*
Recipient *Y*
[4] Receipt for payer
Have received right from $p_P(X,t)$
$p_R(Y,t)$
[5] Certificate for recipient
Have transferred right to $p_R(Y,t)$
$p_P(X,t)$

Figure 10:

set of nominal face values for rights, just as with physical cash. For every payment, one composes the desired amount from several such rights. Of course, it must also be possible to get change at B.

To enable the nominal face value of the converted certificate to be seen when it is used in [2], B uses a different digital signature for each value N used, i.e. a separate pseudonym $p_{B,N}$.

The security of the protocol arises from the fact that at the end of a transfer each of the three involved parties has enough documents regarding the fact that the transfer took place (which they have to keep). During the transfer each party can always either prove to an objective third party the current state of the transfer, or can reproduce it in a verifiable manner by presenting the messages received from others and resending his own messages if their receipt is disputed.

In addition, claims within a transfer which have to be settled can only arise with respect to the witness, who is not anonymous.

If X and Y both comply with the protocol the anonymity of the protocol is maximal because no one obtains any new information about anyone else through the transfer: In a payment, the witness does not obtain either of the pseudonyms which X and Y use elsewhere, but only two new pseudonyms which are never used outside this payment. X and Y do learn from each other the pseudonyms which they use with the witness for this payment, but these do not represent any new information because they cannot be linked to anything and it was in any case clear that some pseudonym would be used with the witness.

To say that the anonymity of the protocol is maximal does not, however, imply that strong anonymity is achieved in every situation. There are other ways of gaining information.

For one, in addition to the specifically selected pseudonym, there are other forms of indications about the users which the partners have to learn, independently from the chosen protocol. In this case, these are the amount and time of the payment. In particular, the payer is only concealed among all those who at this time could have a right for this amount. This is an additional reason for using only a small set of nominal face values.

A second point is that the payment system obviously does not provide any additional anonymity for pseudonyms which are also used in other situations. Should, for example, X have to prove the transfer, the pseudonyms $p_P(X,t)$ and $p_R(Y,t)$ are linked to each other; this is precisely the goal of the proof.

The users can, therefore, fully determine for themselves how much of the anonymity which has been enabled for them they wish to give up by using some pseudonyms repeatedly, or by linking them through statements.

If Y refuses to provide a receipt in [4], then X uses the certificate by the witness from [3] and the confirmation by Y from [1] as a substitute receipt. If this substitute receipt is presented to a third party (not Y), the witness may find out the relationship of $p_P^B(X,t)$ to $p_P(X,t)$ and of $p_R^B(Y,t)$ to $p_R(Y,t)$. Hence, if refusal occurs the anonymity is slightly reduced.

In the situation where X and Y trust each other and do not require a receipt, it is possible to forego witness B's certificate for X that the transfer has been completed. The confirmation from Y in [1], however, is still required because X can only learn the pseudonym $p_R^B(Y,t)$ from Y by means of this confirmation and, for X to be certain that he is transferring his right to the correct party, it must be authenticated by Y with $p_R(Y,t)$. In addition, in this case, either X has to provide binding information what payment will be made in [1], or at the end they must inform each other that the payment was ok. Otherwise it would not be noticed if an error occurred in the transfer, either in the transmission or through B.

5.2 Restricting Anonymity by Means of Prearranged Accounts

It is conceivable that a payment system which is as fully anonymous as that described in 5.1 is not desired because, unless additional precautions are taken, nobody (in particular, not even the tax office) would be able to make statements about the possessions or income of the users. However, this applies equally to customary cash, and even in the currently available cashless payment systems the available information regarding persons who have accounts with several banks is, at least officially, seldom linked.

For these reasons each user could be allowed to use only one account (or a known number of accounts) which must be used for all payments. This can be enforced by non-anonymity of the accounts, or by convertible certificates for the setting up of anonymous accounts. By adapting the protocol from 5.1, it is possible to construct a secure payment system which is as anonymous as possible under this precondition.

The prerequisite can be expressed by saying that $p_P^B(X,t)$ or $p_R^B(Y,t)$ is now the same for all payments made by the user X or Y, respectively, i.e. it is independent of t. The protocol from 5.1 is then no longer fully anonymous because in Step [1], X and Y would unnecessarily tell each other the account numbers $p^B_P(X,t)$ and $p^B_R(Y,t)$, which identify them, and B would see between which two of the fixed accounts a transfer takes place.

The solution is to use anonymous intermediate pseudonyms which change for each transfer. X first withdraws the money from his account and transfers it to his intermediate pseudonym. He then pays Y using Y's intermediate pseudonym. Finally, Y deposits the money in his account. The individual transfers take place according to the protocol from 5.1. In particular, the certificates which prove that a right has been received are converted to other pseudonyms between the partial transfers. Thus, in fact, the payer and the recipient each have two related intermediate pseudonyms. Let

- $p_{acc}(X)$ be the fixed pseudonym which belongs to the account of person X;
- $p_{with}(X,t)$ the pseudonym which the payer X uses to withdraw his money in the transfer t;
- $p_{intP}(X,t)$ describes the intermediate pseudonym which the payer X uses in the transfer t, i.e. the one he uses to pay Y;
- $p_{intR}(Y,t)$ the intermediate pseudonym of the recipient in the transfer t, i.e. the one which he uses to receive the right from X;
- $p_{dep}(Y,t)$ describes the pseudonym of the recipient Y in the transfer t which he uses to deposit the money.

Among these pseudonyms, first X chooses $p_{intP}(X,t)$ and calculates a suitable $p_{with}(X,t)$. In the first partial transfer, he has the right transferred from $p_{acc}(X)$ to $p_{with}(X,t)$, and then converts the certificate to $p_{intP}(X,t)$. In this partial transfer, the steps [1], [4] and [5] of the protocol can be omitted because X does not need to tell himself his own pseudonym and does not require a receipt for the transfer. Enclosing the certificate in [2] can also be omitted because B knows the balance of the account; the certificate is only needed if a dispute arises.

Now Y has to choose $p_{dep}(Y,t)$ and calculate an appropriate $p_{intR}(Y,t)$. Subsequently, the right is transferred from $p_{intP}(X,t)$ to $p_{intR}(Y,t)$ according to the complete protocol from 5.1; this included the creation of receipts.

After Y has converted the certificate regarding the receipt of the right to $p_{dep}(Y,t)$, he transfers it to $p_{acc}(Y)$, once again omitting Steps [1], [4] and [5] and here also Step [6].

The documents which the witness B issues to certify receipt of payment in the first and the second partial transfer, respectively, must not look the same. Otherwise Y could use the certificate from the second partial transfer directly for a new payment, thus bypassing the account. In the context of convertible credentials, this means that B uses two different digital signatures, i.e., two pseudonyms, for withdrawals and transfers. He can distinguish the cases by seeing whether the payer's pseudonym told to him belongs to an account or not.

In order to force Y to transfer his right to $p_{acc}(Y)$ within a foreseeable amount of time, (which, for example, would be a prerequisite for annual taxation), a certificate received from B about a transfer must not be valid for deposit for an undetermined amount of time. At the end of a certain period, B should change the signature key used for authentication. After a further period, which gives all payment recipients time to transfer the rights they have received to account pseudonyms, certificates authenticated with the old signature key should no longer be accepted.

The security of this payment system follows from the security of the payment system from 5.1 because it is only a special application of that system.

Given the condition that fixed accounts exist, the anonymity is maximal because the sensitive pseudonyms, $p_{acc}(X), p_{acc}(Y), p_P(X,t)$ and $p_R(Y,t)$ are kept fully separated by means of the intermediate pseudonyms and the conversion of the credential. More precisely: neither does Y learn $p_{acc}(X)$, nor does X learn $p_{acc}(Y)$, nor does B learn $p_P(X,t)$ or $p_R(Y,t)$, and as the result of a payment everybody can only link previously known pseudonyms of the others to newly selected pseudonyms which will never be used again. Thus, these provide no information.

Apart from this the same comments made in respect of anonymity and receipts made at the end of 5.1 apply. It should be noted that the amount of a payment and the time it was made can allow more significant links than in 5.1, i.e. recognition of the relationship between the two accounts involved in a payment. In order to prevent this a randomly selected period of time should elapse between the individual partial transfers, and the entire amount required for a payment should not be withdrawn or deposited in one piece.

5.3 Proposals Known from the Literature

The fully anonymous and secure payment systems described in 5.1 and 5.2 were developed by combining elements of previously proposed anonymous digital payment systems. These can, however, be described most simply and systematically as weaker versions of the systems above and, for this reason, they are only addressed now.

The idea of using convertible credentials in payment systems is by David Chaum, the inventor of the mechanism used for these credentials, although he gives them a different name in this context. He based a series of related anonymous payment systems on this principle [21, 23, 25].

Common to all of Chaum's proposals is that they assume the presence of fixed non-anonymous accounts. No receipts are given, but rather there are variants similar to that described in 4.1: They enable deanonymization of the payer or recipient through co-operation of the partner and the witness.

The most significant difference between Chaum's payment systems and the system described in 5.2 is that, apart from one variant ([25] Sect. 4.2.1), they do not make use of the fact that interim pseudonyms can be selected in such a way that a digital signature for them exists. This makes it more difficult to guarantee user security, in particular in respect of witness B, because the possessor of a right can no longer unambiguously state where a transfer should be sent as he can if the transfer is authenticated by his signature. In the simplest versions this security is either not achieved at all, or only achieved by reducing anonymity. In a further version ([25] Sect. 4.2.2), at least security in respect of witness B is achieved as follows: Before the certificate of ownership is presented to him, B has to give the intended recipient of the payment a signature assuring him that the right will be credited to no one but him. For this, the payer hands over the certificate to the recipient. Of course, the validity of B's signature has to be limited. Otherwise, B could refuse to transfer a right indefinitely, arguing that he had given assurance to another party that he would credit him with it, but this party had not yet presented evidence that he possessed the right.

Omitting named accounts in digital payment systems first arose in the payment system "anonymous numbered accounts" [56, 79]. Apart from this difference, the system simulates exactly the customary money transfers with digital signatures. The anonymity of the accounts is, strictly speaking, not a characteristic of the payment system; it only concerns the linkability of the pseudonyms used in the payment system to the outside world, and has nothing to do with the security of the system (as long as overdrawing the account is not allowed). Generally, any digital payment system which is strictly secure with named accounts would also be secure with anonymous numbered accounts.

The use of transaction pseudonyms with the bank (i.e., $p_P^B(X,t)$ and $p_R^B(Y,t)$ in the protocol described above) was proposed in [15, 13, 14]. The payment system described there corresponds to the one in 5.1 if the conversion of the certificates is omitted. This does not reduce the security, but the anonymity is reduced, if only marginally, because for each transfer t the pseudonym $p_P^B(X,t)$ is the same as the pseudonym $p_R^B(X,t')$ from an earlier transfer t'. The witness B can, therefore, recognise that in both cases the same person is involved. Furthermore, should the payer W in the transfer t' and the recipient Y in the transfer t co-operate (which is particularly likely if W and Y are the same person), they can also recognise this and thus link the pseudonyms $p_P(X,t)$ and $p_R(X,t')$, which should have been protected.

This system would remain if the mechanism for convertible credentials described in 3.1.2.2, which can currently only be implemented with the special crypto- (or rather signature) system RSA, were broken, but other systems for digital signatures continued to exist. As one can at least prove that breaking some systems is equally difficult to solving a mathematical problem which has long been recognised as difficult, this is not entirely improbable.

5.4 Some Additional Conditions for an Anonymous Payment System

Using an anonymous payment system should not present any disadvantages in comparison to today's payment systems. In particular, a user

- should be free to select the witness for his payments from a number of different banks,
- should be able to transfer money wherever he likes, in particular also to a conventional payment system which is outside the open system and vice-versa,
- be able to anonymously invest money for interest and
- correspondingly be able to borrow money for interest.

Alongside the user requirements of the services to be supplied, the requirements of the banks and the government also need to be taken into account, e.g., an anonymous payment system must not prevent taxation of assets or income.

In particular the limitations on reasonable anonymity need to be considered here; however, in this article they were assumed to lie outside the borders of the open digital system and have therefore not been examined more closely. Without considering them, however, one cannot make meaningful statements about the appropriateness and possibilities, e.g., for taxation in spite of and retaining anonymity.

5.4.1 Transfer Between Payment Systems

In the payment systems considered in 5.1 and 5.2, only one witness, i.e. one bank, was considered. However, for economical reasons as well as for the purposes of anonymity, an anonymous payment system should allow the payer and recipient to use different banks, and even to use different payment systems.

If the payer and the recipient use the same anonymous payment system, but different witnesses, then in Step [1] of the protocol in 5.1, the recipient Y has to indicate a witness B_R he trusts, in addition to the pseudonym $p_R^B(Y, t)$. In [2], the payer informs his witness B_P about the new witness B_R. As B_P and B_R are not anonymous to each other, they can co-operate in an arbitrary way in respect of the payment, and thus be considered as a single witness B. All the communication between B and X is taken over by B_P, and all communication between B and Y by B_R.

A transfer between a non-anonymous and the anonymous payment system can be implemented very simply. The provider of the non-anonymous payment system, i.e., a bank, plays the role of a mediator who can act in both payment systems. The transfer between two users X and Y is split into two transfers between X and the bank, and the bank and Y. In the same way, of course, a user can also transfer money to himself in a different payment system, without reducing his anonymity within the anonymous system.

5.4.2 Interest on Balance, Granting of Credit

In both payment systems considered in 5.1 and 5.2, the rights for which B serves as a witness can be regarded as sight deposits managed by bank B. The owner of the rights can access them at all times, but B is aware of every access. As a result the bank only has limited reason to pay interest and one could, e.g., consider to balance it with the bank charges, i.e., neither interest or nor charges would be specifically computed.

Both payment systems, however, can easily be extended so that a credit balance can be invested for a fixed period of time. In this case payment of interest would make sense for the bank. With fixed accounts this is a trivial matter. Where there are no fixed accounts, one could express various due dates for the rights by using various signatures $p_B^{d_1}, p_B^{d_2}, \ldots$ on the certificates of ownership.

If one wants to permit forms of investment which depend on the total sum of the investment, one has to aggregate the amount to be invested in manner recognisable to the bank. This is most appropriately done by using the system from 5.2 with fixed accounts. Payment of interest is then possible just as it is today.

If such forms of investment are not implemented and the system described in 5.1 is used, each individual right has to be treated as a separate account. The point in time at which the account was "opened" can be established by means of the witness' signature. Interest can then be paid on a right by gradually increasing its value, or by paying out interest each time a transfer takes place [25].

Granting credit and charging interest on it is no more difficult in principle than it is today. In respect of securing the loan, the statements made in Section 3 apply: If the borrower wishes to remain anonymous, he has to give the bank certain securities. If he identifies himself to the bank, in order to re-establish anonymity he simply has to transfer the loan once to himself (e.g., to a second account); then he can use it like a normal positive balance.

Collecting charges for managing the account and for individual services provided by a bank is, as indicated in 3.5, scarcely more complicated in the anonymous case than it is today. For fixed accounts the bank can deduct its charges directly from the credit balance which it manages. If the accounts are not fixed, the banks have to collect their charges during the transfer, i.e. the payer must enclose a "charge transfer order" (a digital "revenue stamp") for the witnessing bank with his transfer order.

5.5 Secure Devices as Witness

If anonymity towards the witness is not deemed to be necessary, it is very easy to implement an anonymous payment system: The protocol from 5.1 can be adapted such that in all payments where user X appears as the payer or recipient, he selects the same pseudonym $p_P^B(X,t)$ or $p_R^B(X,t')$ (i.e. uses a fixed account number as a business-relationship pseudonym) and user B learns the pseudonyms $p_P(X,t)$ and $p_R(Y,t)$. This eliminates the problem of creating the substitute receipts in Steps [4] and [5], as well as the conversion of the certificate in Step [6].

To justify the assumption that the witness can be trusted regarding the anonymity of the user, a tamper-resistant device is typically chosen to play the role of the witness (see 3.1.2.2).

As to the use of such a device, there are two variants:

The first variant uses a single central secure device which witnesses all transactions.

The general remarks made in 2.2 provide reasons why this variant is less than desirable. Furthermore, there is no decisive advantage compared to the non-trustworthy witness in 5.1 and 5.2. The protocol is greatly simplified, as mentioned above, but this only reduces the work done by the computer. It offers no reduction of effort for the user of the payment system, neither does it offer him any new opportunities.

In the second variant each user obtains his own secure device in the form of an "electronic wallet." This device witnesses the user's transactions (in the name of the payment system provider).

The use of secure devices as electronic wallets was proposed in [39, 37], but for reasons of the (apparently necessary) logging they were not yet anonymous. Anonymous versions of the system can be found in [13, 14].

The only genuine advantage of the (anonymous or non-anonymous) electronic wallets is that they are the only payment system which allows off-line transactions, i.e. allow the users to spontaneously make and receive many payments without having to communicate with a central authority in between. This advantage is less important here because only open systems based on a communication network are under consideration.

The disadvantages of electronic wallets are much more serious:

- As the payments are no longer processed by a central authority, the loss of an electronic wallet can result in the loss of payments which have already been received. In order to prevent this, relatively complicated loss tolerance measures have to be implemented [80, 81, 84].
- The security of a payment system which uses electronic wallets as the witnesses is significantly based on the tamper-resistance of the devices. As already discussed in 3.1.2.2, the existence of a device which will remain secure over time is highly doubtful, and the evaluation of the tamper-resistance of existing supposedly secure devices is scarcely possible.
- Using secure devices does not eliminate the need to use cryptographic techniques, in particular for the mutual authentication of the electronic wallets. Hence secure devices do not provide an emergency alternative should all encryption and signature systems be broken. Should only all asymmetric crypto and signature systems be broken, the use of secure devices, in combination with a symmetric cryptographic system, would still be sensible because the secure devices only need a digital identification system (see 3.1.2.1) among them themselves.

As a result of the disadvantages mentioned and the only minimal advantage of electronic wallets for open digital systems of the type under consideration, we do not consider their use to be appropriate.

5.6 Payment Systems with Security by Deanonymization

In [28] an anonymous payment system was introduced which only fulfills a weaker security definition than the one used so far:

- A user may only transfer a right which he has received once. If he transfers it more than once, it has to be possible to remove his anonymity.

The basic idea is the same as in section 4.1, i.e. one hopes that after removing the anonymity the total assets available will be sufficient to cover any claims for damages.

In spite of its weaker security, the system is described here. On one hand it is not less secure than, e.g., today's credit card system, on the other hand, for off-line payments it offers the only alternative to the questionable electronic wallets described in 5.5.

The main difference to the payment systems described above is that, instead of witness B, the payer X himself confirms the transfer to the recipient of the payment Y. If X behaves correctly, his anonymity is maintained. If he does not behave correctly and transfers the right again to a different recipient Y^*, then due to a cryptographic trick the likelihood is very high that both of X's transfer confirmations can be combined in such a way that the identity of X can be revealed. If the right is claimed from B more than once, the identity of X can be revealed by B.

Due to the fact that no witness is required for the transaction, this payment system can be directly applied for off-line payments and is also suggested for this purpose in [28].

It is possible to increase the security by combining the system with secure devices. In place of arbitrary computers, the user has to use secure devices which prevent transferring a right more than once. The combined system fulfils the stronger security definition as long as the secure devices are, in actual fact, secure; otherwise it is as secure as the original system without secure devices.

Unfortunately the payment system has not been fully published yet [19]. Payment systems which limit the off-line characteristic in the sense that the recipient Y of a payment cannot re-transfer the received right without first contacting the bank, are described in [28, 26, 17]. (According to David Chaum a related payment system proposed in [53, 54] proved to be defective.)

6 Outlook

6.1 Open Problems

If one assumes that in the future legal transactions will frequently be carried out by means of open digital systems, and that there might even be high social pressure for everyone to use certain services (e.g., digital signatures, payment and value exchange systems), the security of these systems takes on particular importance.

In order to avoid introducing expensive systems which do not permit the same legal certainty provided by classical systems, or in which this legal certainty has to be created afterwards with considerable effort (e.g., as in the case of an EC card used for cash machines which is stolen together with the PIN), it must be ensured from the onset that the systems which are introduced provide legal certainty. It has been seen in the preceding sections that such systems will be very complex. For this reason a reliable intuitive evaluation is no longer possible, not only for technical non-experts, e.g., lawyers, but not even for computer scientists. The guarantee of legal certainty must, therefore, take the form of a proof.

A proof of legal certainty would show that it is either impossible for an illegal condition to occur, or that if one occurs, sufficient evidence has been created and is in the hands of the right parties so that a legal state can be reestablished (using force, if necessary).

If the proof is constructive, it simultaneously shows generally how an investigation procedure has to work.

For proving the correctness of a digital signature, payment or value exchange system, however, several things are still missing: One is proven basic statements about the security of the aids used, e.g., the cryptographic systems (for which such statements can at least already be partially proven), or "tamper-resistant" devices. Another is a precise formulation of the statement to be proven, i.e. a characterisation of what is meant by "correctness" or "legal certainty" in the system under consideration.

For this, existing law is not only (naturally) still too informal, but mostly also not general and abstract enough.

Hence a joint task for lawyers and computer scientists arises:

In areas with legal regulation where systems based on informational processes are to be introduced, and where no sufficiently general appropriate requirements are known in jurisprudence yet, such requirements have to be derived from the ideas of justice that underlie the current legal regulation. (to cover those which are not already known in jurisprudence). For example, one of the requirements on a signature system would certainly be that it should provide documents with evidential value, as expressed in the (informal) basic requirements for a digital signature described in 3.1.2.1. Another would be that it should offer protection against statements being issued without due consideration.

Furthermore, these requirements should be translated to a formal model.

Naturally, general regulation of this nature has to be expanded through special and widely understandable (hence, informal) comments, which describe which concrete systems have been found to be appropriate and how they are to be used. For example, it could be explained that in the place of a hand-written signature, a digital signature using GMR would always be permissible. The risk that the formal and informal formulation are not equivalent should be easier for society to bear than the risk which the introduction of a complicated system without proof of its legal certainty would present.

6.2 Summary From a Practical Point of View

In the preceding sections we informally presented all the proposals we are aware of which promote both the legal certainty and the anonymity of transactions which are carried out exclusively by means of an open digital system.

The following conclusions can be drawn from a practical point of view:

1. Only the combination of legal and technical measures can ensure the protection of data and legal certainty in open systems. Legal measures alone are insufficient.

2. There are efficient and cost-effective technical aids which guarantee user anonymity in such a way that the user can monitor this process. The aids presented here do not restrict the application spectrum of open digital systems in any way, nor do they make the use of these systems more complicated.

3. Legal certainty and anonymity are not opposites. The fact that the aids discussed are the same in both anonymous and non-anonymous systems suggests the conclusion that both systems can provide equal security against deception. The particular problems which arise from anonymous dispute handling require that special precautions are taken when obtaining evidence and for guaranteeing assets. As these precautions are sometimes considered unnecessary in a non-anonymous situation, anonymous systems may well be even more secure than some non-anonymous systems (including non-digital systems, such as purchases made in a shop).

4. The use of non-anonymous networks, and thus the use of non-anonymous open systems in general, endangers the personal rights of all users for a long time because introducing anonymity at a later date is virtually impossible. In contrast, the use of an anonymous system does not exclude the (voluntary or prescribed) deliberate self-identification of a user. Hence only anonymous systems keep all options open for the future.

As we have seen that legal certainty and privacy can complement each other harmoniously, and because both must be counted among the basic principles of a free democratic constitutional state, the natural anonymity of everyday life should also be transferred to new systems wherever possible.

We thank Dr. Volker Anhäusser, Holger Bürk, Dr. Klaus Echtle, Dr. Jürgen W. Goebel, Prof. Dr. Winfried Görke, Dr. Helmut Redeker, Dr. Jochen Schneider for motivating and fruitful discussions and constructive criticism. We also wish to thank the members of the SIG Computer and Law (Fachgruppe Informationsrecht) of the German Society for Computer Science (GI) who once made us aware of the legal details of the subject. Finally, we thank the Deutsche Forschungsgemeinschaft (DFG) for their friendly support, which made this research possible.

We thank *Dale Whinnett* and *Lothar Fritsch* for first translating text and figures, respectively.

References

[1] C. R. Abbruscato: Data Encryption Equipment; IEEE Communications Magazine 22/9 (1984) 15-21

[2] S. G. Akl: Digital Signatures: A Tutorial Survey; Computer, IEEE, 16/2 (1983) 15-24

[3] R. Aßmann: Effiziente Software-Implementierung von verallgemeinertem DES; Diploma thesis, Institut für Rechnerentwurf und Fehlertoleranz, University of Karlsruhe 1989

[4] AT&T: Einchip-Prozessor zur Verschlüsselung digitaler Signale; Design&Elektronik, Markt&Technik 21 (1986) 8-11

[5] M. Bellare, S. Micali: Non-interactive Oblivious Transfer and Applications; Crypto '89, August 20-24 1989, Abstracts, 517-528

[6] M. Ben-Or, O. Goldreich, S. Micali, R. L. Rivest: A Fair Protocol for Signing Contracts; Proc. of 12th ICALP, LNCS 194, Springer-Verlag, Heidelberg 1985, 43-52

[7] G. Bleumer: Vertrauenswürdige Schlüssel für ein Signatursystem, dessen Brechen beweisbar ist; Studienarbeit, Institut für Rechnerentwurf und Fehlertoleranz, University of Karlsruhe 1989

[8] M. Blum, P. Feldman, S. Micali: Non-interactive zero-knowledge and its applications (extended abstract); 20th Symposium on Theory of Computing (STOC) 1988, ACM, New York 1988, 103-112

[9] M. Blum, S. Goldwasser: An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information; Proc. of Crypto 84, LNCS 196, Springer-Verlag, Heidelberg 1985, 289-299

[10] Gerrit Bleumer, Birgit Pfitzmann, Michael Waidner: A Remark on a Signature Scheme where Forgery can be Proved; Eurocrypt '90, Aarhus 1990

[11] G. Brassard: On Computationally Secure Authentication Tags Requiring Short Secret Shared Keys; Crypto '82, Plenum Press, New York 1983, 79-86

[12] Gilles Brassard: Modern Cryptology—A Tutorial; LNCS 325, Springer-Verlag, Berlin 1988

[13] H. Bürk, A. Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, Proc. of the 4th International Conference on Computer Security, Monte Carlo 1986; to appear in: A. Grissonnanche (ed.), North-Holland, Amsterdam; *Revision:* Interner Bericht 2/87, Fakultät für Informatik, University of Karlsruhe 1987

[14] H. Bürk, A. Pfitzmann: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399-416

[15] H. Bürk: Digitale Zahlungssysteme und betrugssicherer, anonymer Wertetransfer; Studienarbeit, Institut für Informatik IV, University of Karlsruhe 1986

[16] Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983—1 BvR 209/83 u. a.; Datenschutz und Datensicherung DuD 4 (1984) 258-281

[17] D. Chaum, B. den Boer, E. van Heyst, S. Mjølsnes, A. Steenbeek: Efficient Electronic Checks; Eurocrypt '89; Houthalen 1989, Abstracts, 171-174

[18] D. Chaum, H. van Antwerpen: Undeniable Signatures; Crypto '89, August 20-24 1989, Abstracts, 205-212

[19] D. Chaum, H. van Antwerpen: Private communication, 1989.

[20] D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of ACM 24/2 (1981) 84-88

[21] D. Chaum: Blind Signatures for untraceable payments; Proc. of Crypto 82, Plenum Press, New York 1983, 199-203

[22] D. Chaum: A New Paradigm for Individuals in the Information Age; Proc. of the 1984 Symposium on Security and Privacy, IEEE, Oakland 1984, 99-103

[23] D. Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of ACM 28/10 (1985) 1030-1044

[24] D. Chaum: Cryptographic Identification, Financial Transaction, and Credential Device; United States Patent, Patent Number 4,529,870; Date of Patent: Jul. 16, 1985, Filed Jun. 25, 1982

[25] D. Chaum: Privacy Protected Payments—Unconditional Payer and/or Payee Untraceability; Amsterdam 1986; *Revision:* SMART CARD 2000: The Future of IC Cards, North-Holland, Amsterdam 1989, 69-93

[26] D. Chaum: Online Cash Checks; Eurocrypt '89; Houthalen 1989, Abstracts, 167-170

[27] D. Chaum, J.-H. Evertse: A secure and privacy-protecting protocol for transmitting personal information between organizations; Crypto '86, LNCS 263, Springer-Verlag, Berlin 1987, 118-167

[28] D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash; Crypto '88, 1988, Abstracts

[29] R. Clemens: Die elektronische Willenserklärung— Chancen und Gefahren; Neue Juristische Wochenschrift NJW 34 (1985) 1998-2005

[30] I. Damgård: Payment systems and credential mechanisms with provable security against abuse by individuals; Draft, received 88.08.15; Crypto '88, August 21-25 1988, Abstracts

[31] D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer (2nd. ed.); John Wiley, Chichester 1989

[32] D. W. Davies: Apparatus and methods for granting access to computers; UK Patent Application, Application No. 8503481, Date of filing 11 Feb. 1985, Application published 4 Sept. 1985

[33] G. Davida: Chosen Signature Cryptanalysis of the RSA (MIT) Public Key Cryptosystem; TR-CS-82-2, University of Wisconsin, Milwaukee (October 1982)

[34] D. E. Denning: Cryptography and Data Security; Addison-Wesley, Reading 1982 (reprinted with corrections 1983)

[35] Federal Information Processing Standards Publication 46 (FIPS PUB 46): Specification for the Data Encryption Standard; January 15, 1977

[36] W. Diffie, M. E. Hellman: New Directions in Cryptography; IEEE Trans. on Information Theory IT-22/6 (1976) 644-654

[37] S. Even: Secure Off-Line Electronic Fund Transfer Between Nontrusting Parties; SMART CARD 2000: The Future of IC Cards, North-Holland, Amsterdam 1989, 57-66

[38] S. Even, O. Goldreich, A. Lempel: A Randomized Protocol for Signing Contracts; Communications of ACM 28/6 (1985) 637-647

[39] S. Even, O. Goldreich, Y. Yacobi: Electronic Wallet; Electronic wallet; Crypto '83, Plenum Press, New York 1984, 383-386; Intern. Zurich Seminar on Digital Communications, Zürich, IEEE 1984, 199-201

[40] A. Fiat, A. Shamir: How to Prove Yourself: Practical Solutions to Identification and Signature Problems; Crypto '86, LNCS 263, Springer-Verlag, Berlin 1987, 186-194

[41] H.-U. Gallwas, H. Geiger, J. Schneider, J. Schwappach, J. Schweinoch: Datenschutzrecht— Kommentar und Vorschriftensammlung; Kohlhammer, Stuttgart 1978

[42] Shafi Goldwasser, Silvio Micali: Probabilistic Encryption; 14th Symposium on Theory of Computing (STOC) 1982, ACM, New York 1982, 365-377; *Revision:* Journal of Computer and System Sciences 28 (1984) 270-299

[43] S. Goldwasser, S. Micali, R. L. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; 25th Symposium on Foundations of Computer Science (FOCS) 1984, IEEE Computer Society, 1984, 441-448; *Revision:* SIAM J. Comput. 17/2 (1988) 281-308

[44] S. Herda: Authenticity, Anonymity and Security in OSIS. An Open System for Information Services; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer-Verlag, Heidelberg 1985, 35-50

[45] P. Horster: Kryptologie; Reihe Informatik/47, Bibliographisches Institut, Mannheim 1985

[46] I. Ingemarsson: Critique of the Security of Public-key Systems; Intern. Zurich Seminar on Digital Communications, Zürich, IEEE 1984, 171-173

[47] B. S. Kaliski, R. L. Rivest, A. T. Sherman: Is the Data Encryption Standard a Group?; Eurocrypt 85, LNCS 219, Springer-Verlag Heidelberg 1986, 81-95; *Revision:* Journal of Cryptology 1/1 (1988) 3-36

[48] H. Köhler: Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen; Datenschutz und Datensicherung, Teil I: DuD 6 (1986) 337-344, Teil II: DuD 1 (1987) 7-12, Teil III: DuD 2 (1987) 61-67

[49] A. K. Lenstra, M. S. Manasse: Factoring - where are we now?; IACR Newsletter 6/2 (1989) 4-5

[50] M. Luby, C. Rackoff: How to construct permutations from pseudorandom functions; 18th Symposium on Theory of Computing (STOC) 1986, ACM, New York 1986, 356-363; *Revision:* SIAM J. Comput. 17/2 (1988) 373-386

[51] H. A. Maurer, N. Rozsenich, I. Sebestyen: Videotex without "Big Brother"; Bericht F128, IIG Universität Graz 1984; published in: Electronic Publishing Review, Oxford 1984

[52] Matthew: 2,16; in The Bible

[53] T. Okamoto, K. Ohta: Divertible Zero Knowledge Interactive Proofs and Commutative Random Self-Reducibility; Eurocrypt '89; Houthalen 1989, Abstracts, 95-108

[54] T. Okamoto, K. Ohta: Disposable Zero-knowledge Authentications and Their Applications to Untraceable Electronic Cash; Crypto '89, 1989, Abstracts, 443-458

[55] A. Pfitzmann, R. Aßmann: Efficient Software Implementations of (Generalized) DES; Proc. SECURICOM 90, 8th Worldwide Congress on Computer and Communications Security and Protection, March 13-16, 1990, Paris

[56] A. Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhhung des Datenschutzes; Interner Bericht 18/83, Fakultät für Informatik, University of Karlsruhe 1983

[57] A. Pfitzmann: How to implement ISDNs without user observability - Some remarks; Interner Bericht 14/85, Fakultät für Informatik, University of Karlsruhe 1985

[58] B. Pfitzmann: Für den Unterzeichner sichere digitale Signaturen und ihre Anwendung; Diplomarbeit, Institut für Rechnerentwurf und Fehlertoleranz, University of Karlsruhe 1989

[59] A. Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Dissertation, Universityy of Karlsruhe 1989; IFB 234, Springer-Verlag, Heidelberg 1990

[60] B. Pfitzmann, A. Pfitzmann: How to Break the Direct RSA-Implementation of MIXes; Eurocrypt '89; Houthalen 1989, Abstracts, 228-235

[61] A. Pfitzmann, B. Pfitzmann, M. Waidner: Datenschutz garantierende offene Kommunikationsnetze; Datenschutz und Datensicherung DuD 3 (1986) 178-191; *Revision:* Informatik-Spektrum 11/3 (1988) 118-142

[62] G. J. Popek, C. S. Kline: Issues in Kernel Design; Operating Systems, An Advanced Course; LNCS 60, Springer-Verlag, Heidelberg 1978; Nachgedruckt in: Springer Study Edition; Springer-Verlag, Heidelberg 1979, 209-227

[63] H. Redeker: Geschäftsabwicklung mit externen Rechnern im Bildschirmtextdienst; Neue Juristische Wochenschrift NJW 42 (1984) 2390-2394

[64] H. Redeker: Die Benutzung von technischen Medien zur Einlegung von Rechtsmitteln; Computer und Recht CR 2/8 (1986) 489-491

[65] K. Rihaczek: Fälschungssichere elektronische Orderpapiere; Datenschutz und Datensicherung DuD 3 (1984) 197-204

[66] K. Rihaczek: Der Stand von OSIS; Datenschutz und Datensicherung DuD 4 (1985) 213-217

[67] R. L. Rivest, A. Shamir: How to Expose an Eavesdropper; Communications of ACM 27/4 (1984) 393-395

[68] R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of ACM 21/2 (1978) 120-126 und 26/1 (1983) 96-99

[69] C. Schwarz-Schilling (ed.): Konzept der Deutschen Bundespost zur Weiterentwicklung der Fernmeldeinfrastruktur; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn 1984

[70] C. Schwarz-Schilling (ed.): ISDN - die Antwort der Deutschen Bundespost auf die Anforderungen der Telekommunikation von morgen; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn 1984

[71] C. Schwarz-Schilling (ed.): Mittelfristiges Programm für den Ausbau der technischen Kommunikationssysteme; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn 1986

[72] H. Sedlak: The RSA cryptography processor; Eurocrypt '87, LNCS 304, Springer-Verlag, Heidelberg 1988, 95-105

[73] C. E. Shannon: Communication Theory of Secrecy Systems; The Bell System Technical Journal 28/4 (1949) 656-715

[74] G. Simmons: A Survey of Information Authentication; Proceedings of the IEEE 76/5 (1988) 603-620

[75] K. Thompson: Reflections on Trusting Trust; Communications of ACM 27/8 (1984) 761-763

[76] M. Turoff, S. Chinai: An Electronic Information Marketplace; Computer Networks and ISDN Systems 9/2 (1985) 79-90

[77] U. Vazirani, V. Vazirani: Efficient and Secure Pseudo-Random Number Generation; Crypto '84, LNCS 196, Springer-Verlag, Berlin 1985, 193-202

[78] M. Waidner: Datenschutz und Betrugssicherheit garantierende Kommunikationsnetze. Systematisierung der Datenschutzmanahmen und Ansätze zur Verifikation der Betrugssicherheit; Diplomarbeit, Interner Bericht 19/85, Fakultät für Informatik, University of Karlsruhe 1985

[79] M. Waidner, A. Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer-Verlag, Heidelberg 1985, 128-141; *Revision:* Datenschutz und Datensicherung DuD 1 (1986) 16-22

[80] M. Waidner, B. Pfitzmann: Verlusttolerante elektronische Brieftaschen; 3. Fachtagung Fehlertolerierende Rechensysteme, IFB 147, Springer-Verlag, Heidelberg 1987, 36-50; *Revision:* Datenschutz und Datensicherung DuD 10 (1987) 487-497

[81] M. Waidner, B. Pfitzmann: Anonyme und verlusttolerante elektronische Brieftaschen; Interner Bericht 1/87, Fakultät für Informatik, University of Karlsruhe 1987

[82] M. Waidner, B. Pfitzmann: Unconditional Sender and Recipient Untraceability in spite of Active Attacks—Some Remarks; Fakultät für Informatik, University of Karlsruhe, Interner Bericht 5/89, March 1989

[83] M. Waidner, B. Pfitzmann: The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability; University of Karlsruhe 1989; Eurocrypt '89, LNCS, Springer-Verlag, Berlin 1990

[84] M. Waidner, B. Pfitzmann: Loss-tolerant Electronic Wallet; Proc. Smart Card 2000, Amsterdam 1989; shorter version: 20th International Symposium on Fault-Tolerant Computing (FTCS-20); IEEE Computer Society, 1990

[85] M. Waidner, B. Pfitzmann, A. Pfitzmann: Über die Notwendigkeit genormter kryptographischer Verfahren; Datenschutz und Datensicherung DuD 6 (1987) 293-299

[86] M. N. Wegman, J. L. Carter: New Classes and Applications of Hash Functions; 20th Symposium on Foundations of Computer Science (FOCS) 1979, IEEE Computer Society, 1979, 175-182