Institut für Allgemeine Wirtschaftsforschung

Abteilung für Wirtschaftspolitik

INSTITUTIONAL FRAMEWORK OF ELECTRONIC COMMERCE: A CONSTITUTIONAL ECONOMIC ANALYSIS OF THE PROBLEMS WITH DIGITAL SIGNATURES

HANSUELI STAMM

01/3A

ISSN 1437-1510

FREIBURGER DISKUSSIONSPAPIERE ZUR ORDNUNGSÖKONOMIK

FREIBURG DISCUSSION PAPERS ON CONSTITUTIONAL ECONOMICS

Albert-Ludwigs-Universität Freiburg i. Br.

INSTITUTIONAL FRAMEWORK OF ELECTRONIC COMMERCE: A CONSTITUTIONAL ECONOMIC ANALYSIS OF THE PROBLEMS WITH DIGITAL SIGNATURES

HANSUELI STAMM

01/3A

Albert-Ludwigs-Universität Freiburg i. Br.

Extended English version of „Institutioneller Rahmen des Electronic Commerce: Eine ordnungsökonomische Analyse am Beispiel der digitalen Signatur.“ Freiburger Diskussionspapiere zur Ordnungsökonomik 01/3.

FREIBURGER DISKUSSIONSPAPIERE ZUR ORDNUNGSÖKONOMIK
FREIBURG DISCUSSIONPAPERS ON CONSTITUTIONAL ECONOMICS
01/3A
ISSN 1437-1510

Albert-Ludwigs-Universität Freiburg im Breisgau; Institut für allgemeine Wirtschaftsforschung; Abteilung für Wirtschaftspolitik; Kollegiengebäude II; Platz der Alten Synagoge; D - 79085 Freiburg i. Br.
Tel. Nr.: +49 +761 / 203 2317; Fax. Nr.: +49 +761 / 203 2322
http://www.vwl.uni-freiburg.de/fakultaet/wipo/wipo.htm

INSTITUTIONAL FRAMEWORK OF ELECTRONIC COMMERCE: A CONSTITUTIONAL ECONOMIC ANALYSIS OF THE PROBLEMS WITH DIGITAL SIGNATURES

Hansueli Stamm, University of Freiburg i. Br.[1]

Contents

Abstract

Subject of this paper are the problems of trust in electronic commerce that have originated because of the falling apart of authenticity and identity of digital signatures. It is shown, that this problem of trust between unknown persons is one step ahead of the usual trader- or prisoner-dilemma-problem. It is possible, however, to solve it on a private basis by so called "certification authorities". Nevertheless, there is a lot of state regulation in the area of digital signature. The respective regulations define standards which have to be met for formal recognition of the equivalence of electronic and handwritten signatures. This is a condition for electronic commerce to be used in contracts for which the written form is required or for using digital signatures as proof in trade disputes in a state court.

German Summary

Das Paper beschäftigt sich mit dem Auseinanderfallen von Authentizität und Identität bei digitalen Signaturen als einer Quelle von Unsicherheit und den daraus entstehenden Vertrauensproblemen beim elektronischen Handel. Es wird gezeigt, dass diese Vertrauensprobleme dem beim Handel zwischen Unbekannten üblichen Handels- oder Gefangenen-Dilemma-Problem um eine Stufe vorgelagert sind und somit nicht mit den bekannten Institutionen gelöst werden können. Dennoch kann es im bisherigen institutionellen Rahmen dank dem Entstehen von sog. Zertifizierungsstellen auf rein privater Basis gelöst werden. Trotzdem sind an vielen Orten zur Zeit staatliche Regulierungsbemühungen zu beobachten. Diese haben u.a. zum Ziel, Transaktionen, für deren Gültigkeit Schriftform verlangt wird, dem elektronischen Handel zugänglich zu machen, indem sie entsprechende Standards festgelegt werden, die es ermöglichen sollen, die digitale der handschriftlichen Unterschrift rechtlich gleichzusetzen.

[1] I would like to thank Ingrid Zoll and the participants of the workshop „Ordnungsökonomik und Recht" for helpful comments and Otto Stamm for the English translation of the paper.

1. INTRODUCTION

There is no newspaper which does not publish almost daily an article nor is there a discussion relating to the stock exchange where Electronic Commerce and Internet are not mentioned.[2] The rapid and continuous progress in information technology has lead to an evident transformation in ways of doing business. Distances have been shortened or totally eliminated, new markets have emerged, others have disappeared, new skills and know-how are asked for. These structural changes are generating new impulses which in turn influence our behaviour: the institutional framework within which we act, is continuously changing.

However, the fundamental principles that motivate our actions remain the same. Thus, also in the "E-Age", the objective of trade is the realization of potential profits resulting from an exchange of goods; this is achieved by everybody exchanging those goods which can be produced at a comparative advantage, for such goods, which are needed but which others can produce on more favourable terms. The prerequisite of such an exchange is the trust in the other partners participating in this exchange, i.e. that they will stick to the agreed conditions. Trade comes about only if the potential profit is higher than the degree of insecurtity.

As a new and open[3] medium, the Internet opens up completely new possibilities for doing business. These possibilities are commonly summed up by the term "Electronic Commerce".[4] Innovations, that "invade" traditional ways of doing things cause insecurity. Insecurity on the other hand increases costs and these costs may prevent a transaction. There may be various reasons for this insecurity. One of these is the lack of trust in unknown trading partners as a consequence of using this new medium for the transaction.[5]

Problems of trust are not fundamentally new in economic history. Up to now solutions have always been found that were able to reduce these problems so that the "endangered" transactions took place anyhow. There are roughly two ways of solving these problems:

---

2 When looking in the "Neue Zürcher Zeitung" for the headword "Internet", there are exactly 1000 entries for 1997, in 1999 nearly twice as many entries appeared and in 2000 more than 2700.

3 Electronic Commerce in closed networks, i.e. networks which are laid out by the involved enterprises and which are not accessible to third parties, has existed since the sixties (so-called Electronic Data Interchange EDI) (see GREENSTEIN & FEINMANN 2000: Chapter 4).

4 "Electronic Commerce" is defined differently in the literature (see for example OECD 1999:28f, BACHETTA ET AL. 1998:5 or MESENBOURG 1999). The only subject of this paper is the conclusion of a contract as a fundamental part of a transaction (not only) over the Internet. So it is a deliberate decision not to add a new definition neither to distinguish between "business to business" (B2B) - and "business to consumer" (B2C)-Electronic Commerce.

5 Problem of trust in this context means that an agreement will not be concluded because e.g. it is not sure whether the transmitted data were not changed, or because it is not clear who is party to the agreement.

Private solutions emerging spontaneously among the participants and solutions that were planned and implemented by the state.

Polls have confirmed that a problem of trust exists with Electronic Commerce. This problem will be analyzed in the present paper by means of an act which is fundamental for the realization of an electronic transaction, namely the digital signature. It will become evident that due to the falling apart of authenticity and identity in electronic signing a problem for creating trust unknown until now has emerged. In addition it can be seen that this problem can be solved within the framework of existing governmental regulations by institutions which have emerged spontaneously. In a next step the problem of governmental recognition of the equivalency of electronic and handwritten signatures is dealt with.

2. WHAT IS NEW WITH RESPECT TO ELECTRONIC COMMERCE?

The need for a change in the institutional framework of a system appears, whenever the old framework is no longer adequate. In order for an existing framework to no longer fulfill its tasks, especially the reduction of insecurity, a change in its surroundings must have occurred. This change has to be greater than the one which could be expected within the normal dynamics of the economy and which could be coped with by the availability of existing rules. If there is a real requirement for new rules for Electronic Commerce, it must first be shown that there are real problems that did not exist before. That would mean that these problems did not exist when doing business in the conventional way and that they cannot be solved by the existing rules.

The objective of this paragraph is to identify those elements that create insecurity. Surveys have been conducted and evaluated. Conclusions can be drawn from these surveys as far as what enterprises or their representatives consider new about Electronic Commerce.

During the last three years several surveys concerning electronic commerce were published. Primarily they focus on listing business opportunities and mentioning factors that lead to success. In addition they deal with problems that arise when doing business over the Internet.[6] Even if the main subject of the various contributions is not always the same, the conclusions are quite similar. An important point that often shows up is the lack of commonly used

[6] See among others „Electronic Commerce Enquête I and II“ by MÜLLER & SCHODER (1999) respectively by EGGS & ENGELERT (2000), as well as KURBEL & TEUTEBERG (1998) or SMEDINGHOFF (1998).

business practices.[7] This, however, is certainly not so new that it could be traced back solely to the new electronic medium.

As important as this statement are points that have a direct reference to the Internet. Some examples are the burden of proof with online-transactions, the guarantee of the integrity of the transmitted information or problems with the security of payments via the Internet. On top of this list is also the reliability of unknown web-participants and – related to this – problems concerning electronically signed contracts.

What importance do these problems have? Where must they be integrated? NORTH (1990:34f) distinguishes between three general ways of exchange which have developed in the course of time. His enumeration starts with the personal exchange, where no third party exists which enforces contracts. This type prevailed for a long time. At that time the costs of production consisted on one hand in high transformation costs due to the limited division of labour and on the other hand in low transaction costs because of the small risks when only few parties were involved. With the extension of the range of trade, technical innovations that enhance infrastructure an a growing specialisation, transaction costs were decreasing. However, due to the steadily increasing group of participants in trade and the lack of governmental institutions (enforcement authority),[8] the insecurity connected with a transaction has become more and more insecure, which has lead to high transaction costs. The third stage is impersonal exchange with low transformation costs which is possible because of the institutional innovation in the form of a national state with its monopoly of power used as third party enforcement. This institutional innovation has drastically reduced the transaction costs.

Where does the electronic exchange fit into this enumeration? Thanks to the new possibilities of providing and processing information the dimension of distance has disappeared almost completely. As a result, a further extension of the range of the markets became possible in the Electronic Commerce.[9] Therefore, an additional reduction of transformation costs may be expected.

---

7 The survey of MÜLLER & SCHODER (1999) shows that more than 71% of the interviewees rated this point as accurate. It got the leading rating out of 32 potential obstacles to electronic commerce. STRAUSS & SCHODER (2000) consider it still to be on top of the "ten most important obstacles to Electronic Commerce".

8 Even worse: The "state" acted at that time rather as an additional factor of insecurity, because its behaviour was mostly unforeseeable (see NORTH 1990: 35).

9 More accurately the trade with electronic, i.e. digitalized goods should be discussed here. For trade with "traditional" goods the new possibilities still apply for the arragement of an agreement (global possibilities for information on different offers), the corresponding negotiations and the conclusion of the agreement.

The situation is not so clear when looking at the transaction costs. There is no doubt that the simplification of the exchange of information drastically reduces transaction costs. But according to the polls mentioned above several situations exist which lead to insecurity amongst traders. This eventually increases the transaction costs again so that exchange is prevented. In addition, Electronic Commerce often is international trade with the well-known problems of an inadequate legal system in foreign trade. This leads to a further increase in transaction costs. In the system of NORTH the emergence of Electronic Commerce in the field of production means an additional step forward, but from the institutional point of view for the time being a step backwards.

3. CONSTITUTIONAL ECONOMIC POINT OF VIEW

Aim of this paper is to show possible institutional deficits that are not covered by the existing framework of rules. Conceivable solutions for this problem will be presented as well ones that can be implemented, by dealing with the problems associated with digital signatures. The theoretical basis for this analysis is the constitutional political economy ("Ordnungs-ökonomik"). This method gives recommendations in the form of hypothetical imperatives that indicate how to solve a social problem from an economic point of view. The goal is a "desirable" result for all individuals involved. Such a hypothetical imperative is "if one wants X, one should do Y". The implementation of what is demanded in such an imperative needs on the one hand the proof that X is in the interest of all individuals involved and on the other hand, that Y is a suitable method to reach X.[10]

When dealing with constitutional economic recommendations we have to distinguish between interests which are open to consensus and those which are not. In addition the differentiation between constitutional and subconstitutional decisions plays an important part. On the constitutional level the rules of a "game" will be decided on, whereas on the subconstitutional level the decision will be based on the moves of the game which are possible according to the rules.[11] The aim of a constitutional analysis of economic measures must be to render an opinion on whether they are desirable, i.e. in the consensual constitutional interest of all those concerned.

[10] See VANBERG (1997:709f).
[11] See VANBERG (1996:11f).

What does that mean for the problems of electronic commerce, in particular the problem of security, often mentioned in the surveys and its importance in the context of the digital signature? It means that the hypothetical imperative "If one wants to solve the trust problems of the electronic commerce, Y is to be done" must be looked at more closely. It must be shown that the "if"-part is of consensual constitutional interest to the involved persons and that the recommendations for Y solve the trust problems adequately from a constitutional political point of view.

Because of the likelihood of an expansion of the market it can be expected that there will be more prosperity. That is why one can expect a consensus among all participants to solve the new institutional problems of electronic commerce.

Three steps are conceivable to evaluate the necessary measures. In a first step, the concrete reason must be identified that causes such a big problem of trust which prevents the transaction from taking place when trading over the Internet. In a second step, the question has to be answered whether the existing rules and regulations do allow the formation of institutions which reduce the new insecurity. In the past the existing rules were able to solve the problems in a satisfactory way. If they also reduce the new insecurity, it is to be expected that new rules do not improve the situation. They only restrict the trade possibilities authorized until now but have no security improving effect.[12] If it is clear that an amendment to the rules is necessary, a third step is needed. The proposed rules have to be examined to see whether their application is appropriate enough to solve the problems of trust in Electronic Commerce.[13]

4. PROBLEMS OF TRUST WITH DIGITAL SIGNATURES

This chapter illustrates by means of the example of digital signature, that there are new problems of trust in Electronic Commerce due to the separation between authenticity and identity in the case of electronic signature. It becomes apparent that in order to overcome this problem new institutional solutions must be found because the costs of the insecurity are greater than the potential profit. Several approaches to solve the problem will be discussed, as well as arguments presented why the state intervenes in this process with new rules.

[12] The right of the above hypothetical imperative would therefore consist of an empty set, i.e. no measures are to be recommended.

[13] This description in three steps is simplified in so far as it eliminates the dynamics of the existing framework of rules. However, this simplification is justified because normally a verification is not a single event, but will be repeated periodically or on specific occasions.

4.1. The Digital Conclusion of a Contract

The principal part of an economic transaction is the conclusion of a contract. For this, there are several methods available. An important version of such an agreement is the contract in writing, followed by the handwritten signature of both or all parties to the contract. This makes it possible to identify the signers and to make them liable in case of a breach of any clauses of the contract. Therefore the parties to a contract may be sure that the signature is in fact from his business partner (authenticity) and that he is able to identify him. This separation of authenticity and identity is normally needless for handwritten signatures. It is, however, necessary to understand the problems that have arisen with the development of electronic contracts.

A digital signature consists[14] of data which represent the complete information to be signed and is produced by a respective arithmetic instruction.[15] It is codified with the private key[16] of the signer and it will be added to the signed data.[17]

With the help of cryptographic methods it is doubtlessly possible to assign a digitally signed message to the key with which it was generated. By this procedure, authenticity, i.e. the verification of the (technical) origin of a message, is guaranteed. But in contrast to a hand-written signature, a digital signature contains no information about the identity of the signer.

It is exactly this gap between authenticity and identity which represents one of the new problems of Electronic Commerce. It is one of the causes of the new insecurity with transactions via the Internet. A trader will not agree to a conclusion of a deal if he has no certainty with respect to the identity and therefore to the trustworthiness of his contractual partner.

---

[14] In this paper the term "digital signature" will be used synonymously with the term "electronic signature". In other publications the two terms are used differently, though not uniformly. Especially in legal texts the digital signature is directly associated with the technique of the Public-Key-Procedure (see Appendix). The electronic signature on the other hand is defined independently of technique (cf. e.g. the change of name from the old to the new German law of signature: the old one is named "GESETZ ZUR *DIGITALEN SIGNATUR*", the new one as an adoption to the Brussels terminology "GESETZ ÜBER DIE RAHMENBEDINGUNGEN FÜR *ELEKTRONISCHE SIGNATUREN*").

[15] These data are produced by means of a so-called Hash function, which reduces a message which may be as long as one likes, to the information content of a few characters which in all probability are unambiguous (see Appendix).

[16] For some time so-called asymmetric encryption procedures in cryptography have existed. Here the key consists of a private and a public part. Whereas the private part is secret, i.e. is known only to the owner, the public part of the key may be used by everybody. A message encoded with the private key can be decoded exclusively with the corresponding public key, a message encoded with the public key only by the owner of the private key (see Appendix).

[17] See the more detailed discussion of the technical process to generate a digital signature in the Appendix.

4.2. The Traders-Dilemma

The theoretical framework in which the analysis of the AI-gap will take place is the (simplified) situation of the traders-dilemma. Two traders have the choice whether or not to comply with the contract they have signed (cf. the pay-off-matrix in the table below). Without any securing institutions to force them to adhere to the contract, they both have an incentive not to comply. An example will illustrate this situation: Imagine that the contract between two traders provides an exchange of a certain volume of wine with a certain volume of wool. The winegrower (A) will realise that he is better off, if he waits until he gets the wool (B complies) and then decides not to send any wine (A does not comply). So A will have both the wine and the wool. And of course it will be favourable for the winegrower not to send any wine (A does not comply) if the wool-producer has decided not to fulfil the contract (B does not comply). The wool merchant can be expected to make the same considerations. So, independent of the decision of the other party, they both will end in the (1/1)-field. The deal will not take place because of the missing trust between the contracting parties.[18]

		Trader B	
		complies	does not comply
Trader A	complies	2 / 2	0 / 3
	does not comply	3 / 0	1 / 1

Pay-off-matrix of a traders-dilemma-game

Obviously there is trade, so there must be solutions to overcome the traders dilemma. In various publications usually two possibilities are mentioned how to accomplish the trust needed to realise possible gains from trade, i.e. how to force both parties to choose "compliance" in the matrix displayed above. One of these possibilities is a repetitive game with a high probability of meeting each other again. If one trader cheats, this will affect his reputation and he will soon be out of business. The other possibility is the enforcement of a contract by a third party accepted by both participants. Usually this third party is the state with its monopoly of coercive power. If one trader sent his goods but didn't receive any compensation as fixed in the contract he can rely on the judicial system to enforce his claim.

[18] The resulting pay-off-matrix is the same as the one of a prisoner's dilemma-game where both parties (prisoners), independent of each other, have an incentive not to confess. The prisoners as well as the traders end up in the non optimal Nash-equilibrium at (1/1). See e.g. NORTH (1990: 11ff and 54ff) or ELSNER (1997).

4.3. The Structure of the Problem: The Authenticity-Identity-Gap

In Electronic Commerce the "traditional" trust problems with trade as described in chapter 4.2 are solved as they are solved in the traditional trade.[19]. But in Electronic Commerce a new trust problem emerges because of the gap between authenticity and identity (AI-gap) of a digital signature. This gap is one step ahead of the traders-dilemma-problem. Both authenticity as well as identity of all participants of the exchange have to be known, before the solution of the traders-dilemma can work. It is easy to illustrate this point with the example of an electronic conclusion of an agreement taking place within a jurisdiction where one can presume that the state guarantees the enforcement of the contracts. In such a situation, the traders-dilemma would be solved. If a dealer is sure about the authenticity of the digital signature of a contract, but does not know the identity of his counterpart, the enforcement mechanism of the state cannot help him enforce his rights in case of a breach of contract. Even the state has no possibility to determine the identity of the signer by his digital signature. This problem also exists in the case of the solution with the repetitive game because reputation is tied to the person (identity). Without gap-closing institutions there is no certainty that the (authentic) signature is given each time by the same person (identity).

The gap between authenticity and identity in the case of signatures is a problem that demands new solutions. The reputation mechanism or the delegation of the solution to the state with its enforcement possibilities in situations of uncertainty because of missing security fails, as long as there is no information about whose reputation is being damaged or from whom the state has to collect the debts.

As long as the gap between authenticity and identity cannot be filled institutionally, there is no widespread Electronic Commerce to be expected between people who do not know each other. However, Electronic Commerce exists, which suggests that there are possibilities to close the AI-gap.

4.4. Methods of Resolution

The first step to enable Electronic Commerce is to close the authenticity-identity gap. Without additional institutions this is only possible if those participating in the trade know each other. In the electronic trade this would be the case with enterprises, which had contacts already

[19] For the solution of the problem in the medieval trade see e.g. MILGROM ET AL. (1990). A good description for the solution in the field of the incomplete legislation of foreign trade gives SCHMIDT-TRENZ (1990).

before the "E-time".[20] With the change-over from existing business relations to the new medium the efficiency of the available resources can be increased, but the actual advantage of the net, i.e. extension of its market, is only possible when the AI-gap can be closed by means of suitable institutions.

In the area of Electronic Commerce, specifically in the context of the digital signature, so called "Certification Authorities" (CA) have emerged. These institutions offer "public key"-infrastructures to close the illustrated gap.

4.4.1. Private Solution: Public Key-Infrastructure

Public key[21]-infrastructures (PKI) are offered by private, mostly profit oriented institutions. Three services are provided which belong together. First, electronic certificates[22] are issued that connect the digital signature with the identity of their owner. Second, in order to do this in a credible way, this institution has to offer a kind of registration of new candidates applying for a certificate confirming the identity of the owner of such certificate (Registration Authority). And thirdly, a publicly accessible database is necessary where all valid, expired, and blocked certificates may be inspected (Revocation List). These three functions make it possible to close the information gap between authenticity of the digital signature and the identity of its owner.[23,24]

---

[20] An example from the B2C-field is the introduction of Electronic Banking for bank customers, who already have an account or deposit at the respective bank.

[21] The term "public key" means the cryptographic method with which digital signatures are produced (see Appendix).

[22] A certificate is a public entry, i.e. one which can be inspected by everybody, in a database at a certification authority. This entry must contain on the one hand the identity of the owner of the certificate and on the other the public key with which the digital signature may be decoded. Certificates have a certain period of validity and must be renewed after expiration. If the owner violates the conditions for registration, his certificate is marked as blocked.

[23] It may be conceivable that certification authorites act also as centers of information for solving the problem of reputation which occurs with large groups of trade participants. Here the information which a certificate contains with respect to its owner, would also include an entry concerning his earlier business practices. Before a trader concludes an agreement with somebody, he would consult this information and only then decide whether he would like to enter into business relations with him. First approaches for such institutions are to be found e.g. at online-auctions in the C2C-field (cf. e.g. the feedback-system of eBay.de (http://pages.ebay.de/services/forum/feedback.html)).

[24] This type of "certification-institution" which makes certain information about somebody concerning certain characteristics of this third person available, is not new. They guarantee this information with their own name (reputation). Such examples are the office of trade register which among other things lists the representatives of a firm and provides, if requested, corresponding "certificates", or the examination authority of a university which issues "certificates" in the form of diplomas, which confirm that the owner has a certain spectrum of knowledge. The difference between such existing institutions of certification and the ones which allow the closure of the AI-gap, is that they make getting the information easier; however, trade or the filling of a vacant position would be conceivable without this (mechanism of reputation or test of qualification respec-

One problem, however, has not yet been solved by this structure of the external third PKI-institutions. With these institutions the trust problem has been removed on the lowest level but it simply reappears on the next higher level. In other words: who guarantees the trustworthiness of the certification authorities?

Four solutions are possible:

a) The institutions certify each other, i.e. the loss in reputation of one Certification Authority would depend also on the reputation of the other one.

b) The owners of the institutions guarantee the reputation of the PKI-institutions. In that way the Certification Authority adopts the reputation of its investors.[25]

c) The competition between the Certification Authorities and the advantageous and rapid possibilities of information in the net (e.g. it would be conceivable that rating agencies would make available respective information for investors[26]) will result in great negative impact for the institutions concerned in case a loss of reputation occurs.

d) The Certification Authorities create a common institution with a set of standards that are binding for its members. Members which do not follow these stipulations are excluded.

4.4.2. The Role of the State

The new problem of insecurity in the context of the digital signature which came up with the Electronic Commerce is solved thanks to the bridging of the gap between authenticity and identity by means of Certification Authorities. It could be assumed that already existing regulations seem to be adequate to enable contracts via an electronic medium and that the new institution "Certification Authority" develops spontaneously within the existing legal environment. Why are laws needed that have been passed recently in most of the industrialized countries that define standards for digital signatures and the validity thereof?

Most legal transactions take place with no respect of the form. That means that for their validity no special rules exist except the mutually declaration of intent. This absence of any

---

tively by potential employer). Certification Authorities (CAs) which offer Public Key-Infrastructures, simplify not only the conclusion of agreements in the Internet amongst partners not knowing each other, but as a matter of fact, they make these possible in the first place. Without CAs, trade via the new medium is not to be expected in view of the reasons given in paragraph 4.2.

[25] Such an example is Swisskey, a certification authority sponsered by two leading Swiss banks, the former Swiss Telecom monopoly and a union of the chambers of commerce of the cantons (see SWISSKEY 1999).

[26] This would however lead to a further level where theoretically the same game would start again.

formal obligation is applied for most civil law contracts. For several legal acts national regulations stipulate, however, the written form with a handwritten signature.[27] All these transactions will only be legally binding in its electronic form, when the digital signature has the same legal status as the handwritten signature. The same is true for the recognition of electronic signatures as proof in trade disputes in a state court.[28]

In the same way as the state requests the fulfillment of certain formalities[29] for a handwritten signature to assure its validity in court, it is to be expected that the legislator sets up certain standards for digital signatures if they are to be equally binding as the traditional ones. Therefore the justification for activities of the state in the area of digital signature consists of the formal recognition of the equivalence of electronic and handwritten signatures and of the definition of standards that are to be fulfilled by the electronic signatures. In reality the state itself certifies the digital signatures of those certification authorities that issue certificates which fulfill the standards of the state.

One Problem that always arises with the definition of national standards is the recognition of digital signatures that are accepted in other countries. The problem of trust is comparable to that of the traders vs. the trustworthiness of the certification authorities. Here as well several solutions are conceivable:

a) Bilateral agreements are concluded by which the states recognize electronic signatures on a mutual basis. These are subject to governmental regulation.
b) The states try to coordinate their standards on an international level, e.g. via a supranational organization.

4.5. Summary

The emergence of private certification authorities can solve the problem with trust that originated because of the disparity between authenticity and identity. Also the problem of reliability of these certification authorities is conceivable on a private level and exists in

[27] Over 3000 of such legal acts exist in the German national regulations (see KUNER & MIEDBRODT 1999: 6, footnote 20).

[28] See the illustration of BAKER & HURST (1998:266): „Imagine A wishes to sell Blackacre for $5000 and publishes an offer to sell his property to the first person who submits a ‚signed and binding acceptance of this offer.' B accepts the offer using an email and his digital signature. Another bidder then submits a hand-written and hand-signed offer to pay $6000. Is A bound by B's acceptance because it came first? Or can he refuse to accept a digitally signed bid?"

[29] Among others specifically a hand-written signature in contrast to a copied, stamped or faxed signature (see e.g. the corresponding German paragraphs in the law and court decisions in KUNER & MIEDBRODT 1999:6).

reality thanks to the mechanisms presented in chapter 4.3.1. The existing rules of the game are sufficient to stop the uncertainty-problems. It can be expected that new rules that affect this area will find no majority.

In the existing national regulations, there are, however, clauses that demand the written form for a transaction to be valid. To enable Electronic Commerce, a change in the existing framework of rules is necessary:[30] Either the obligation to use the written form is removed from all corresponding paragraphs, or the digital signature gets the equivalent status as the handwritten signature. Under the (simplified) assumption, that the rules were mutually agreed upon, it can be expected that the introduction of the equivalence of handwritten and electronic signatures will be accepted and this equivalence established as new rule . Such an acceptance, however, will depend on whether this equivalence will be accepted by all those involved, but also on other factors such as freedom from discrimination of the rule[31] or its recognition in other legal systems, etc.

In the next chapter a rough outline is given of three approaches for actual regulations in this field.

5. SURVEY OF SOME EXISTING APPROACHES FOR REGULATION

The clearance of the Internet in 1991 for private commercial offering of electronic services was the starting point for Electronic Commerce.[32] Owing to the asymmetric encryption technique it was possible to guarantee for the authenticity of transmitted data. In the middle of the nineties the first commercial services for certification came into being in order to safeguard the identity of the electronic signer. Soon also public authorities realized that in the foreseeable future electronic trade would play a prominent role in the economy. In several declarations of intent it was made known which role they would like to take over in developing the corresponding institutional frame.[33] Since then different legislators have become active and promulgated new regulations especially in the field of digital signatures.

---

[30] In analogy to this is the validity e.g. for the recognition of digital signatures in litigation in court.

[31] A regulation on which a consensus could not be found, was in the original law for digital signatures of the US-state of Utah. This restricted the liability of certification authorities licensed by the state. The non-licensed authorities on the other hand were fully liable. See BAKER & HURST (1998: 268). These two authors comment the situation in a correct way: "If Utah becomes the norm, the freedom to act as a certificate authority without a state license may be illusory".

[32] See OECD (1999: 9).

[33] See CLINTON & GORE (1997), MITI (1997), EU-COMMISSION (1997).

The objective of the following paragraphs is not to provide a detailed analysis of the intentions and effects of the three presented approaches for regulation. Rather an impression shall be given of how such approaches work in reality and of the rapid developments that are taking place at present. For that purpose those rules and guidelines of the USA, the EU and Germany regarding the electronic signature, will be looked at.

5.1 USA

In July 1997 the US-Administration published a "Framework for Global Electronic Commerce" (CLINTON & GORE 1997) in which the principles are set forth according to which the legislative challenges of the electronic trade will be handled; also concrete themes which shall be dealt with, are specified. The first of these principles is "The private sector should lead" (CLINTON & GORE 1997:2);[34] in the comment it is said among others "Innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry"(ibid.).[35]

As expected it also contains the formulation of the following statement which deals with the security of data and with digital signatures: "The Administration, in partnership with industry, is taking steps to promote the development of market-driven standards, public-key management infrastructure services and key recoverable encryption products" (ibid. 15).

In the USA a multitude of laws for digital signatures existed for the individual states.[36] This situation was terminated by the "ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT" signed by president Clinton on July 30, 2000. The essence of the new law, which was enacted on October 1, 2000, is granting an equal status to the electronic signature with the handwritten signature and the setting of standards which must be fulfilled in electronic transactions. It also eliminates restrictive regulations in some states which for

[34] The remaining four are: "Governments should avoid undue restrictions on Electronic Commerce", "Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce", "Governments should recognize the unique qualities of the Internet", "Electronic Commerce over the Internet should be facilitated on a global basis" (CLINTON & GORE 1997: 2f).

[35] In the field of data protection this principle presents itself as follows: "We [the Administration] believe, that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy" (CLINTON & GORE 1997: 14).

[36] GIDARI ET AL. (1998) speak of an ″inconsistent state regulation and an absence of standards for the cross-border recognition of electronic signatures″. Cf. also BAKER & HURST (1998).

instance required a certain security technique. The standards of the law of June 30 originate to a good deal of concessions in favour of consumer organizations, which had opposed the law for a long time.[37]

5.2 European Union

In 1997 also the EU issued a basic declaration[38] on its intentions concerning activities to be undertaken and principles to be followed. The objective of the initiative is "the strong promotion of electronic trade in Europe" (EU-COMMISSION 1997:6). For that purpose the EU would like to take an active part in providing among other things a "favourable regulatory framework" (ibid. 21 ff) as well as a "favourable business environment" (ibid. 30 ff). Contrary to the American declaration of intent of CLINTON & GORE (1997), the EU considers the creation of the necessary regulations as being its task as well as a well-aimed encouragement of electronic trade, e.g. by means of pilot projects.[39]

The digital signature is addressed at different occasions. It is said that its legal recognition in the internal markets as well as the establishment of minimum criteria for the certification authorities are important. Further, global agreements should be necessary concerning digital signatures (EU-COMMISSION 1997:27). The realization of these requests occurred on December 13, 1999, with the "DIRECTIVE ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES". Article 16 of the arguments which precede the actual legal text summarizes the main points of the EU-Directive in a perfect way:

> "This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognized."

The Directive defines amongst other things the requirements for qualified certificates in several appendices and qualified institutions offering certification services (certification

[37] See LERNER (2000), EILPERIN & SCHWARTZ (2000).
[38] See EU-COMMISSION (1997)
[39] Thus e.g. page 28 of the EU-Communication "A European Initiative in Electronic Commerce" (COM (97) 157) of April 15, 1997, reads: "Best practice pilot projects play an important role in raising awareness." They are designed especially to draw the attention of enterprises to the new possibilities.

authorities). If a certificate does comply with these requirements the respective signature must have the same legal effect as a handwritten signature. If a certification authority complies with the respective requirements it should be entitled to issue qualified certificates. In addition electronic signatures originating from other EU-countries and being considered as qualified, must also be accepted as a qualified signature in the country in question (country of origin principle).[40] The Directive makes no mention of how to deal with corresponding electronic signatures from Non-EU-Countries.

The Directive which had to be integrated into the national legislations of the member states by mid 2001, contains the hitherto existing experiences of the national legislations. Especially countries with relatively restrictive regulations will have to adjust their laws to the liberal provisions of Brussels.[41]

5.3 Germany

Germany has one of the most ancient laws for the regulation of the digital signature (SIGG). It consists of article 3 of the "GESETZ ZUR REGELUNG DER RAHMENBEDINGUNGEN FÜR INFORMATIONS- UND KOMMUNIKATIONSDIENSTE" of July 22, 1997, and of the „VERORDNUNG ZUR DIGITALEN SIGNATUR" (SIGV) of October 23, 1997, which followed it. According to § 1, alinea 1, it is the purpose of the law "to create general conditions for digital signatures to guarantee their safety […]".

Typical of the German law for signatures is the duty to obtain an authorization for operating a certification authority which is laid down in § 4.[42] The competent authority is the "REGULIERUNGSBEHÖRDE FÜR TELEKOMMUNIKATION UND POST" (REGTP). Only somebody complying with the restrictive criteria in the sector of personnel, technical components and security can expect to obtain a respective concession of the REGTP.[43] On the other hand the applying institution will then obtain certification of the highest level.

The German regulation provides the possibility to offer or to acquire officially recognized certificates, but at the same time does not yet consider the respective signatures as being

[40] See Article 7, paragraph 1.
[41] See BAKER & YEO (1999: 13), or paragraph 5.3.
[42] § 4, alinea 1, of SIGG: "The operation of a certification authority needs the approval of the competent public authority. This has to be granted on request."
[43] See the respective provisions in the SIGG and in the SIGV as well as REGTP (no year: 12).

equivalent to handwritten ones. This lack of motivation for using electronic signatures together with very restrictive regulations for operating an authority for certification may explain that up to now there are only three officially admitted certification authorities.[44] In spite of the de facto licence requirement,[45] numerous firms[46] offer certificates for digital signatures; however they inform their clients that these certificates are not yet within the law. At the same time they refer to the EU-Directive which has to be integrated into German law and then would render also their certificates legally valid.

A first step in direction of this broader accessibility has been planned for the first semester of 2001. On August 16, 2000, the federal cabinet passed a bill on general conditions for electronic signatures, which should be agreed to by the Bundestag in fall. In trying to comply with the instructions of the EU-Directive the federal cabinet lowers the demands for the electronic signature and abolishes the licence requirement for certification authorities. Among other things also the country of origin principle of the EU is recognized for the acceptance of foreign electronic signatures and therefore newly included into the law. But what is still missing in Germany even after enforcement of the new SigG and notwithstanding the obligation according to the EU-Directive to do so, is the acknowledgement of the equivalency between handwritten and electronic signature. A bill for adjusting the formal provisions of the private law to the Electronic Commerce is in process.[47]

6. FINAL REMARKS

On a private level commerce via Internet institutionally has no obstacles with respect to the security about the identity of the transaction partner. More important, a barrier for getting into Electronic Commerce are high information costs because of the rapidly developing technique and the application of the new possibilities. Part of these high information costs are the missing common business practices which were the reasons most quoted in the polls mentioned in chapter 2.

---

[44] The certification authority of the "Deutsche Telecom AG" (http://www.telesec.de/), of the "Deutsche Post" (http://www.signtrust.de/start.htm/) and of the "Bundesnotarkammer" (http://www.bnotk.de/). The first two administrate only 20'000 certificates (see KRÄGENOW (2000)). "Verisign" on the other hand, domiciled in the USA, the market leader in the field of digital certificates administrates 4 millions certificates (see http://www.verisign.com/about/index.html).

[45] Also the German SIGG provides in §1, alinea 2, a loophole for the operation of non-licensed certificates authorisations: "The application of other procedures for digital signatures is free, as long as according to this law digital signatures are not stipulated by law". But BAKER & YEO (1999: 13, especially footnote 15) refer to a discrepancy with §13, alinea 4, which renders §1, alinea 2, non-applicable.

[46] An example is the firm "TC TrustCenter GmbH" in Hamburg (http://www.trustcenter.de/).

[47] See Press release of the BUNDESMINISTERIUM FÜR WIRTSCHAFT UND TECHNOLOGIE of August 16, 2000.

As far as state regulations are concerned we have at present a "phase of consolidation". In the EU as well in USA the individual laws for the digital signature are coordinated by means of centralized regulations. This does not eliminate the competition for the most suitable solution but at least partly shifts it one step upwards.[48] It may be expected that this process of search for the suitable rules on state level will continue, parallel to the technical development.[49] However, it is evident that a framework of rules which permanently is changing, is no optimal condition for legal security and trust amongst those affected. Here too, the present scepticism of many of the potential participants in Electronic Commerce is understandable.

Theoretically the institutional prerequisites for the "breakthrough" for a secure trade via the Internet are available. Therefore, in the foreseeable future – NORTH's three-stage model for the development of exchange of goods (cf. chapter 2) –the third stage with low production costs and low transaction costs will be reached in Electronic Commerce, too.

How will this continue? What today still seems to be troublesome and complicated will be a natural thing tomorrow. The framework of rules will become consolidated and the business practices will get going. It will be an exciting task to follow up this process on all levels.

APPENDIX

The security problems directly linked to the Internet may be divided into four categories:[50]

- **Confidentiality**

  Information which is sent via the Internet and which is confidential must be safeguarded against inspection by third parties.

[48] Cf. with respect to the competition for a suitable framework of rules for the Electronic Commerce e.g. the passage in the EU-Directive for Electronic Commerce (EU-COMMISSION 1990: 3): "Europe's main competitors have already resolutely seized opportunities offered by Electronic Commerce - with the USA building a substantial lead". Similarly, it is said in a corresponding publication of the Japanese Ministry for Trade and Industry: "However […! the introduction of Electronic Commerce in Japan lags behind those efforts of the United States in particular, due to restrained investment in information technology after the bursting of the economic bubble" (MITI 1997: 1).

[49] Since May 1, 2000, Switzerland has enforced a "VERORDNUNG ÜBER DIENSTE DER ELEKTRONISCHEN ZERTIFIZIERUNG",which in its Article 1 is called explicitly a "test regulation". The intent of the legislator is to gain experience useful for subsequently being incorporated into a law the draft of which is presently being evaluated by the Swiss parliament.

[50] See e.g. GREENSTEIN & FEINMANN (1999: 228f).

- **Integrity**

  By guaranteeing the integrity of the data it should be ensured that the message sent off is identical with the message arriving at the addressee, i.e. that on its way nobody could alter anything.

- **Authenticity**

  In exchanging electronic messages it is of crucial importance to know, whether the sender is indeed the one which he claims to be, i.e. his identity must be verifiable.

- **Non-Repudiation**

  It must be prevented, that the existence of an obligation can be denied notwithstanding its real availability. It also must be ensured, that a message is actually sent off (proof of origin); this avoids that the sender later on may claim never having given the order. Then the receiver has to confirm that he obtained the message (proof of receipt), in order to be made liable for eventually not having carried out the order. Finally, a proof of content is needed to give evidence for what exactly the content of the message was.

In a first step these problems may be solved by encrypting the data to be transmitted. Here the data are put in a form by means of a mathematical algorithm which can be decrypted to the original state only by somebody having the corresponding key. It must be distinguished between symmetrical and asymmetrical encryption, the latter better known as "public key"-procedure.[51]

With **symmetrical encryption methods** the same key is used for encrypting and decrypting. The problem with the symmetrical encryption is the safe exchange of the keys.

With **asymmetrical encryption methods** we have a private, i.e. secret key, and a public key which is accessible to everybody. If the sender would like to transmit a confidential message to the receiver, he will encrypt this message with the public key of the receiver and forward it to him. The message encrypted in that way may be decrypted only with the private key which matches the public key. This means that the receiver has to decrypt the encoded text sent to him with the private key known only to him.

[51] Independent of the kind of encryption, the length of the key (expressed in Bit) is considered as a degree of the security thereof. The faster the computer hardware, the longer the key has to be for decoding. The requirements necessary for decoding would then not be worth the effort. At present (2001) 128 Bit-encryption is considered to be secure.

Via the encryption of a message with the public part of a key **confidentiality** may be established, because it is guaranteed that only the owner of the private part of the corresponding key will be able to decrypte the message.

If the keys are used in the reverse sequence, i.e. the message is encrypted by the sender with his private key, then (at least technically) **authenticity** is guaranteed because nobody else could produce an encoded message which could be decrypted with the corresponding public part of the key. However, the confidentiality is no longer guaranteed because the encrypted message could be decrypted by everybody by means of the public key.

The most widely used method to guarantee the **integrity** of the data is the so-called Hashing. Here the entire message is represented by means of a suitable arithmetic instruction in a Hash-value.[52] This value is attached to the actual message and transmitted along with it. After the arrival of the message, the Hash-value is calculated a second time, now by the receiver. If the transmitted and the calculated value are identical, it may be assumed that the message was not changed.

A great deal of the problems mentioned initially can be removed by the application of suitable combinations of the procedures described above for the data to be sent off (cf. Table 1). In this context the so-called digital signature is of special importance.

Security Problem	Encryption (Sender)	Decryption (Receiver)	
Confidentiality	Public Key of the Receiver	Private Key of the Receiver	
Integrity	Calculation of the Hash-Value	Calculation of the Hash-Value and Comparison	} Digital Signature
Authenticity	Private Key of the Sender	Public Key of the Sender	
Non-Repudiation[53]	Generation of the Digital Signature	Decoding of the Digital Signature	

Table 1: Application of cryptographic procedures as a contribution to the solution of problems of security with Electronic Commerce

For the generation of a **digital signature**, in a first step the Hash-value of the message is calculated. In a second step this Hash-value is encrypted with the private key of the sender.

[52] This Hash-value, also called "digital fingerprint", has a length of 128 bit, which corresponds to the information content of 16 letters. If in the whole message only one single Bit is changed, the calculated Hash-value is changed too.

[53] Here in addition the so-called "Timestamps" may be used, which document the exact time of sending off and of arrival, or "Confirmation Services" which automatically confirm the arrival.

The result of this procedure represents the digital signature, a unique combination of the content of a message with the private key of the sender. The receiver also calculates as a first step the Hash-value of the arrived message. Then by means of the public key of the sender he encrypts the digital signature which was received along with the message; thus the Hash-value is obtained, which characterized the message of the sender. If both Hash-values are identical, the receiver may be sure that the message was indeed encrypted with the private key of the sender (authenticity) and that its content has not been changed (integrity).[54]

[54] If additional confidentiality is required the integral message has to be encrypted by the sender as well by means of the public key of the receiver. A new encryption of the digital signature is not necessary, because the Hash-value does not allow insight into the content of the message.

REFERENCES

BACCHETTA, MARC; LOW, PATRICK; MATTOO, AADITYA; SCHUKNECHT, LUDGER; WAGNER, HANNU; WEHRENS, MADELON (1998): Electronic Commerce and the Role of the WTO. Special Studies 2. Geneva: WTO.

BAKER, STEWART A. & HURST, PAUL R. (1998): The Limits of Trust: Cryptography, Governments, and Electronic Commerce. The Hague: Kluwer International.

BAKER, STEWART & YEO, MATTHEW (1999): Survey of International Electronic and Digital Signature Initiatives. Internet Law & Policy Forum (ILPF) (http://www.oecd.org/dsti/sti/it/ secur/act/wksp_ilpf.pdf).

BUNDESMINISTERIUM FÜR WIRTSCHAFT UND TECHNOLOGIE (2000): Pressemitteilung vom 16. August 2000. (http://www.bmwi.de/presse/2000/0816prml.html).

CLINTON, WILLIAM J & GORE ALBERT (1997): Framework for Global Electronic Commerce. Washington. (http://www.ecommerce.gov/framewrk.htm).

EGGS, HOLGER & ENGELERT, JÜRGEN (2000): Electronic Commerce Enquête 2000. Empirische Untersuchung zum Business-to-Business Electronic Commerce im deutschsprachigen Raum. Computer Zwitung, Leinfelden-Echterdingen; Institut für Informatik und Gesellschaft, Albert-Ludwigs-Universität Freiburg.

EILPERIN, JULIET & SCHWARTZ, JOHN (2000): "Electronic Signature Bill Passes the House." The Washington Post, 15. Juni 2000.

ELSNER, WOLFRAM (1987): “Institutionen und ökonomische Institutionentheorie. Begriffe, Fragestellung, theoriegeschichtliche Ansätze”, WiSt, Vol. 16, Heft 1, 5 - 14.

EU-KOMMISSION (1997): A European Initiative in Electronic Commerce of April 15, 1997 (COM (97) 157). (http://www.cordis.lu/esprit/src/ecomcom.htm).

GIDARI, ALBERT; MORGAN, JOHN P.; COIE, PERKINS (1998): Update: Survey of Electronic and Digital Signature Legislative Initiatives in the United States. Internet Law and Policy Forum. (http://www.ilpf.org/digsig/update.pdf).

GREENSTEIN, MARILYN & FEINMAN, TODD M. (2000): Electronic Commerce. Security, Risk Management and Control. Boston: Mc Graw Hill.

KRÄGENOW, TIMM (2000): "Bundesregierung fördert die digitale Unterschrift." Financial Times Deutschland, 16. August 2000.

KUNER, CHRISTOPHER & MIEDBROD, ANJA (1999): Written Signature Requirments and Electronic Authentication: A Comparative Perspective (http:/www.oecd.org/dsti/sti/it/ secur/act/wksp_kuner.pdf).

KURBEL, KARL & TEUTEBERG, FRANK (1998): Betriebliche Internet-Nutzung in der Bundesrepublik Deutschland - Ergebnisse einer empirischen Untersuchung. Arbeitsbericht des Lehrstuhls für Wirtschaftsinformatik der Europa-Universität Viadrina, Frankfurt (Oder).

LERNER, DAN (2000): "E-Signature Given Legal Status." Financial Times, 14. Juni 2000.

MESENBOURG, THOMAS L. (1999): Measuring Electronic Business: Definitions, Underlying Concepts, and Measurement Plans. US Census Bureau. (http://www.census.gov/epcd/ www/ebusines.htm).

MILGROM, PAUL R.; NORTH, DOUGLASS C.; WEINGAST, BARRY R. (1990): "The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs." Economics and Politics, Vol. 2, 1 - 23.

MITI (1997): Towards the Age of the Digital Economy. For Rapid Progress in the Japanese Economy and World Economic Growth in the 21st Century. (Draft). Ministry of International Trade and Industry, Japan. (http://www.miti.go.jp/intro-e/a228101e.htm bzw. http://www.gip.jipdec.or.jp/~hirai/fujimori/digital02-e.html).

MÜLLER, GÜNTER & SCHODER, DETLEF (1999): Electronic Commerce - Hürden, Entwicklungspotential, Konsquenzen. Ergebnisse aus der Electronic Commerce Enquête. Arbeitsbericht Nr. 137 des Instituts für Informatik und Gesellschaft/Telematik der Universität Freiburg i. Br.

NORTH, DOUGLASS C. (1990): Institutions, Institutional Change and Economic Performance. New York: Cambridge University Press.

OECD (1999): The Economic and Social Impact of Electronic Commerce. Preliminary Findings and Research Agenda. Paris: OECD.

REGTP (o.J.): Die digitale Signatur. Regulierungsbehörde für Telekommunikation und Post (http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/10.pdf).

SCHMIDT-TRENZ, HANS-JÖRG (1990): Aussenhandel und Territorialität des Rechts. Grundlegung einer Neuen Institutionenökonomik des Aussenhandels. Baden-Baden: Nomos.

SMEDINGHOFF, THOMAS J. (1998): ABA/ACCA Survey of Electronic Commerce Practices. Summary of Results. American Bar Association, Science and Technology Section, (http://www.abanet.org/scitech/abbaacca.html).

STRAUSS, RALF & SCHODER, DETLEF (2000): e-Reality 2000 - Electronic Commerce von der Vision zur Realität. Status, Entwicklung, Erfolgsfaktoren und Management-Implikationen des Electronic Commerce. Consulting Partner Group GmbH, Frankfurt.

SWISSKEY (1999): Certification Practice Statement. (http://www.swisskey.ch/pdf/cps2.1_d.pdf).

VANBERG, VIKTOR J. (1996): Ökonomische Rationalität und politische Opportunität. Zur praktischen Relevanz der Ordnungsökonomie. Lectiones Jenenses. Heft 8. Jena: Max-Plank-Institut zur Erforschung von Wirtschaftssystemen.

VANBERG, VIKTOR J. (1997): "Die normativen Grundlagen von Ordnungspolitik." ORDO, Vol. 48, 707 - 726.

VERISIGN (1999): Certification Practice Statement. (https://www.verisign.com/repository/CPS1.2/CPS1.2.pdf).

LEGAL TEXTS

Germany

GESETZ ZUR DIGITALEN SIGNATUR (SIGG) vom 22. Juli 1997.

VERORDNUNG ZUR DIGITALEN SIGNATUR (SIGV) vom 22. Oktober 1997.

ENTWURF EINES GESETZES ÜBER DIE RAHMENBEDINGUNGEN FÜR ELEKTRONISCHE SIGNATUREN UND ZUR ÄNDERUNG WEITERER VORSCHRIFTEN in der Fassung des Kabinettsbeschlusses vom 16. August 2000.

EU

DIRECTIVE ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES (1999/93/EC) of December 13, 1999.

Switzerland

VERORDNUNG ÜBER DIENSTE DER ELEKTRONISCHEN ZERTIFIZIERUNG vom 12. April 2000.

USA

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT of June 30, 2000.

FREIBURGER DISKUSSIONSPAPIERE ZUR ORDNUNGSÖKONOMIK
FREIBURG DISCUSSION PAPERS ON CONSTITUTIONAL ECONOMICS

98/1 **Vanberg, Viktor J.**: Markets and Regulation – On the Contrast Between Free-Market Liberalism and Constitutional Liberalism. Published in: Constitutional Political Economy Vol. 10 No. 3, October 1999, p. 219 - 243.

98/2 **Pejovich, Svetozar**: Toward a Theory of the Effects of the Interaction of Formal and Informal Institutions on Social Stability and Economic Development.

99/1 **Vanberg, Viktor J.**: Standortwettbewerb und Demokratie.

99/1A **Vanberg, Viktor J.**: Globalization, Democracy and Citizens' Sovereignty: Can Competition Among Governments Enhance Democracy? Published in: Constitutional Political Economy, Vol. 11, No. 1, March 2000, p. 87-112.

99/2 **Vanberg, Viktor J.**: Ordnungsökonomik und Ethik. Zur Interessenbegründung von Moral. Veröffentlicht in: B. Külp, V. J. Vanberg (Hrsg.): Freiheit und wettbewerbliche Ordnung, Haufe Verlagsgruppe: Freiburg, Berlin, München, 2000, S. 579-605.

99/2A **Vanberg, Viktor J.**: Constitutional Economics and Ethics – On the Relation Between Self-Interest and Morality.

99/3 **Cassel, Susanne**: Die Rolle von Think Tanks im US-amerikanischen Politikberatungs-prozess.

00/1 **Sideras, Jörn**: Systems Competition and Public Goods Provision. Published in: Jahrbuch für Neue Politische Ökonomie, Band 19, Tübingen: Mohr Siebeck, 2000, S. 157 - 178.

00/2 **Vanberg, Viktor J.**: Markets and the Law.

00/3 **Vanberg, Viktor J.**: F.A. von Hayek.

00/4 **Vanberg, Viktor J.**: Der konsensorientierte Ansatz der konstitutionellen Ökonomik. Veröffentlicht in: H. Leipold, I. Pies (Hrsg.): Ordnungstheorie und Ordnungspolitik - Konzeptionen und Entwicklungsperspektiven, Schriften zu Ordnungsfragen der Wirtschaft, Band 64, Stuttgart, 2000, S. 251-276

00/5 **Vanberg, Viktor J.**: Functional Federalism: Communal or Individual Rights? On B. S. Frey's and R. Eichenberger's Proposal for a "New Federalism". Published in: KYKLOS, Vol. 53, 2000, p. 363-386

00/6 **Zoll, Ingrid:** Zwischen öffentlicher Meinung und ökonomischer Vernunft: Individuelle Meinungen über Globalisierung und Wettbewerb.

01/1 **Sideras, Jörn:** Konstitutionelle Äquivalenz und Ordnungswahl.

01/2 **Märkt, Jörg:** Knut Wicksell: Begründer einer kritischen Vertragstheorie?

01/3 **Hansueli Stamm:** Institutioneller Rahmen des Electronic Commerce: Eine ordnungsökonomische Analyse am Beispiel der digitalen Signatur.

01/3A **Hansueli Stamm:** Institutional Framework of Electronic Commerce: A Constitutional Economic Analysis of the Problems With Digital Signatures.

01/4 **Viktor J. Vanberg:** Evolutorische Ökonomik: Homo Oeconomicus, Markt und Institutionen.

01/5 **Viktor J. Vanberg:** Rational Choice vs. Program-based Behavior: Alternative Theoretical Approaches and their Relevance for the Study of Institutions.

01/6 **Viktor J. Vanberg:** Citizens' Sovereignty and Constitutional Commitments: Original vs. Continuing Agreement.