59

# Digital Identity and its Implication for Electronic Government

Clemens H. Cap and Nico Maibaum
*Chair for Information and Communication Services, University of Rostock*

**Abstract:** The present use of identity concepts is analyzed. A requirements analysis for "identity" reveals the different identity properties necessary in various administrative and business processes, A classification of identity tokens is given and compared with passport identity and established forms of digital identities. A fundamental problem with digital signature identity schemes is explained. Implementation strategies for non-transferable identity tokens are outlined. Finally, conclusions and implications for the e-government processes and solutions of tomorrow are presented in the form of six Theses and with the goal of stimulating further discussion.

## 1. INTRODUCTION

Electronic commerce applications draw public attention to security problems of the Internet. Almost every netizen is familiar with the unpleasant feeling when sending his credit card number to a web server in the Internet, as this act could provide sensitive information to a criminal hiding his identity behind a fancy web page. On the other hand, many surfers are very careful whom they reveal information leading to their identification. Giving away an email address fills one?s electronic mailbox with masses of unwanted advertisements and other solicitations. Shopping profiles and patterns of surfing behavior provide companies with unfair bargaining advantages, reducing a customer to a revenue generating black box with marketing relevant properties.

In electronic government processes, the issues of identity and anonymity are even more important: Here the dangers are not only of a monetary nature. Personal freedom, civil and democratic rights are at stake. Citizen rights groups point out the danger of *Big Brother* whom they fear in every electronic administration pro-cess. On the other hand, experiences with Florida voting machines in the 2000 US presidential elections call for a more reliable technology. From the cryptographic point of view, electronic voting algorithms (Herschberg, 1997) are a well studied subject.

The situation of the voting process illustrates the issues very clearly: The *identity* of a voter must be verified beyond any doubt to make sure that he or she is legally entitled and correctly registered to vote. When casting the vote, *anonymity* of the vote constitutes the basis of democracy. Although *transaction numbers* (or physical or organizational means with the same effect) are necessary to identify and to count every single vote and to make sure that a voter casts at most one vote, this transaction number (or the specific ballot sheet) must not allow identification of the voter. All three central issues at stake with identification personal identity, pseudonymity (ie. session or transactional identity) and anonymity - are contained in the single act of voting.

In *this paper* we describe the *concepts* of identity and the implications for electronic government processes when mapping traditional identity to electronic identity. In Section 2 we explain the basic concepts and present a requirement analysis for "identity. We introduce a new token concept for identity and compare it to established digital identity schemes. Section 3 outlines, how this token concept can be implemented. Section 4 discusses legal, social and process implications of identity concepts in e-government. It demonstrates why and how *a renewed analysis of identity concepts* is imperative for successful e-government operations.

The paper *does not* provide a complete account of implementation strategies for all combinations of requirements for digital identity since this is not the primary goal of the paper nor can it be achieved within the given space limitations. We have verified that every presented attribute allows an implementation by known cryptographic or biometric methods or by straight forward adaptations thereof. Given the achievements of (Chaum et al., 1989), (Chaum, 1985) and the cryptographic basis illustrated in (Schneier, 1995), the technical feasibility is beyond doubt.

# 2. WHAT IS IDENTITY?

## 2.1 Requirements Analysis for “Identity”

In the "real world", identity is a handle to a person serving various purposes: It is used to determine parameters associated with that person (eg. name, age, place of work), to ensure that real world operations are invoked on the correct individual (eg. putting a person in jail, awarding a prize to a person) to verify, whether a person has certain rights (eg. to drive a car, to pick up tickets for a theatre performance) or to engage in communication acts with the intended addressee (eg. sending a letter or an email).

Governmental processes use various schemes to regulate identity: Unique administrative numbering systems such as the Swiss AHV number or the US social security number, names augmented by place and date of birth to guarantee uniqueness, or official documents with photograph and signature. Occasionally these several systems have to be translated into each other, eg. to obtain the name belonging to a certain social security number.

**Passport and anonymous identity:** Most identity schemes in present government processes are linked to what we shall call the *passport identity* of a person, ie. the name, nationality, place and date of birth of that person. Some schemes provide an *anonymous identity*, by establishing a session identity without revealing further information on a citizen. The classical example is the anonymous AIDS test, where an identity concept has to ensure that every individual receives his own test results, but maintains full anonymity.

Closer analysis reveals different administrational needs of associating what we shall call *tokens* with a person. We can identify several dimensions of requirements:

**With regard to transfer:** *Non-transferable tokens* are parameters, rights, properties or obligations linked to a specific person. They should be implemented in a form that they cannot be passed to others. In contrast, *transferable tokens* are acquired by a person, who then can pass them along to another person.

**With regard to divisibility:** A transferable token can be *atomic*: If it is passed to another person, the original owner no longer owns it. It can be *splitable*: When passed to another person the original owner may retain his ownership at the same time. A splitable token can be *intransitive*, ie. after it has been passed along it no longer can be passed on to others. However, if it is *transitive* it can be passed on and on by those who received the token.

**With regard to consumption:** A token can constitute a right which may be exercised arbitrarily or under certain restrictions, eg. Only once, for a certain number of times or before a certain date.

**With regard to access permissions:** The rights to create, delete or modify a binding or ownership between a token and a person can belong to that person himself or to another entity.

**With regard to evidential power:** Suppose the owner of a token presents the token to a business partner. Then, only this business partner has to check the validity of the token. In this case, the token must be designed for *evidential power towards a (collaborating) second person.* Now suppose that the business partner claims that the token is invalid. In this case, the token owner and his business partner will have to convince a judge of their claims. The token must be designed for *evidential power towards a third person.* See the examples below (PIN and SET) for examples on this important but not always fully obvious property.

**Examples:** In the following, an *intentionally long list* of examples shall demonstrate that most combinations of above requirements can be found in real life identity applications. A *drivers license* is a non-transferable token. The owner is not entitled nor able to pass it along to others. The license document itself can be passed along, but the owners photograph prevents providing the non-transferable "right to drive" to other individuals. A drivers license may be created only by an is-suing authority, however the owner may destroy it any time, surrendering his right to drive. A *prison punishment* is a non-transferable token as well. It is different from the drivers license in so far as his "owner" cannot destroy his binding to it. A similar token is required to implement a discount which is offered to customers only on the occasion of the first shopping order. *Passport identiy* as defined above, is a non-transferable token combined with name and further parameters. A *one dollar bill* or a *stock certificate* is an atomic transferable token. It can be passed along to other persons but the original owner loses his binding by passing it along. The right to *cast a vote* is a non-transferable token, associated with a notion of consumption and the restriction that for every election it can be utilized at most once. The *power of attorney to act in a certain legal matter* is a transferable token (I may pass this right to others), it is splitable (I do not lose the right to act in these matters by myself) and usually is intransitive (the persons to which I pass the power of attorney cannot pass this right on to others). The *right to pick up a parcel* at the post office is connected with the addressee who should be able to pass this right along to others without losing this right himself. Furthermore those to whom this right is passed on should be allowed to further pass this right: If I ask my neighbor to pick up a parcel for me, I do not mind if the neighbour sends his son to do this job. In the real world, the right to pick up a parcel often is connected to presenting a specific piece of paper, the notification on that parcel. This is an incorrect implementation of a right by an atomic transferable token where a splitable transitive transferable token should have been used. A different, even more unfortunate implementation is to require the person collecting the parcel to identify himself by a passport, ie. A non-transferable token. The *AIDS test result id* as a kind of session id preferably is a non-transferable token, allowing immediate counseling in the case of a positive test result. The well known *personal identification number* (PIN) with which a bank customer proves his right to make a cash withdrawal usually is mailed by the bank to the customer. The PIN therefore has evidential power towards a second person (ie. the bank, recognizing again the PIN it sent to the customer) but not to-wards a third person (ie. a judge). In principle, it could have been a bank clerk who made the withdrawal. In contrast, the *secure electronic transaction (SET) protocol* based on digital signatures establishes a payment contract between customer and retailer which utilizes cryptographic means to establish evidential power towards second and third persons. A *precharged telephone card* is a transferable token with a restriction regarding the consumption (ie. the remaining card value). It can be implemented by storing consumption information physically on the card itself (leading to an atomic token) or by storing it on a server of the phone company (leading to a splitable token, ie. a calling card which can be used if one knows the number of the calling card).

## 2.2 Passport Identity versus Token Identity

The cited examples demonstrate the varying requirements for "identifying" a per-son in administrative settings. In most situations, no passport identity is required, but established governmental procedures nevertheless require citizens to produce passport-like identities. The following example will demonstrate what we have in mind.

The traditional drivers? license provides not only the non-transferable token "right to drive" but also conveys the civil identity of the driver, ie. the name, the nationality, in some countries even the address of residence and the date of birth. If a civil servant is checking whether a person is legally entitled to drive, the implementation of a non-transferable token including this right would be sufficient; further data on the driver (name, address) not necessarily have to be revealed. If, however, the driver was witness at a traffic accident, he might have to testify at a trial. In this case a different non-transferable token must enable the administration to summon the driver to the trial and, in case the witness would not show up, allow that punishment to be carried out which is available in case of a refusal to testify. Again, neither the name nor the nationality of the driver must be made available; they can be revealed by the driver voluntarily and they can be made part of the employed token so that they are revealed automatically. For implementing the govern-mental business process, they are not required: Electronic communication can be anonymous via pseudonyms or more elaborate methods (Chaum, 88), (Reichenbach et al., 1997) and monetary fines can be implemented using anonymous payment methods (Chaun et al., 1989). See (Chaun, 1985) for an introduction to cryptographic protocols available for such situations.

Replacing the passport-type of identity by taken based identities adapted to the requirements of the specific administrative processes can have a number of important effects for electronic government. While ensuring the required token properties, only those data on a citizen are employed which really are required for the process. The approach observes the data protection principles of *data economy* and *data avoidance*. It respects the citizens' right for privacy, implementing at the same time the proper administrative acts required by law. Most important, it can advance the acceptance of e-Government, since it actively deals with "big brother" anxieties. Most especially, it leads to a more fair and equal treatment of citizens by their administration. Neither title, name, age or other attributes stored on a passport or in a file could now influence administrative decisions within the discretionary power of a civil servant - only those properties being available with the specific required token could play a role in the regulatory process. Whether the latter property is considered an advantage or a disadvantage is, of course, a matter of one's political standing.

## 2.3 Other Concepts of Digital Identity

In the digital world, "identity" often is associated with concepts like digital signature, user names, passwords, PIN and TAN codes.

**Real world signature:** In the real world, a signature is a *willful act* by which an individual certifies his or her approval of the content of that document which gets signed. Apart from the approval, the act of signing psychologically serves as a *warning function,* calling to the attention of the signer that he is about to enter into a binding commitment.

A signature per se *does not* provide the identity of an individual, especially in the case of common names (eg. John Smith). The link to the individual can only be made by a passport or by a similar official document linking picture and signature (ie. non-transferable, biometric properties) with the name, nationality, birthdate and birthplace of a person, which usually are considered sufficient data to identify that person. This link is established only for those who are personally present at the act of signing and have checked the passport themselves. If this link is required for the benefit of third parties, a notary public certifies it with his seal and authority.

**Digital Signature:** If we apply a certain well known (see for example the introductory literature on this topic, eg. (Schneier, 1995)) cryptographic algorithm $A$ on a document $d$ and a *private key* $p$, we obtain the *digital signature* $S = A(p, d)$. The private key $p$ is mathematically connected with a *public key* $q$ in such a way that a second application of the algorithm on the signature $s$ and the public key produces the original document: $A(q,s) = A(q,A(p,d))=d$.

For purposes of digital signing, a person generates a pair of a public and a private key. The public key will be registered in a trustworthy agency as belonging to that specific person. The private key will be safely stored away and shall be known only to his owner. Therefore it is only the owner who can derive the signature $s$ from the document. Everybody can verify the signature on a document $d$ by obtaining the public key $q$ of the undersigned person at the trustworthy agency and by checking that $A(q,s) = d$. See (Schneier, 1995) for the exact mathematical details of this procedure.

**Problems with digital signatures:** Practical implementations of digital signature schemes raise a considerable number of issues. Often, the private key is stored on a computer which performs the calculations of the algorithm A on behalf of the user. Given the well known threats of viruses, Trojan horses and worms and facing the unreliability of present personal computers, there is *no way to make sure* that the computer applies this algorithm only when the user directs the machine to do so. There is *no guarantee* that the algorithm is applied only to the document presented to the user on the computer screen and in exactly the form as it appears on that computer screen. A *bogus program* could trigger the signing of documents unbeknownst of the signer or even could transmit the private key into the Internet. Schemes to protect the private key are reliable only if the *entire hardware, software,* *operating system and the firmware can be fully trusted* - a goal which cannot realistically be achieved on a personal computer. This fact explains the trend to small cryptographic devices, since it is easier to design a flawless and trusted device if it has reduced complexity and its only functions are the storage of the private key, the display of the document which shall be signed and the calculation of the digital signature.

Furthermore, the digital signature only tells us that a certain mathematical algorithm has been applied to a certain document. The link of this code to the signer and his identity is *not provided to a sufficient degree.* Using above terminology, a digital identity establishes only a splitable transferable token. Providing another person with one s private key amounts to passing the digital identity along, accidentally or on purpose, while keeping associated rights to oneself at the same time. There is, however, some hope that a user does not give away his private key on purpose, facing the possible abuse of his key for signing acts performed outside of the original motivation for giving away the key.

**User names, passwords, PINs and TANS:** The well known user names, as well as personal identification numbers (PINs) implement the simplest form of (splitable, transitive) transferable tokens (without a notion of consumption). Trans-action numbers (TANS) provide consumable transferable tokens which usually are valid for one transaction.

In the common application arena of cash dispensers and online banking systems, these approaches are severely flawed. PINs and TANs are generated by the issuing agency and sent to the user. Therefore, a link to the passport identity of the user always is possible. Since PINs and TANs are known to the issuer, they do not have evidential value in a dispute between issuer and user: Suppose a bank customer claims not having authorized a specific online transaction and the bank claims the customer did execute the transaction, presenting as a proof the TAN submitted by the user. In this case there is no proper method for a judge to find out, who is telling the truth, since the bank could easily have forged the proof. It is quite disturbing that most cash dispensing machines and online banking systems still rely on such improper techniques. Closer analysis makes it obvious that these systems would require non-transferable tokens instead of transferable ones.

# 3. IMPLEMENTING IDENTITY TOKENS

## 3.1 Non-transferable Tokens

A design of non-transferable tokens must focus on the *four attack modes* presently conceivable: The present owner of the token might *want* to transfer it, or he *does not want* to transfer it but is forced to do so by others. The person to which the token shall be transfered is *ready to receive* it or *does not want to receive it.*

Furthermore, the likely interest of an attacker and the damage of an illegitimate transfer must be considered.

The *design options* in Table 1 are either of a non-digital nature and have false acceptance or false rejectance failure modes, or they are digital in nature but require implantation or tedious restraining techniques, both of which are ethically not acceptable. Depending on the sensor used, additional factors such as hygiene, public acceptance, cost, time and others play an important role.

Table 1: Non-transferable tokens

| | |
|---|---|
| Physical attributes | Iris (Seal et al., 1997)<br>Fingerprint<br>Finger Lenght<br>Face Recognition |
| Biological attributes | DNA<br>Body Odor (Davies, 1997) (Grassfield, 2000) |
| Behaviour | Handwriting (ie. Signature)<br>Characteristic Movements (Bartmann, 1997)<br>Voice Recognition |
| Artificial tokens | Implants (eg. RFID-tags)<br>Unremovable Bands |

From a *security point of view* the sensor and the signal path from the sensor to the processor matching the measured signal with a stored template is most critical. Firstly, a fake duplicate could be presented to the sensor (eg. a picture of a face presented to a face recognition system, latex duplicate or cut-off finger presented to a finger print sensor). Countermeasures comprise high sensor quality (eg. a finger print sensor tests for the temperature and electrical characteristics of a live finger) and the combination of several tokens, since a successful fake of several recognition systems seems highly unlikely. Secondly, the owner of the token could collude with the attacker, presenting his token for the benefit of the attacker. Here, the solutions depend on the situation of the token presentation. If the real world benefit involves access to a high security area, physical barriers can ensue that only the person presenting his finger print or iris is allowed access. If the situation involves proving ones identity to a police officer, the officer can ensure that the correct person offers his body to a sensor measurement. Finally, the signal path from the sensor to the processor executing the comparison algorithm, this processor itself and the place where the reference template for the token is stored can be attacked. Physical means must prevent tampering with this part of the system. Non-colluding "owners" of a biometric property who are forced into providing their token, in some systems can call for help by intensionally giving a wrong signal (eg. by using a special alarm finger to call for help or by talking in an unnatural voice to prevent correct voice recognition).

From a *data protection point of view* measuring physical, biological and behavioural attributes of a person is problematic. The obtained data could be used for other purposes than for which these data were provided. Especially data obtained from a DNA test could be used to determine genetic diseases of the involved person resulting in health insurance or employment troubles. The provided data could also help an attacker to misrepresent himself as the original "owner" of the biometric properties.

Special thoughts must therefore be given to the place where the *reference templates* of the biometric signal are stored. This could be in a *central data* base of a trusted agency where the identity of a person is established using traditional means and the biometric signal is rendered and stored under close supervision and in a controlled environment. From a privacy protection point of view this is a bad idea and should be restricted to specifically defined cases such as law enforcement. Another possibility is the *decentralized storage in a device* under the control of the user, for example in a smartcard. This also requires an enrollment of the reference signal under the control of a trusted agency. The user then presents this device and exposes the required biometric signal to the sensor. The *optimal architecture,* however, requires that also the biometric sensor and the entire matching process is located on this device. Only this setup ensures that the biometric signal of the user cannot be stored; furthermore the sensor and the matching device are under the supervision of the user, effectively reducing privacy concerns. Unfortunately such a closed architecture is difficult to achieve for many biometric systems. For the fingerprint case, smartcard solutions are likely to be available in 3 to 5 years, Devices in the size of a PCMCIA card are presently under development (Sedov et al., 2001).

A totally different approach to non-transferable tokens would be to motivate the token owner *not to give away* a specific transferable token (Goldreich et al., 1998). Such a motivation could be built up, if passing along the token led to considerable economical or social damage. If a certain transferable token were a universal token required to exercise all one's civil rights or to access one's bank account, voluntary surrender by the owner would be highly unlikely. In the legal frameworks evolving for digital signatures such an approach is taken: If a digital signature given with a private key residing on the smartcard of a citizen is always considered as legally binding signature it is highly unlikely that the card owner will collaborate with an attacker.

However, this approach is *highly dangerous.* Firstly, the transferable token could be lost or stolen. The dangers of losing most of one's civil rights by losing a single token have already been amply discussed by civil rights groups and pose an unacceptable threat to the citizen. The often proposed solution of securing these devices with a PIN code or password is also not acceptable, since PIN codes and passwords tend to be forgotten - or written down by their owners.

## 3.2 Transferable Tokens

Transferable tokens can have rather different requirements. Many of them are well known in the field of cryptographic algorithms. For space constraints, we shall only present an incomplete overview, leaving a detailed and cryptographic discussion to a later publication.

Transferable tokens are not bound to an individual, thus a biometric link no longer is necessary and the token can be realized by a bit string which can, of course, be passed along and copied arbitrarily. A generic implementation therefore produces a splitable and transitive token which a priori imposes no limit on the number of consumptions. Evidential power depends on who is generating the bit string, issuing it to the user and who is checking the validity.

The required access permissions can be implemented with digital signature schemes, preventing unqualified persons from tempering with token data or from generating unauthorized tokens.

Manufacturing an *atomic* token is a well known requirement in the fields of electronic money and digital content copyright: If I give away a dollar or a music CD I should no longer own it: I might still physically posses the token but it has become useless for me. Strategies to tackle with this requirement in an intangible, purely digital manner, have been developed in anonymous electronic money schemes (Chaum et al., 1989). Physical tokens which cannot easily by duplicated or manipulated (eg. cryptographic smartcards) could be used as well. Restricting the number of consumptions can be implemented as a simple add-on to electronic money schemes and easily are implemented in smart tokens.

## 3.3 Real World Implementations

In a single real world business process, different identity tokens might be required. Suitable devices such as PDAs or smartcards will act as a *representative* for the user and will guarantee that the proper protocols are used. They will ensure the correct choice of the token type and *insulate* the owners true identity from the ones required in specific processes. (Sedov et al., 2001) describes possible architectures.

Certainly, such an important device can be lost. Technology from Section 3.1 links the device to its owner and prevents abuse. Storing the tokens on a cryptographically sealed backup device protects against a sudden “loss of ones identity”.

# 4. CONCLUSIONS AND IMPLICATIONS FOR E-GOVERNMENT PROCESSES

**These 1:** Presently, in most administrative processes the citizen has to reveal his passport identity, supplying more data on himself *than really is required* by the administrative act. We propose for discussion the *reengineering of governmental processes* in order to reduce the amount of revealed data. Instead of providing his passport identity, the citizen should provide (only) those identity tokens materially required by the respective administrative act.

For example, the administrative act of "verifying whether a person has the license to drive a car" should be reduced to checking the *non-transferable token* "has the right to drive a car". There is no need to reveal the name of the person in this process.

*Consequences* are an improved privacy and a more fair and equal treatment since only legally required data form the basis of a discretionary administrative decision. Furthermore, some possibilities for centralized statistical surveys and demographical studies are lost.

This suggestion is not as radical as it might seem, being the logical consequence and spirit of the US *Identity Theft Protection Act,* stating in its preamble the following purpose (Anon, 01):

> ... to *prohibit* the establishment in the Federal Government of *any uniform national identifying number,* and to *prohibit* Federal agencies from *imposing standards* for identification of individuals *on other agencies or persons.*

This development, however, is more typical of Anglo-Saxon and American governmental culture, where there is considerable less central registration of citizen data than in most European administrative cultures. Whereas the former does not know mandatory formal registration of a residential address and the citizens? place of living is checked informally and only when public or private services are utilized (eg. registering to vote, registering a car, claiming social benefits) it is mandatory in the latter culture and even centralized registers of residential addresses are common. This comparison, however, is not uniformly true for all administrative areas given, for example, the highly organized structure of the US Internal Revenue Services IRS. See (Clarke, 1994) for a comparison of national policies.

**These 2:** Present *digital signature schemes and laws* have a *fundamental flaw.* They not necessarily guarantee the "wilful act" and "warning function" properties required from a "real world" signature and lack the non-transferable binding to a person.

We suggest to enhance present digital signature technology and law by *mandatory biometric components* establishing the required non-transferable token.

Furthermore, implementations should be restricted to devices sufficiently small that the operating system and signing software cannot be tampered with as easily as a PC.

**These 3:** *Citizen trust* in online security is low. We therefore *need a better public understanding* of the concepts of identity, digital signature and online security, as well as of the threats of their presently flawed implementations.

We suggest that parallel to technological and legal improvements towards truly trusted signature and identity schemes, *public awareness strategies are developed* to establish a feeling of trust in digital identity systems with our fellow citizens. With more than 85% of all Internet users perceiving security as significant or even deciding factor in online business (Anon, 1998), one can imagine the dramatic acceptance problems large scale e-government solutions will have otherwise.

**These 4:** In order to obtain *perceived and real trust* in identity schemes, we have to *develop audit technology, open protocols and standards* and should *ban proprietary or closed source identity schemes.*

Only open source systems whose entire design principles are available to critical public analysis make it possible to safely verify the claims of adhering to established regulations and protocols. Therefore, only such systems should be used in e-government identity processes. Obviously, this criterion must apply to *all* parts of the system, including operating systems and bootstrap codes. Thus, most presently used operating systems must be eliminated from security relevant e-government processes.

We furthermore need an administrative culture which is *open for public auditing* of its technological environment and *encourages discussion of security issues, especially security flaws.*

**These 5:** We need *laws dealing with digital identity and identity theft based* on digital id.

First activities in this direction are the *Identity Theft Protection Act* or the *Social Security Number Protection Act* in the US.

This legal framework must also deal with the theft of biometric properties 2 and with the fraudulent manipulation of identity establishing biometric sensors and systems. On the other hand, open discussion and research into the flaws of these systems must not be restricted, as it is presently done with copyright protection technology by the Digital Millennium Copyright Act.

**These 6:** We should stimulate *the participation of the public* in the discussions on e-government systems. (Chaum, 85) observes:

> As the initial choice for the[ir] architecture gathers economic and social momentum, it *becomes increasingly difficult to reverse.* Whichever approach prevails, it will likely have a *profound and enduring impact* on economic freedom, democracy, and our informational rights.

Today, 15 years later, more than 85% of the Internet population is heavily concerned with online security. If the quick path to e-government which is taken today for economic reasons continues to neglect the impacts on the citizen and does not reevaluate its position with regard to identity, we will either end up with the wrong solution or with an unexpected low rate of acceptance. In both cases costly reengineering will be required.

# 5. ACKNOWLEDGEMENTS

The paper could be significantly improved thanks to the remarks made by two of the referees.

# 6. REFERENCES

[Anon, 1998] Anon. Georgia tech research corporation, tenth www user survey report. October 1998.

[Anon, 2001] Anon. Identity theft protection act of 2001. Bill H. R. 220 at http://thomas.loc.gov/, 2001.

[Bartmann, 1997] D. Bartmann. Psylock - identification eines tastaturbenutzers durch analyse des tippverhaltens. In Mathias Jarke, editor, Informatik als Innovationsmotor, Aachen, September 1997, pages 327-334. Springer, 1997.

[Chaum et al., 1989] D. Chaum, A. Fiat, and M. Naor. Untraceable eletronic cash. In Advances in Cryptology, Crypto88, pages 319-327. Springer, 1989.

[Chaum, 1985] David Chaum. Security without identification: Transaction systems to make big brother obsolete. Communications fo the ACM, 28(10): 1030- 1044, 1985.

[Chaum, 1988] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology, 1(1):65-75, 1988.

[Clarke, 1994] Roger Clarke. Human identification in information systems: Management challenges and public policy issues. Information Technology & People, 7(4):6-37, December 1994.

[Davies. 1997] Ann Davies. The body as password. Wired, 5(7), July 1997.

[Goldreich et al., 1998] O. Goldreich, B. Pfitzmann, and R. Rivest. Self-delegation with controlled propagation - or - what if you lose your laptop. In Advances in Cryptology, Crypto 98, pages 153-168. Springer-Verlag, 1998.

[Grassfield, 2000] Lisa Grassfield. Biometrics: Securing electronic commerce. http://www.tinucci.com/Papers/Grassfield - Biometrics.html, 2000.

[Herschberg, 1997] M. Herschberg. Secure electronic voting over the world wide web. Master's thesis, Massachusetts Institute of Technology - Laboratory of Computer Science, May 1997.

[Reichenbach et al., 1997] Martin Reichenbach, Herbert Damker, Hannes Federrath, and Kai Rannenberg. Individual management of personal reachability in mobile communication. In Louise Yngstr om and Jan Carlsen, editors, Information Security in Research and Business, IFIP TC 11 13th International Conference on Information Security SEC?97, Copenhagen, Denmark, pages 164-174. Chapmann & Hall, 1997.

[Schneier, 1995] Bruce Schneier. Applied Cryptography. Wiley, 1995.

[Seal et al., 1997] Chris H. Seal, Maurice M. Gifford, and David J. McCartney. Iris recognition for user validation. British Telecommunications Engineering Journal, pages 113-118, July 1997.

[Sedov et al., 2001] Igor Sedov, Marc Haase, Clemens Cap, and Dirk Timmermann. Hardware security concept for spontaneous network integration of mobile devices. In Proceedings of the Workshop on Innovative Internet Com-puting, Ilmenau June 2001. TU Ilmenau, 2001.