Governing Legal Identities
Lessons from the History of Seals and Signatures

Prof. Dr. iur. *Bernd Lutterbeck*, Dipl.-Inform. *Kei Ishii*, Dipl.-Inform. *Robert A. Gehring*

Technical University of Berlin

Departement of Computer Science and Society

«Internet Governance» Working Group

Abstract

In this paper we present the thesis that digital signatures failed to meet the expectations set in their success because of a "cultural gap". This "cultural gap" exists between the needs of the people living in cyberspace and the assumptions of the advocates of digital signatures. In our research we try to identify this "cultural gap". Therefor we investigate different areas of technology-based social interaction with and without authentication and identification.

We discuss three case studies from our recent research: The Japanese culture of seals; The role of seals and signatures in the Middle Ages. Following the historical description of the means and constraints of identification and authentication we make the step into the cyberspace and discuss the needs of identification and authentication in the virtual world with the example of 'ebay'.

We go further and show new directions in governing legal identities in the cyberspace. Our summary goes that the use of digital signatures makes sense - in some contexts. Other contexts of human activities in the cyberspace simply don't need strong authentication in the way digital signatures provide it: A well-tempered risk management strategy within an self-regulated environment does the job and allows people to cooperate successful.

Note: This paper contains the full version of the presentation given a the Information Security Solutions Europe Conference (ISSE) 2000 in Barcelona on September 28, 2000.

About the Authors

Prof. *Bernd Lutterbeck* is lawyer and professor for computer science and society at the Technical University of Berlin. He is "Jean Monnet Professor" of the European Union. *Kei Ishii* and *Robert Gehring* are assistant lecturers with Prof. Bernd Lutterbeck. Both hold a degree in computer science from the Technical University of Berlin. *Robert Gehring* also works as an independant consultant. Together they form the "Internet Governance" working group. The aim of their research are the current developments in the fields of regulation and self-regulation in the information society, problems of internet governance and electronic commerce as well as legal developments with the focus on intellectual property. Their publications are in part available online at http://ig.cs.tu-berlin.de/wir/impressum.html. The authors can be reached via email: mailto:sekr@ig.cs.tu--berlin.de.

Survey and Introduction

In the European Union the first laws on Digital Signatures were enacted some time ago. The once high expectations in the success of the digital signature have not been met. Digital signatures do not play a significant role neither on the internet nor elsewhere. Thorough examinations lead us to recognize at least three levels of difficulties:

* **Issues of regulation and governance**
  The chosen legal, technical and social instruments do not provide adequate means. The current state is far away from good governance. Digital signatures lack broad implementation and application.

* **Issues of user acceptance**
  Cultural constraints have in far been overlooked yet - with more constraints in the one culture and less in the other. For example the concept of 'identity' is a cultural construct. On the internet for example one can have more than a single identity. An approach to governance of identities has to respect this fact.

* **Issues of long term stability and reliability**
  Long term stability and reliability require both user acceptance and «good governance». One without the other must fail. We may think of 'long term stability' as of 'long term usability'. A signature has 'long term reliability' if it keeps its reliability over times even under changing conditions.

We present the following thesis:

> ***The high expectations in the legislation of digital signatures have not been met due to regulative incompatibilities and cultural misunderstandings. Large parts of our society do not provide the culture that digital signatures according to law require to be successful. That is even more true on the internet.***

We try empirically to substantiate this thesis. The chosen examples provide clues to the variety of possible solutions to the problem of «governing identities». Solutions do not have to be of legal nature. The different case studies show the dependencies of the solution on their cultural constraints. Successful solutions respect their constraints and implement more than just technical and/or legal approaches.

From our research we present three examples of the historical and contemporary practice..

* Our first example describes the Japanese culture of seals and its roots in history. In Japan seals together with registration certificates play the role that signatures play in Europe and almost all other countries. This situation is well suited to adopt digital signatures.

* Our second example sketches the historical ancestors of handwritten signatures on paper, and how signatures superseded the older system of seals.

* In our third example we turn towards the internet. We examine the role legal identities and social self-regulation play at 'ebay'. 'ebay' is the largest auction platform in the world, not only on the internet.[1] 'ebay' enables a multi-billion dollar business without digital signatures.

We can learn from the examples that social interaction -even legal interaction- is possible without strong authentication and identification. We emphasize that human interaction on the internet is more than commercial interaction.

The promising example of Japan may be proof of the thesis that digital signatures as a means of identification and authentication are appropriate where the cultural is familiar with comparable means. The old culture of seals in Japan supplies a suitable ground to build on. It takes only a small step to go over from seals and certificates on paper to seals and electronic certificates. The Japanese enthusiasm for new technologies gives an advantage, too.[2]

Our research give us hints that the situation on the internet shows some similarities to the medieval culture. The circumstances in the Middle Ages and those on the internet have in common that national borders do not exist. Competing laws and rules are applied to different aspects of live. There is no such thing as a unique identitiy out of context. The infrastructure is somewhat unreliable. Most activites take place in communities[1] with rules of their own. Centralized regulation is an exception.

In the Middle Ages contracting involved witnesses. Thus the risk of administrative failure was spread. The memory of the witnesses provided sufficient long term reliability. The idea of having witnesses to assist commercial transactions on the internet might be worth of further discussion. 'ebay' implemented a system for witnessing of reputation. That system is the basis of self-regulation inside the 'ebay community'. To us, 'ebay' seems to be an example of 'good governance'.

---

[1] We use the term "community" to point to the similarities between the medieval social structure and the "Virtual Communities" described first by *Howard Rheingold*[3].

We conclude with two recommendations:

1. More attention should be given to the strengths of the community concept and its culture.

2. Before digital signatures can succeed, an appropriate culture has to be developed.

One thing is to point to: The meanings of terms such as *identity* and *authenticity* change over times. That should not be neglect. Not every period of time had a concept of identity or authenticity. Or even if there was such a concept the meaning could have been strictly opposite to our modern appreciation. One should keep this in mind if in the following sections *identity* and *authenticity* are used sometimes in an unfamiliar way.

First Example: Seals in Japan

Introduction

In Japan seals take the place that signatures have in our culture. In the first part of this section we describe the contemporary use of seals in Japan. The second part gives a short historical survey.

Today seals in Japan play the role that signatures play in other countries. Official documents are sealed instead of being signed. Passports are sealed as are all other documents of every-day business. The seals are made of different materials and the use is that of a stamp, i.e. the seal is pressed on the paper.

A significant difference to our signature-based authentication system is that a person has more than one seal at its disposal. The use of the different seals depends on what is to be sealed. The context dictates the choice of seal.

Types of Seals in Japan

The most important seal is the '**jitsu-in**'. The '**jitsu-in**' is a personal seal. It is applied in all official matters such as documents attested by a notary, estate affairs, the registry of marriage, in credit matters etc.

Before a '**jitsu-in**' can be applied it needs to be registered with the local registration authority. The registration consists of the escrow of a seal print on a paper and the presentation of the personal identification card. The registration authority supplies the applicant with an official certificate. The seal and its accompanying certificate constitute the Japanese complement to our handwritten signature. A human being is allowed to register not more than one single '**jitsu-in**'. Other personal seals are not officially certified.

According to its importance in legal transactions the '**jitsu-in**' seal has to be kept in a secure way. The one who has the seal and the certificate at his disposal is able to do every legal transaction in the name of the owner.

A legal person as for example an enterprise owns a similar seal, the '**kaisha-jitsu-in**'. An additional seal, the '**sha-in**', is necessary to register the enterprise.

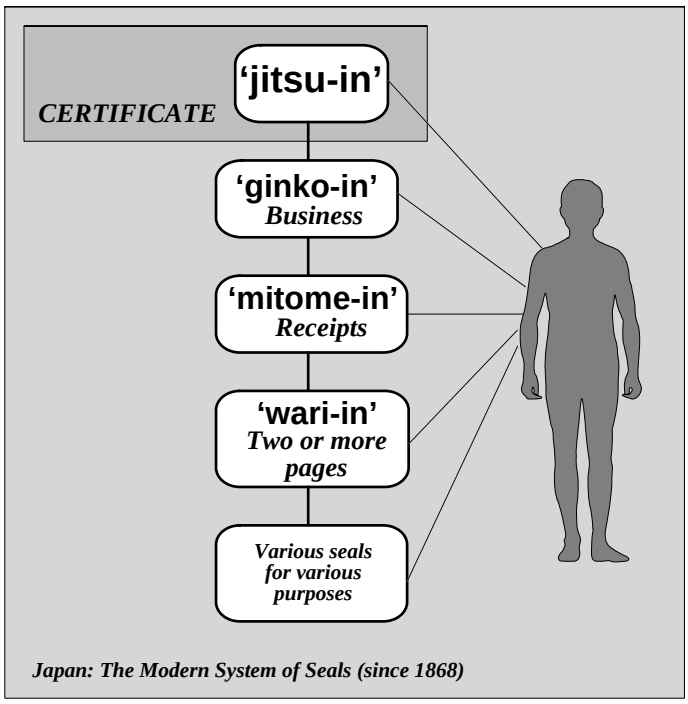
As we mentioned above a person owns more than one single seal. Depending on the character of the transaction the owner chooses the appropriate seal:

* For usual business on the bank a '**ginko-in**' is employed. Enterprises use their '**kaisha-ginko-in**' instead.

* Receipts for letters or parcels are sealed with the '**mitome-in**'.

* The so called 'split-seal', the '**wari-in**', is applied on documents consisting of several pages. The seal is pressed simultaneously on two pages of the document.

* There are more seals with a special meaning. Even seals for a certain kind of fun exist.



Japan: The Modern System of Seals (since 1868)

The seals are made of different materials. The really important seals (the ‘**jitsu-in**’, occasionally the ‘**ginko-in**’) are hand--made. Thus they are unique. The less important seals are industrial products of diffent quality. Such seals can be purchased for a small amount of money ‘just around the corner’.

The important seals are made of ivory, the horn of the water-buffalo or ebony. The ‘**jitsu-in**’ bears the symbol of his owners name. The symbols for the other seals can be chosen freely.

Some remarks on the history of Japanese seals

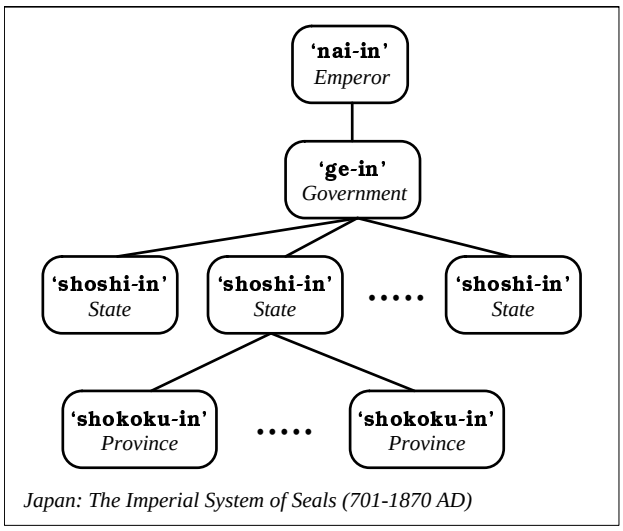
Both our modern signatures and the Japanese seals have a common ancestor: The Mesopotamian seal. In the 4th millennium BC seals were in introduced in Mesopotamia. These seals were pressed into the unburned clay of the ‘documents’. After the burning they were unremovable and thus authenticated the document.

From Mesopotamia seals found their way into the Chinese administration. This was the same time when the Chinese writing evolved. Japan learned the use of seals from the Chinese. The oldest Japanese seal we know of is a Chinese seal made of gold. In 57 AD it was given as a gift to the Japanese emperor by the Chinese emperor. Since about 550 AD seals have been produced in Japan. This age is also known as ‘borrowing from China’. The import of the Chinese writing is another aspect of this cultural influence.

The whole Japanese administration was reformed according to the Chinese model. This so called ‘taika reformation’ started in the year 701 AD. By that a hierarchical system of seals representing the hierarchy of power was introduced. At this point we can see a similarity to the system of seals with power that was in use in the medieval Europe.

In Japan the ancient system of seals was organized in four layers:

* The ‘**nai-in**’ was at the top. It was the seal of the emperor.
* Below it was the ‘**ge-in**’, the national seal. The ‘**ge-in**’ was applied to official documents of the government. It stayed in use until today. Some special documents require the use of this seal even today.
* On the next level below was the ‘**shoshi-in**’. It was used in the state administration.
* The ’**shokoku-in**’ belonged to the lowest layer. Its field of application was the provincial administration.



Japan: The Imperial System of Seals (701-1870 AD)

All these seals were emitted by the imperial court. The use of other seals was prohibited.

After the imperial system of seals gained authority and trust it became quite usual to use seals as a means of authentication and authorization. In spite of the prohibition more and more institutions had their own seals. Such institutions were temples, shrines, counties, villages etc.

Within the period of 800-1200 the power of the emperor eroded and shifted to local rulers. A system of independent seals substituted and complemented the hierarchical system of the imperial seals. Despite this development the imperial system nominally kept its position until 1870.

For a shorter period of time signatures came in use. The signatures had the advantage to be more individual. They could serve as a means of individual expression. A '**kao**', as they were called, could transmit the power of a warrior for example. A warrior made strong and thick strokes to sign. Members of the court painted thin and elegant lines.

Very sophisticated signatures were painted. As one can imagine such signatures required a reasonable amount of work. Instead of painting with the usual paintbrushes, every time a document was to be signed, seals were made bearing the image of the signature. '**Kaos**' as a means to sign got out of fashion and were substituted again by seals.

A curiosity should be mentioned. Between 1600 and 1868 a system of biometric seals served in matters of foreign trade. The imprint of a fingernail ('**tsume-in**') was used to authenticate human beings. Even persons unskilled in the Japanese writing could use this system. The possibilities to distinguish people through such fingernail seals seems to have been good enough for the times.

With the 'meiji-reformation' of 1868 administrative, legal, political and scientific achievements of the western powers were introduced to Japan. The imperial system of seals that was formally still in force was superseded by the modern system of seals and registration described at first.

Latest developments

The Japanese industry and government take efforts to transmit the established system of different seals (with and without registration) into the world of electronic commerce. There are legal developments and technological experiments that point to this direction. Tentatively the registration certificates are stored on a magnetic card and can be used in combination with the real seal. From patent applications of newer date (for example: U.S. Pat. 5,689,567: Electronic signature method and apparatus) one can conclude that part of the research is directed to the transmission of digitized seals into the internet.

Conclusion

The established system of seals is going to be adapted to the new requirements instead of being superseded. The system in force with its seals and certificates is well suited to adopt digital signatures. The success is likely.

Resources: [2], [18]

Second Example: Seals and Signatures in the Middle Ages

Apart from the internet, handwritten signatures on papers are today's most accepted means of authentication. At least we can say this about the European culture and the areas influenced by it. If we want to understand how this happened we have to go

back in history. The cornerstones can be identified in the Roman law and its medieval reanimation under the conditions of a system of competing powers.

In the early times of the Roman empire seals and witnesses were employed to authenticate legal transactions and contracts. Legal documents with respect to a legal transaction were sealed and carried the names of the witnesses, if they were made at all. Only a few legal transactions required legal documentation. Most transactions had the character of symbolic acts. Witnesses observed the act and later, in case of an argument, the witnesses were called to testify.

In the classic period the Romans made written documentations of legal transactions. In many cases notaries were involved. Different types of documents can be distinguished: the 'notitia', the 'chirographum' and the 'carta'. The concrete use of either depended on the respective kind of contract.

Legal documents were signed by the parties to the contract. In many cases witnesses such as notaries signed the contract too. And often witnesses were present to sign the contract. A prerequisite was that enough people were able to read, write and to distinguish the handwriting of different persons. In the case of an argument that was of great importance. Despite the use of signatures, seals did not lose their importance. Rather they were used in combination with the signatures to authenticate the documents.

After a few centuries the Roman culture declined and fell into poor conditions. The empire broke into parts and the immediate influence of the Roman law decreased. During the last centuries of the Roman empire the illiteracy grew. Signatures lost importance. Seals as an instrument that is useful even if one is illiterate stayed in use. But the scope of application became smaller.

With the transition into the early middle age only the highest offices, i.e. church offices and the royal chanceries, usually lead by clerics kept the Roman knowledge of written contracts. They served as readers, writers and translators.

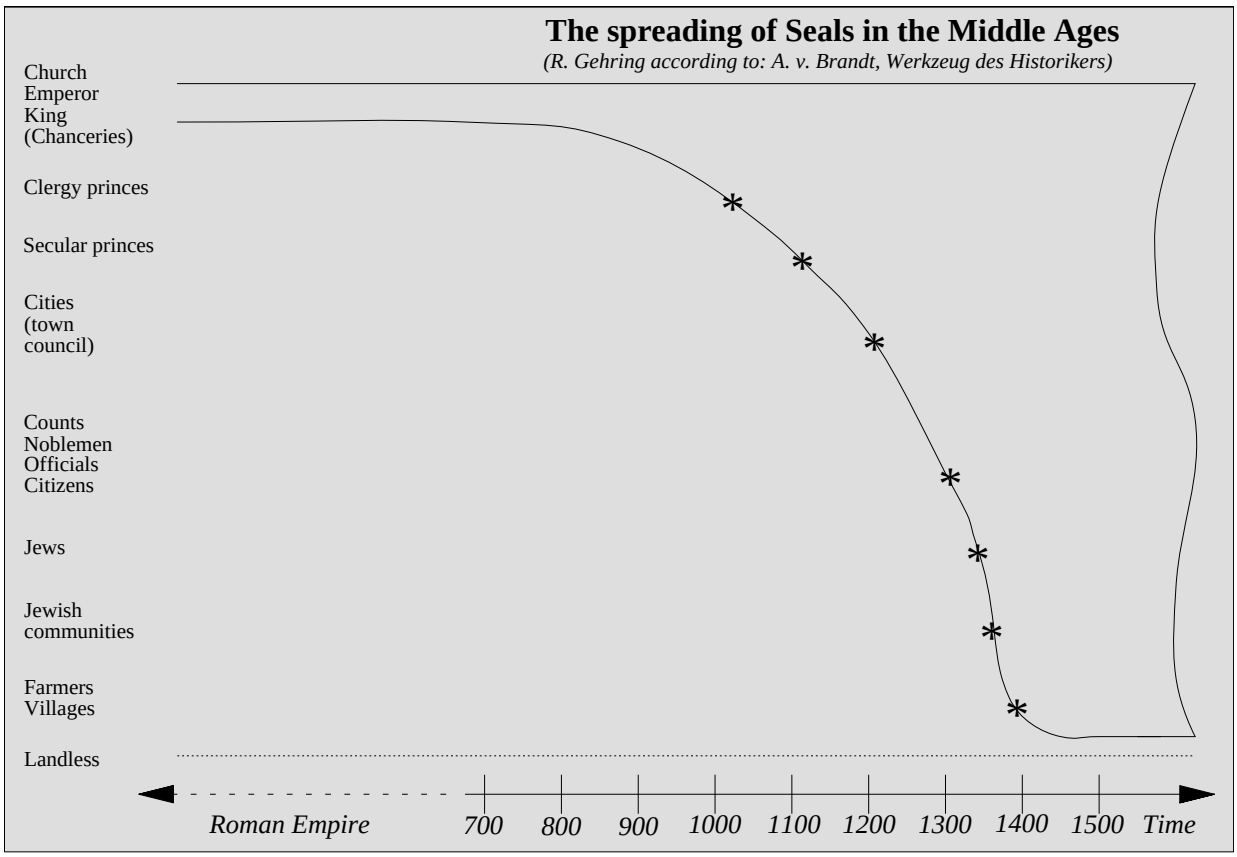
The Merovingians were the last literate emperors of the early Middle Ages. The following medieval kings were unable to write and used seals to authenticate documents. The early Carolingian emperors used Roman engraved gems as seals. A seal usually was not coupled to the identity of its owner. Instead it was coupled to its role and position, to its '*person*' in the antique understanding.[4] Since there was nothing like a state or a central administration there was no single way of identification.

To identify a human being meant to ask someone who did know this person. People had no last names during the early and high Middle Ages. The documentation process could not be build on a reliable identification process going beyond questioning. Immediate execution of a legal transaction was the safest way. And sealed legal documents served only as a means of formal reminder of the legal transaction.

Seals had a kind of power to authenticate. This power derived from the '*person*' (role) of its owner. The more power the '*person*' was associated with the more power the seal bore. To authenticate very important documents very powerful seals were necessary. Such seals were produced by the royal chancery or the episcopal chanceries. Without one or more powerful seals a specific document was not authentic.[5]

The system of different seals with different power reflects the confused situation with respect to power, rights and law. The system corresponds in a way to the imperial system of seals and the competing use of local seals in Japan.

In the later high Middle Ages cities started to evolve. The growing municipal production in the next centuries brought along a great diversity of products. Trade profited from this diversity. Trans-European channels of distribution were established. The communication and the administration of trade required a written documentation. To learn to read and write lost exclusivity at first in the cities. The use of seals was no longer reserved to the chanceries but became a common means of authentication. Seals were applied to contracts, goods and properties. The picture shows the spreading of seals throughout the medieval society.



The seals' unique quality to be identifiable even if one is illiterate supported their success. With the beginning of the 14th century seals were an ubiquitous means of authentication. A seal no longer had power of its own. A seal simply was the tool of someone to authenticate a document.

Since the transition from the late Middle Ages into the Modern Times a person's name and handwritten signature have belonged together. We still use this system. That's a period of about 500 years.

Seals have been continuously used for more than two thousand years. The contemporary form are stamps. Today, signatures are of greater importance for us.

Summary

Seals as a means of authentication provided amazing long-term stability. They kept the property to be of value in legal transactions independently of the changing social structures. They survived all radical changes. Seals were easily adopted to new social, administrative and legal requirements. They provided fall-back security in times of illiteracy.

Signatures have a significantly shorter history. They require a higher level of literacy to be of value. Signatures are based on a concept of 'identity' where each human being has a unique identity. Written contracts with signatures on paper are used in a society with a sophisticated legal system.

Authentication has to do with power. Social environments with a hierarchical system of power as our modern states prefer a single system of identification. A system of competing powers as it existed in the medieval Europe prefers authentication with witnesses (to testify the subject), instead of identification.

Resources: [4], [5], [6], [7], [8], [9], [10]

Third Example: 'ebay'

'ebay' as an e-business community

We start with a short description of 'ebay', and how to participate there. We have chosen 'ebay' as an example of how commercial activities can take place on the internet without absolutely reliable authentication. In our investigation we focus on the seller-buyer relation. We investigate how trust is enabled in the auction process.

'ebay' is the largest commercial auction community on the internet.[1] People distributed all over the world can sell goods with ebay's help. 'ebay' itself does not sell anything. Rather it supplies a platform to help users make commercial transactions

reliable. The way goods are sold is by auction. The platform ‘ebay’ maintains stores all the necessary information about the seller and the bidder to give a sufficient basis of trust.

Registration

How do transactions take place? At first the seller has to register with ‘ebay’. To be allowed to register a seller has to give the following information about himself[12]:

* Email address.
* Full name.
* Postal address.
* Phone number.
* Additionally a credit card number is required to charge the selling fees.

Other information is optional. This data is not checked ‘in a hard way’. Certainly the email address has to be valid. Otherwise the selling process is disabled.

The seller may choose a pseudonym to be used. Otherwise his email address will appear in the transactions. After the registration the seller chooses the section on ‘ebay’ were he wishes to place his offer.

Offer, bid, sale

For every offer at ‘ebay’ there is an initial fee between 25 cents and $2 depending on the opening bid the seller requests. If the seller is successful and sells his goods he has to pay a second fee. The amount depends on the final sales price. It usually ranges between 1.25% to 5%.[13]

After the supplier has placed his offer he can wait for the result. Every bid is valid for a limited period of time. After the bidding time passed by the bidder with the highest bid has won. He gets an email of ‘ebay’ that notifies him about his success. Now both the seller and the bidder have three days to agree on the terms of payment and delivery. A common way is to pay cash and send the money by mail. Payment with credit card is also quite usual.

As the seller has to register before he is allowed to make his offer a potential bidder has to register before he may bid. A bidder registers similarly to the sellers. The supply of a credit card number is only required if the bidder gives an anonymous email address (with yahoo for example). Once a bidder is registered as a member of the ‘ebay’ community he may take part in as many auctions as he wants to.

The process of offer, bid and sale is quite simple and there’s nothing mysterious about it. The whole process works without involvement of any official authority. No one is asked to check for the validity of the given names or addresses. There is no preselection or real identification of the participating parties. But it works.

‘Built-in trust’

What are the mechanisms that establish trust in the process? In short one can remark that the trust is enabled by the memory of the system. The ‘ebay’ platform stores information about the transactions. The seller and the bidder give feedback about their deal. The feedback of both parties is stored and becomes part of the ‘ebay’ history of the respective party.[14]

The stored history allows every bidder to form an opinion about the supplier in advance of the intended transaction. He doesn’t form his opinion based on security but based on probability. A bidder judges from the stored experiences of other bidders and perhaps from his own. ‘ebay’ supports this forming of opinion and expectation with the following information:

Feedback is classified into one of three categories: positive, neutral and negative comment. The feedback is shown summarized over the past seven days, the past month and the past six months. A bidder can for example read that the supplier got 301 positive comments and no neutral or negative feedback within the past six months. Also he gets the information that the supplier has an overall feedback (i.e. a history) of 1189 positive feedbacks from 666 different users. In contrast he got 3 neutral and two negative feedbacks. Feedback has a standardized form of a symbol and possibly a few informal words. It is possible to investigate what the supplier offers besides (at ‘ebay’) and at which price.

All the information one is able to gather gives one a solid base for risk-benefit-analysis in advance of a transaction. The bidder knows the price he is willing to pay. He knows what’s at stake if the transaction fails and how chances are that it will fail. The stored public opinion gives him a reliable basis for business. ‘ebay’ promises to not delete any reasonable comment from its databases. Exceptions (through law enforcement for example) are reasonably specified.

Failure management

In the case of a failure without abuse ‘ebay’ provides a dispute resolution service. The opinions about what happend -a failure or abuse- may differ between the parties. A neutral mediator is of great value in such cases. A dispute may show in differing comments of seller and bidder. The one who often causes disputes loses reputation. Thereby his reputation for business gets weakened in the (stored) public opinion.

Abuse leads to negative feedback. One may try to fraud a few times. The negative comments of the deceived bidders get stored for all time as a warning sign. Who will do business with someone who bears the sign to be a fraud? Who wants to buy anything from a person without reputation? One loses its commercial basis if one fails to meet the expectations of the customers.

‘ebay’ supports the victims of misuse with its so called ‘SafeHarbor’ facilities.[15] [It should be noted that ‘ebay’s’ ‘SafeHarbor’ facilities are something else than the ‘Safe Harbor’-principles for data protection that the EU and the U.S. agreed upon.]

Initialization

The attentive reader may have noticed that there is an initial period of time were a newcomer lacks a history. It takes some time to build reputation. The question is how one is able to start his business at ‘ebay’ without reputation.

‘ebay’ offers two appropriate features[15]:

- An escrow service. This is not free of charge. The buyer gives the money to the escrow agent. The he receives his order. After the buyer gave his approval the seller gets the money from the escrow agent.
- An assurance of $200 refund (less $25 dollars deductible) in the case of a failed transaction. This is free of charge.

Both features give the buyer support in his personal risk management strategy. The unknown seller is enabled to gain reputation and thus to take part in the ‘ebay’ community. And the buyer is able to estimate the probable ‘profit’ from the deal. He can compare the possible profit against the possible maximum loss. This personal cost-benefit-analysis gets support from ‘ebay’.

Summary

Obviously ‘ebay’ is a platform for electronic business on the internet. It works without strong authentication. Instead the history of the business partners is available for examination in every case of a new commercial transaction. Trust depends on the expectations of the parties to be successful. Personal risk management deals with the assumptions of loss and how to proceed with.‘ ebay’ gives the parties a reliable basis to weigh up. In a way we can compare the ‘ebay’ community to the inhabitants of a village or small who that know each other. ‘ebay’ enables the social control and self-regulation of its ‘inhabitants’. Thus it can refrain from perfect control and governmental authority.

The authors are not affiliated with ‘ebay’. We chose ‘ebay’ as one of the best known commercial websites on the internet.

Resources: [12], [13], [14], [15], [16]

The cultural gap

The cultural gap that we mentioned at the beginning has two faces.

There is a cultural gap between the material culture of writing and the virtual world of electronic communication. The handwritten signature of the material world cannot be compared to the digital signature of the virtual world. They are of completely different nature. Both belong to different cultures.

To stress out some of the most obvious conflicts (without preference):

* **Handwritten signatures** are of material character. They support both strong identification/authentication and ‘fuzzy’ identification/authentication. Thus they enable subtly differentiated risk management strategies in transactions.

  Digital signatures are of virtual nature. They don’t support ‘fuzzy’ identification/authentication. They disable subtly differentiated risk management strategies.

* **Paper with signatures** and/or seals as a means to authenticate legal transactions has developed under *conditions of uncertainty and doubt*. A signature or a stamp is subject to uncertainty and interpretation. Our social structures are adapted to these conditions. They supply *adequate risk management structures*. They tolerate errors and mistakes. (*‘‘It’s a feature, not a bug!’’*)

  Digital signature infrastructures still fail to implement similar appropriate risk management structures. Such infrastructures (PKI’s for example) are operated and used by humans and thus are unable to rule out *uncertainty and doubt*. Mistakes and errors do happen. One should be able to cope with.

* **Handwritten signatures** are efficient. It only takes a paper and a pen to sign within a few seconds. Everywhere, every time.

Digital signatures in their available manifestations are inefficient. If the exchange of electronic documents is more efficient that's due to its digital nature and not because of digital signatures are applied.

* **A genuine signature** cannot belong to more than one unique human being. That is inherently impossible. One cannot transfer one's signature.

  A valid digital signature can be produced by anyone who is able to obtain the means. That is inherently possible.

* **Handwritten signatures** (or seals in Japan) proved to be both 'long-term stable' and 'long-term reliable'. That is not because of their infallible nature. Rather it is because of the society has learned to cope with their imperfectness.

  There is no clue of digital signatures being 'long-term stable' or 'long-term reliable'. Society had no learning period yet.

Another cultural gap exists between the promoters of digital signatures with their hierarchical approaches on the one side, and the internet communities with their systems of self-regulation on the other side.

Of which kind are the issues?

* **The history** of the internet is a history of communities. Inside the communities governance of (multiple) identities and self-regulation is given.

  The digital signature approach lacks history and self-regulation.

* **Internet inhabitants** interact in networks (communities) with self-defined and self-enforced rules. These rules are not framed by traditional borders or legal boundaries.

  Today's digital signatures require hierarchies. They introduce rules of their own without taking notice of the already given social structures on the internet. The regulation is done by law.

* **Trust** is not a matter of technology. Trust is a quality of human interaction. To enable trust is not the same as to enable technology.

  Digital signatures provide technical security in technical interactions. They do not enable trust.

* **Good governance** should respect the already given cultural diversity. The internet is a space where the concept of 'identity' is different from its real world counterpart. People can have more than one identity on the internet. They heavily make use of this feature. The internet users favor subsidiary solutions over 'one-fits-all'-approaches like digital signatures.

  It is not recognizable how today's digital signatures will respect the already given cultural diversity. They are focused on to "heave" the concept of 'one single legal identity' onto the internet with it's 'multiple identities'.

* **The internet needs** transaction security and reliability.

  Digital signatures according to law provide legal security.

There are more issues. But the ones given here should be sufficient to give an idea of the problem. The list might serve as a starting point for further investigations. Future plannings for electronic signature systems should be examined with respect to their cultural compatibility.

Summary and Prospect

It is not necessary nor even reasonable to assume that e-commerce on the internet is impossible without digital signatures. 'ebay' proves the opposite. And 'ebay' is only one example. We can find more. The point is to focus on transaction security and transaction reliability. Trust in commercial transactions is based on these two features. Legal security is of less interest on the internet.

Important is to respect the cultural constraints. Where this rule is obeyed, success is likely to come (example: Japan).

Reliability and trust on the internet may be established through (among others):

* Communities with a social memory (witnesses)
* 'Multiple identities' (pseudonyms) with a social history
* Social control and self-regulation (checks and balances)
* Risk management strategies including cost-benefit-analysis, escrow, insurance, mediation and arbitration

Here we see a promising direction for further developments.

That is not to say that digital signatures have no place in the information society. That is to say that a lot of places on the internet do not require digital signatures.

> ***"Cyberspace is not a place. It is many places. The character of these many places is not identical." (L.Lessig: Code ..., p.63)***[17]

One should carefully examine where digital signatures are appropriate - before relying on them.

Resources

[1] **"Wenn der virtuelle Hammer fällt. Die Auktion und ihr Aufstieg im Internet"** (When the Virtual Hammer Falls. The Raise of Auction on the Internet), S.14, Neue Zürcher Zeitung, 29./30. Juli 2000

[2] Kei Ishii: **"Gegenwart und Geschichte japanischer Unterschriftenstempel"** (Present and Past of Japanese Seals), version of 17.5.2000, unpublished

[3] Howard Rheingold: **"The Virtual Community: Homesteading on the Electronic Frontier"**, HarperPerrennial, 1993; dt.: "Virtuelle Gemeinschaft. Soziale Beziehungen im Zeitalter des Internet", Addison-Wesley, Bonn u.a. 1994

[4] Aaron J. Gurjewitsch: **"Das Individuum im Europäischen Mittelalter"** (The Individual in the European Middle Ages), S.116ff, C.H.Beck, München 1994

[5] Ahasver von Brandt: **"Werkzeug des Historikers"** (Tool of the Historician), 15. Aufl., W. Kohlhammer, Stuttgart u.a. 1998

[6] Hartmut Boockmann: **"Einführung in die Geschichte des Mittelalters"** (Introduction to the History of the Middle Ages), 6.Aufl., C.H.Beck, München 1996

[7] Ivan Illich: **"Im Weinberg des Textes. Als das Schriftbild der Moderne entstand"**, Luchterhand, Frankfurt/Main 1991; engl. Ivan Illich: **"In the Vineyard of the Text: A commentary to Hugh's Didascalion"**, Univerity of Chicago Press, Chicago 1993

[8] Adrian Frutiger: "**Der Mensch und seine Zeichen. Schriften, Symbole, Signete, Signale"** (The Man and his Signs: Script, Symbols, Signs, Signals), 6.Aufl., Fourier, Wiesbaden 1998

[9] **"Deutsche Geschichte in Quelle und Darstellung. Band 1: Frühes und hohes Mittelalter 750-1250"** (German History in Documents. Volume 1: Early and High Middle Ages 750-1250), Reclam, Stuttgart 1995

[10] Uwe Wesel: **"Geschichte des Rechts"** (History of Law), C.H.Beck, München 1997

[11] Karl S. Bader, Gerhard Dilcher: **"Deutsche Rechtsgeschichte. Land und Stadt - Bürger und Bauern im Alten Europa"** (History of German Law. Land and Town - Citizens and Farmers in the Ancient Europe), Enzyklopädie der Rechts- und Staatswissenschaft, Springer, Berlin u.a. 1999

[12] http://cgi4.ebay.com/aw-cgi/eBayISAPI.dll?SSLRegisterFromCountries&siteid=0&co_partnerid=2&UsingSSL=0; Jul 28, 2000

[13] http://pages.ebay.com//help/basics/n-fees.html; Jul 28, 2000

[14] http://pages.ebay.com/help/basics/n-is-ebay-safe.html; Jul 28, 2000

[15] http://pages.ebay.com/help/community/index.html; Jul 28, 2000

[16] http://www.ebay.com; Jul 28, 2000

[17] Lawrence Lessig: **"Code and other Laws of Cyberspace"**, Basic Books, 1999

[18] U.S. Patent and Trademark Office, on the internet: http://www.uspto.gov; Jul 28, 2000