RETHINKING TRUST AND CONFIDENCE IN EUROPEAN E-GOVERNMENT

LINKING THE PUBLIC SECTOR WITH POST-MODERN SOCIETY

Reinhard Riedl
University of Zurich

Abstract: In this paper, we shall discuss the meaning and the relevance of trust for e-government. First, we shall identify trust concepts from philosophy, which might be important for trust engineering in e-government. Then we shall look at trust models for e-commerce, and we shall discuss how they may be transferred to e-government. Afterwards, we shall present the results of two empirical studies among young people. The theoretical and the empirical results will be used to derive recommendations for trust engineering in practice. Finally, we shall have a second look at philosophy, discussing the implications of post-modern reality for the design requirements for e-government solutions, and we shall derive a research agenda based on recent results in applied cryptography.

Key words: trust and confidence, digital identity, anonymity, e-government, e-voting, credential technology

1. INTRODUCTION

Many experts on information and communication technology have provided educated speculations about the importance of trust and confidence, including the author of this paper. However little can be found in the literature on this topic. In many cases trust and confidence is mixed with security, although it is evident that trust and confidence rather relates to *perceived security* than to *security* itself.

In late 2000, the FASME IST project (http://www.fasme.org) has analysed the heterogeneity among 7 European municipalities. One of the results

was that the attitudes of citizens towards authentication technology and data protection were differing severely, and that the opinions of civil servants were rather diametrically opposite to each other. For example, while in one municipality the administration fully accepted the right of citizens to stay anonymous, the administration of another municipality was strongly interested to implement DNA-based authentication. Public opinions on digital ID cards were controversial, and the Italian role concept of the head of family turned out to be rather unique. At that time it seemed rather impossible that the European Union could agree on a joint concept for the use of trust and confidence technology in e-government.

Little convergence has been achieved since then. Several countries have issued electronic identity cards or have identity card projects running: Finland (FinEID), Austria (Bürgerkarte), Belgium (Electronische Identiteitskaart), Estonia (Estonian eID card), Italy (Cartà d'Identita Elettronica), Spain (pilot project with civil servants), and France (Titre Fondateur project). Further, the Swiss Federal Department of Justice and Police has published plans for a digital identity card, in Spain and Norway, local municipalities have issued citizen cards, and the European Union is funding the demonstration project eEpoch, which is supposed to propose solutions for the harmonisation of smart card infrastructure. However, the public enthusiasm for digital identity cards has been modest so far. Estonia had the biggest relative success with approximately 130 000 cards issued.

The cards in use and the card concepts in development differ with respect to the personal data set they carry (protected or unprotected), the ability to store digital documents and multiple applets on the card, and the nature of the CA running the PKI (government or private sector). See chapter 4.6 in [Auerbach 2004] for a detailed comparison. What we are observing is the emergence of increasingly mature identity management technologies, both in e-business and in e-commerce, which will eventually lead to lots of smaller and bigger islands, with very different trust and confidence technologies and data storing principles in use. It might seem a natural attempt to look for interoperable, European-wide scaling solutions, but we shall not pursue that approach. Instead, we shall suggest to fundamentally rethink the concept of trust and confidence in e-government. Is it really so strongly correlated with security and digital identity? And if it is: with which security and identity technologies?

We shall first review several philosophical discussions of trust as well as the historical development of trust in society. Then we shall review trust models for e-commerce and discuss, how they map to e-government. Next we shall present the results of two small empirical investigations among young people, which have been carried out, in our research group, and we shall shortly discuss the perspectives of civil servants. Integrating these per-

spectives, we shall deduce several recommendations for action to increase the trust in e-government.

After having thus analysed trust issues from a conventional point of view, we shall have a look at the meaning of role structures in the public sector and in post-modern society. This will lead us to a novel concept for trust and confidence, based on previous work by several experts from cryptography. Finally, we shall derive an R&D agenda to deal with the resulting open questions.

2. THE PHILOSOPHY OF TRUST

In [Bailey], Tom Bailey sketches a short history of trust in philosophy: "*Trust is as elusive in philosophy as in practice. Philosophers often simply ignore or presuppose it, and when they do consider it, they often struggle to explain it or confuse it with other things. Nonetheless, by considering some major philosophers' thoughts on trust and related matters, we can reveal certain important features of it, and see why it might be so elusive, in both philosophy and practice."* He then surveys the most important theories on trust according to his judgement, opposing Glaucon (Socrates' brother), Machiavelli and Hobbes with Hume, Locke, Kant and Marx. The first group argues that self-interest will always cause a human being to be evil unless fear of detection and punishment threaten him. Machiavelli draws the conclusion that the Medici should commit any cruelty to maintain power. Thomas Hobbes (compare [Hobbes 1994] justifies the existence of the state. He believes that trust makes life simpler and safer and is a precondition for many co-operative activities, but he doubts its rationality in most situations. On the contrary David Hume (compare [Hume 1978]) believes in the good in mankind, as the behaviour of human beings is governed by their remarkable desire for company. John Locke and others even presuppose a shared sense of morality, which may be cultivated to overcome self-interest. Tom Bailey concludes his paper with the thesis, that – different from the opinions of both groups of philosophers – "*my reliance on others can be ensured simply by their taking responsibility for how their behaviour will influence my decisions about how to act in a particular regard*". He then gives examples such as medical doctors, who take some responsibility for our health.

While Bailey's concept reads rather elusively by itself, we think that its main point is the following: Trust means that we believe that someone else will take responsibility for us according to the social role in which she is performing in a particular context. Such a definition fits well with the concept of an independent third party in electronic commerce.

In [Luhmann 2000], Niklas Luhmann describes trust as a means to reduce the social complexity. He highlightens the necessity of trust by stating that no one would be strong enough to leave his bed in the morning without trust: "*Solch eine unvermittelte Konfrontierung mit der äussersten Komplexität der Welt hält kein Mensch aus.*"

Luhmann says that trust is mostly irrational and used to deal with situations where there is a deficit of information or knowledge. Thus, trust arises in conditions where Herbert Simon's *bounded rationality* governs human behaviour, but it is characteristic only for those situations with a considerable risk and a clear orientation towards the future, for which predictions based on trust rather then on information are made. Furthermore, Luhmann notes that familiarity is an important precondition for trust as well as for distrust.

Contrary to Luhmann, in [Coleman 1990] James Coleman describes trust as a rational behaviour related to the calculation of the quotient of two expectation values, which has strong similarities with ROI, namely the expected gain divided by the expected loss. He states that trust increases the bandwidth of possible gains and losses. He stresses the importance of collecting information in order to increase the reliability of the individual estimate of the quotient, which again rephrases the situation of bounded rationality. And he emphasises the role of time in the development of trust towards a person.

Integrating all these partially contradictory views we may say

- Trust relates to risk, caused by incomplete information and/or principal unpredictability
- Trust is needed due to the impossibility to deal with the world in its full complexity, the impossibility to avoid this complexity completely, and the impossibility to protect oneself completely against all risks of evil behaviour from others
- Trust is further motivated by the benefits of co-operation with others, and by the possibility to increase the bandwidth of possible gains
- Trust may be justified in several ways, such as institutional security, the establishment of global moral and role-based, social standards for right behaviour, and the collecting of experience in a relationship
- Trust may (and should) be partially replaced by the collecting of information, thus increasing the rationality of trust.

3. THE HISTORY OF TRUST

Government comprises all activities, which are set up to serve res publica. It has always been a goal of good governance to create trust and confi-

dence for the citizens as a basis for economic behaviour. However, in recent history, the necessity of open exchange with others for the economic success of a society has been understood. Thus government now intends to create trust without creating too many dependencies and other constraints to freedom. A lack of trust prevents co-operative activities and destroys the markets for exchanging goods and services. It thus hinders the success of economy significantly. However, if the price for trust is dependency, this will have similar negative effects as distrust.

Historically, trust was first bound to the family and the tribe. Later on, there were three competing institutions: family, religious organisations (e.g. the Catholic Church), and the government. Ironically, the concept of love, which has been used by Hume and others to explain the human inclination, is a rather modern quality of family, which was attributed to magic rather than to the nature of mankind in earlier times. The concept of friendship may be considered as a much older artificial conceptual extension of family.

In recent centuries, non-profit organisations were formed to support welfare, which implicitly contributes to trust in society. The trust in professional roles of knowledge workers is nowadays a central foundation of trust. Thereby, the trust in a person performing in a particular role is no longer necessarily causally related with the trust in her performing in other roles. Furthermore, in the 20th century the average amount of trust in society has become strongly positively correlated with the health of economy.

Thus we are now facing a much more scattered trust landscape than in earlier times. Religious beliefs are fading. Cultural guarantees (like the handshake in the Alps) are dying out and are increasingly replaced by law technology. On the opposite, economic theory is focussing on trust issues, e.g. when it compares the principal agent theory and the shareholder value concept with the stakeholder concept and the team production model offering a trust dividend. Further, the post-communist period in Eastern Europe has demonstrated that the trust in institutions and the effectiveness of G2B administrative procedures is a key success factor for economy. And the success of digital information and communication technology has created new possibilities and challenges, like biometry for truly secure authentication and Internet business without synchronous interaction.

The complexity of the situation may be one of the reasons why a globally unique and interoperable, digital identity seems to be the silver bullet for trust and confidence as well as for the security of the state. While in earlier times, balanced power among the trust providing institutions (competing for power) provided a maximum of trust and freedom to the people, these days many people are calling for a joining of the forces of all institutions to fight the evil. The capabilities for data networking of digital information and communication technologies may help that this vision becomes reality

(compare [Popp 2004]). However, our empirical investigations have indicated that the networking of trustworthy institutions is perceived as untrustworthy and dangerous.

4. THEORETICAL TRUST MODELS

Most authors discussing trust issues in e-commerce name some or all of the following trust building elements: technical security, protection of privacy, trustworthiness (trust property, trusting beliefs) of the supplier, public reputation of the supplier, certification by a trusted third party, quality of the Web-design, quality of products, and the individual skills of the customer. In particular, they consider trustworthiness of e-commerce to be positively correlated with public reputation. For example, in [Papadopoulou 2001], the following trust properties are given: benevolence, integrity, predictability, competence, ability, credibility, reliability, goodwill, fairness, etc.

There are several models for trust in e-commerce, which describe the interplay of trust building factors, among them [McKnight 2002] and [Egger 2000] (see also [Zachar 2002]. McKnight considers in his model the dependencies among trust building levers (perceived vendor reputation, perceived site quality), trust in vendor (trusting beliefs, trusting intention / willingness), institutional and structural factors (structural assurance of the Web, perceived Web risk), and the behavioural intentions of the customer (intention to follow vendor advice, intention to share personal information with vendor, intention to purchase from site). Egger partitions his trust model into tiers: pre-interactional filters (general intention to trust, general attitude towards e-commerce, reputation, and transference of opinions from others), interface properties (appeal, overview, usability), and information content (products and services, company, security, privacy, communication).

Both models consider site quality, security, reputation, individual skills, and the development of trust as rather important, although they describe these features differently. For example, in [Egger 2003] trust development is implicitly represented by the relationship management for the interaction process, as he stresses the importance of communication. In addition, Egger integrates products and services and privacy into his trust model.

The basic concepts of these models can be transferred to e-government, but we have to consider the differences between e-commerce and e-government when trying to draw up a trust model for e-government. First, the citizen interacts with government in a much richer set of different contexts and life episodes than with a single e-commerce vendor. She has less freedom to choose the interaction and the data collected are often of an especially sensitive nature, e.g. religious belief or personal income. Usually, she

is also aware that data mining is an important technique for government to fight crime and terrorism. Consequently, the networking of these data threatens her more than the networking of e-commerce data, which is why privacy will play a more dominant role in e-government. Second, while in the last years e-commerce customers have learned to distinguish between different providers, e-government is perceived and advertised as one strategic mission of the state. It is thus rather the structural assurance of e-government than that of the Web in general, which counts. Third, in many countries trusting beliefs with respect to government institutions are stronger than with respect to business companies, despite of the fact that public reputation may be lower ("e-government is slow, civil servants are expert sleepers"), while in some countries with a short democratic history they are weaker. Depending on the country, reputation may be little of a problem or a big problem, which has to be handled on a more global scale. However, independent of the reputation, privacy concerns towards government play a major role in most European countries due to history. Fourth, the trust and confidence technology currently considered for e-government is much higher developed than that used in e-commerce. This suggests that e-government could be advertised by stressing its technological advantage with respect to security over e-commerce. Fifth, we conjecture, that e-government is much less known than e-commerce, as it has been appearing more rarely and for a short period of time in the media, which implies that user acceptance is low simply for the fact the a majority of citizens do not know the offers yet. Sixth, since the interaction in e-government is mostly defined by Law, and because in many cases it is perceived as an unpleasant duty, it is not the nature of products, which plays a significant role, but the degree of reduction of interaction efforts. Finally, legal principles require an equal treatment of all citizens. Although that does not explicitly imply equal efforts to establish trust and confidence from all parts of society, there are strong arguments in favour of an equality of trust winning efforts, which pays particular attention to elderly people.

We conclude that the pre-interactional filters in e-government are available information, Internet skills, assumed privacy and security risks, the attitude towards e-government as a whole – and in some countries the lack of reputation. The usability is part of the product/service, and it may dominate the general distrust in the Internet or e-government services. This is particularly true, if the time spent on the unpopular interaction with public administration is significantly shortened. Further, rich communication facilities will increase the trust-worthiness of the e-government services. Thus, [McKnight 2002] and [Egger 2000] partially apply to e-government, but the priorities there are rather different and they depend on the country.

5. EMPIRICAL INVESTIGATIONS

The target group for the empirical investigations in our research group was young people in Zurich. We did not intend to obtain representative numbers, but rather we wanted to identify trends among young people since they are opinion leaders with respect to the use of Internet technology. Due to the globalisation of youth culture, these trends are likely to generalise to the whole of Europe. However, the impact of the long and special tradition of direct democracy in Switzerland should be taken into account. Although voting is much more complex in Switzerland than in most other democratic countries, young people are very well informed about the traditional voting procedures.

In the fist study (see [Pfleghart 2003]) 166 pupils in the canton of Zurich, between 17 and 21 years of age, answered a questionnaire on e-voting. In the second study (see [Zumsteg 2004] 371 students of the University of Zurich answered a more complete questionnaire on e-government as a whole.

5.1 E-Democracy and the 80-20 Law

Based on the assumption that only people searching for political information on the Web would use e-voting, in [Lindner 2001] it was estimated that the overall increase of participation in votings could be at most 3.5%. The results of the first study exhibit a typical 80-20 law with respect to e-democracy other than e-voting and they strongly question the above type of reasoning. About 80% had no interest to discuss on politics via the Internet and did not use the Internet to access political information, although they were collecting political information from newspapers and the Bundesbüchlein. However, 60% said they wanted Internet voting using the web-browser, although half of them had strong doubts that electronic voting was safe from manipulation, two third were somewhat or strongly concerned that electronic votes could be lost, and half of them were concerned about possible violations of anonymity. Thus, the pupils between 17 and 21 years had strong interests in web-based e-voting, despite of the fact that they distrusted its security, but they had little interest in other forms of democracy.

5.2 Contradicting Opinions and Lack of Information

The second study among students at the University of Zurich has shown that 70% are using the Internet on a daily basis. When asked whether they would have a stronger trust in government or in commercial companies, half of them preferred government and one eighth preferred business. A more detailed analysis showed, that trust in Justice was strongest, followed by

trust in the national government, which was better trusted than public administration and the Houses of Parliament.

Internet voting was nearly equally popular as voting by mail (75%), and twice as popular as ballot box voting (40%). Half of the students had serious security concerns, but nearly 80% said that they would use e-voting despite of their concerns. Nevertheless, only 10% had a considerable knowledge about the first Swiss e-voting trial!

The situation was similar for the electronic submission of tax declarations: 60% wanted to submit the tax declaration electronically, but 50% noted that they had privacy and security concerns, although 80% considered the technology itself to be trustworthy. Further, more than 50% said they would not use e-assistance services if they had to provide personal data.

Among the measures to reduce fears, the use of digital ID Cards and the declaration on data protection on the Web-site were considered most important, followed by the information provided by family and friends. Furthermore, the possibilities to contact the administration by e-mail or phone, information about security on the Web-site, the use of biometric authentication, easy navigation on the site, cost reductions (e.g. for e-taxes), information from the media, and help-buttons on the Web-site were considered as useful, in the order they are cited here.

Part of these observations might seem to constitute a contradiction in itself, but we think that they reflect three important facts

- trust and confidence are emotionally perceived, not intellectually (which is why contradictions may occur)
- the Swiss government has failed to properly inform about e-government and e-democracy initiatives (which is why contradictions are likely as many citizens have not much thought about the issues they are concerned about)
- the benefits of e-services are considered higher than the risks by young people in Switzerland (which is why significant concerns do not hinder user acceptance)

Finally, we asked which of the e-government Web-sites were known. The result was remarkable: Nearly 80% did not know the Swiss national e-government portal www.ch.ch at all and only 6% had visited it.

5.2.1 Summary

There was no statistically relevant correlation between experience and attitudes. E-voting via Web-browsers and electronic submission of tax-declarations enjoy a high acceptance. Indeed, the benefits of e-voting are considered to be more important than the strong concerns about it. On the contrary, e-assistance earns user acceptance only if users do not have to pro-

vide personal data. The most important concerns are privacy and lack of security. The biggest deficit so far is the failure of PR activities for e-government. Students all make extensive use of the Internet, but they simply do not know about high profile activities. Remarkably enough, the less direct contacts students have with forms of e-government, the better they trust them. However, there is also a strong concern that privacy might be in danger when one uses e-government services.

These results confirm our conclusions in section 4, drawn from previous trust models for e-commerce. Furthermore, James Coleman's definition of trust is confirmed: It is the quotient of gain (multiplied by its likelihood, compare the results on e-assistance) and risk which determines trust. On the contrary, Niklas Luhmann's assumption that familiarity is a precondition for trust or distrust does not seem to hold in this context.

6. CIVIL SERVANT PERSPECTIVES

The views from civil servants somewhat differ from those of citizens. For example, in [Knörri 2003], security for the e-voting in Zurich is depicted as made up of four elements: technical security (30%), security through organisation (40%), security through threatened punishment (20%), and security through user handling (10%). We may observe the combination of traditional concepts (Glaucon and Hobbes, although in the absence of Machiavelli) with modern concepts of effective government, inspired by the management concepts in [Drucker 2001]. In two personal interviews, Knörri who is a civil servant himself has confirmed the importance of organisational security, usability, and pilot projects. However he was much less enthusiastic towards an early integration of users and an early information of the public. Furthermore, he said that the use of open source software for e-voting projects was an academic idea, which was no option for e-voting in practice.

This clearly shows that there is a strong distrust in transparency among civil servants. Other studies carried out in our research group have confirmed this observation (see [Sidler 2003]. Rather than protecting data, it is data protection, which is highly protected and kept secret by the civil servants implementing new data pools.

7. RECOMMENDATIONS FOR ACTION

The following recommendations try to combine the theoretical and the empirical findings above with the opinions observed in interviews and e-

mail communication with civil servants. They address current development of e-government solutions rather than R&D issues.

1. Develop a risk-sensitive integrated road map for all national e-government initiatives. One failure of a high risk application might block all activities
2. Use state of the art security technology – and do advertise that fact!
3. Consider the introduction of digital identity cards[4] - or a similar solution with corresponding functionality but improved privacy.
4. Respect data protection carefully and talk about it. Clear and easy to understand declarations of pursued privacy policies are a must.
5. Design easy-to-navigate Web-sites for all and keep in mind that usability is part of the value of an e-government service. People want to use e-government services because they expect that the time spent on them will be much less than with traditional government services.
6. Start to advertise the e-government services. The attitude to keep pilot projects secret points in the direction of failure. The time has come to really talk with the citizens about e-government.
7. Consider the needs of the citizens and perform empirical studies!

Our investigations obviously do not generalise to all sectors of society in Switzerland, the less to Europe as a whole. However, they demonstrate that folklore is wrong. For example, trust is not always a precondition for user acceptance. Or rather, it is trust in the sense of Coleman, which counts, not trust in general. In depth empirical studies are needed for a better understanding of the reasons for trust and the impact of trust.

8. RETHINKING IDENTITY

We have seen that data protection is a key issue for trust in e-government services. Rather than patching violations of privacy wherever they occur, we suggest to completely rethink digital identity as a whole in order to develop sustainable solutions for the future.

8.1 Privacy, Government, and Post-Modern Reality

Electronic Government, or e-Government, comprises all aspects of *the use of digital information and communication technology in the public sector* including the resulting structural *change*. Technological developments,

[4] Unfortunately, biometric technology is not ready yet for a use which confirms to the European guidelines on the protection of biometric data.

information, and productivity are not at the heart of e-government, as they are not a primary concern of modern society. It is the managed institution being an instrument of society, which creates results (compare [Drucker 2001].

But how do these institutions, how does the public sector work? It is based on a clear role structure. There is a long tradition, dating back thousands of years, that the role is more important than its performer. The structural design of e-government solutions must implement these role structures.

E-government creates a new, virtual public space, but how do the role structures in real public space develop? Since several decades, the public space is increasingly being invaded by private life. This means, that the distributed context structure of public space is much more scattered and heterogeneous as it used to be. Social rules for behaviour in public are less stringent but also more difficult to understand. The virtual public space of e-government has to be designed according to the needs of the citizen. It must not ignore cultural trends of the presence, and thus, it must admit a rich mix of role-structures and context definitions.

We are living in post-modern society. What are the consequences for our communication habits in private and in public? The coupling of the roles we play in different communication channels gets looser and looser. We focus more on the context, as we have been taught that the message is created at the receiver. Our statements are usually made with explicit or implicit reference to a context. If that context is removed, our words are more contradictory than it would have been socially accepted a hundred years ago. Western communication style thus approaches African traditions of personal relationship management. As a consequence, the real threat to our identity is not, that privacy is violated in a known context, but that personal data are stripped their context and combined for a context unknown to their producers.

Our identity is more open and fragmented than it used to be hundred years ago. It consists of all the roles in which we are performing in different contexts. Thus it is made up of situated identities. Our interaction with the Internet creates personal data, the sum of which constitutes our digital identity. However, these situated data are valid for a particular context only. Combining digital from different strongly roles violates our privacy. This observation is represented by the context principle in European data protection principles[5]. Personal data created and stored for one context must not automatically be reused in another context.

[5] Directive 95/46/EC

We thus conclude that the public sector and post-modern reality are both furnished with rich role structures, which are becoming increasingly complex. The design of e-government solutions must support these role structures and their management by the citizens and the government agencies (although organisational measures have to take care that no definition of roles for the sake of the exploitation of technology takes place). Further care has to be taken that only productive role structures and role structures with productive side-effects on the institutional culture are designed and implemented. These considerations lead us to a new concept of digital identity, where the certificates of identity do not necessarily provide the name of the certified citizen, but only some of her attributes.

8.2 A Holistic Concept for Identity

In its broadest sense, digital identity may be understood as the set of all personal data of a person (compare [Köhntopp 2001]). Subsets of these data represent partial identities. Any certified subset of these data constitutes a trustworthy digital identity. We usually use the term "credential" for such a certificate. If it is impossible to identify the represented person from the partial digital identity given, we may call it an anonymous digital identity. Depending on the existence of certificates this anonymous digital identity may be trustworthy or not. If there is a means to provide evidence that one owns a trustworthy digital identity (i.e. that a set of personal data is a valid description of oneself) without creating an identifiable digital trace, this constitutes an untraceable trustworthy digital identity, which by its very definition is anonymous.

Trustworthy partial digital identities may be used to access digital services based on a role concept. The latter means that authorisation to access a service is based on an access control list made up of pairs of roles and trust levels. A role consists of attributes, i.e. it is an anonymous partial digital identity, and a trust level defines the rules to accept a certification of a role, that is the credential. If credentials are non-traceable, then it is impossible to violate the privacy of the credential holder without his notice: Citizens performing in different roles cannot be traced across roles. In fact, even more is true: In general, it is impossible to deduce how many persons are personifying a role.

Several mathematical concepts for such credential systems have been developed, e.g. [Chaum 1987], [Brands 2000], and [Camenisch 1999]. The last one presents to the best of our knowledge the up to date most advanced credential technology. It has the following properties (among others): The user has control over her data and her transactions are not linkable. Organisations do not know the identity of the user, but only her pseudonym. The revoca-

tion of credentials in case of fraud is possible. And based on the credential protocol alone, co-operating users are not able to receive credentials which they would not receive without co-operation.

IT architectures have been designed and prototypically evaluated which use this credential technology for real world scenarios. In particular, it has been shown that it is possible to anonymously access different e-government services through a single-window e-government broker ([Király 2003]) as long as now tracing based on lower level protocols is possible (see [Roduner 2003]). We may conclude from these results that a system of digital identities is technically feasible, although lots of technical problems exist to be solved yet. Thus, for the future our suggestion number 3 in chapter 7 should be rewritten: Make use of credential technology for the implementation of trustworthy digital identity!

This statement is supported by the fact that European data protection principles require that the storage of personal data has to comply with the context needs in size and quality. It is not admissible that more data are stored than needed. This implies in particular, that any transaction, which can be carried out anonymously, must be carried out anonymously. Trustworthy anonymity guarantees data quality and widens the range of e-government transactions which do not require the name of an involved citizen to be given- It thus strengthens privacy protection and it provides a most elegant implementation of the data protection principles.

8.3 Time for Decisions

Any holistic concept of digital identity should exhibit the following three properties

1. It should support role structures and digital interaction based on these role structures.
2. It should enable the citizen to control her privacy and her relationships with organisations offering digital services to a maximal extent, which requires that she controls the distribution of her personal data
3. The risk of identity theft and of any crime through the manipulation of the relationships between a citizen and organisations offering digital services should be kept to a minimum.

Credential technology fulfils requirements 2 and 3 to a large extent. Since there is a one-to-one correspondence between credentials and roles, credential technology is the natural candidate for the implementation of the role concept in future IT solutions for e-government.

The next steps in e-government will be concerned with GAI – government application integration. In [Leitner 2003], chapter 4 of part 1, the vision of future integrated e-government is depicted. Its implementation will

decide what digital identity will be like in the next decades. Integrated e-government requires G2G integration, which in turn requires a clear concept of identity. Once this concept has been coded in expensive software it will persist for a long time. We have to decide now, if we want to implement a full protection of privacy or not.

9. RESEARCH AGENDA

As we have argued above, there is a strong need for both a better protection of privacy and a better digital support of post-modern role structures. This puts the following issues on our R&D agenda:

User acceptance for anonymous digital identity & usability of credential management systems. Trustworthy anonymous digital identity is not a trivial concept. It provides a means for risk avoidance, but not an affordance by itself, which should be communicated clearly. Keeping control over all personal data, which we have spread in the world, is impossible so far. But even if technology, service provider acceptance and the support from government would provide us with the technical capabilities to track and control our lots of partial digital identities, this would be an enormous cognitive challenge. Therefore, credential management systems are needed, which are easy to understand and use for all and which enable users to effectively manage privacy risks rather than to track their individual relationships with service providers in detail and to control all their partial identities one by one.

Process analysis with respect to the legal needs to use fully identifiable personal data. From a technological point of view, it seems to be possible to design e-tax services based on anonymous credentials. For example, based on the credential system presented in [Camenisch 1999], the extended digital identity concept in [Auerbach 2004] and the IT architecture for anonymous service access in [Király 2003], this could be achieved by the following type of script (see [Riedl 2004]), where the root-CA (root credential authority) controls whether a citizen has paid her taxes or not:

1. Root-CA sends a request to each registered citizen to fill in his tax declaration form. 2. Each citizen requests and obtains wages credentials from her employer and expenses credentials for all expenses she may subtract from her income before taxation. She then submits her tax declaration form together with all credentials to the tax office. 3. The tax office requests and gets transcripts for all citizen credentials from a revocation manager. It delivers theses transcripts to the root-CA, which does a global revocation and checks whether all credentials belong to the same main secret, and then reports ok or not ok to the tax office. 4. Based on the answer of the root-CA,

the tax office creates a 'taxes paid' credential and sends it to the citizen, who may thus prove to the root-CA that she has paid her taxes.

This protocol would prevent any linking of the actual contents of the tax file with the name of the citizen. However, it is unclear whether the implementation of such a protocol is legally admissible and organisationally feasible. Likewise a wide range of traditional e-government services could be implemented with trustworthy anonymous digital identity and similar scripts. Therefore, an extensive investigation on the legal and organisational constraints for administrative processes with unidentified citizens seems to be worthwhile. Clearly, most e-assistance services will be within the practical application domain for trustworthy anonymous digital identity, but in other cases the situation is unclear.

Development of design principles for balancing the complexity of role structures in an information society. The more complex the role structures are and the more advanced e-government services are, the more difficult it will be to control one's personal data affiliated with particular roles and the more difficult the implementation of security infrastructure is – in particular when the need for delegation of rights comes into play. What we need is a new discipline of transparency engineering. In distributed systems terminology, transparency has a double meaning, namely "single system image" as a technical design goal and "visibility of crucial activities" as an organisational design goal. From the user perspective, digital identity management should provide a balanced transparency that allows her to handle technical and organisational complexity in a way, which is optimal for her abilities and life contexts. This implies that customised user interfaces with differing degrees of complexity must be provided by the digital identity management system and that the role structure and the application structure are designed appropriately. The latter is a conditio sine qua non for the success of holistic identity concepts in a highly heterogeneous and cognitively challenging world. Therefore, research on useful role structures for the public sector is needed, which should be performed jointly with research on transparency engineering for IT architectures.

Development of a PCI (public credential infrastructure) concept analogous to PKI & development of standardised ontologies to achieve European-wide interoperability of future credential architectures. The deployment of credential technology on a larger scale in practice requires the development of a PCI, which is an extension of the well-known PKI (compare e.g. [Austin 2001]), as it has to deal with richer forms of revocation. Thereby, the analogues of the CP (certification policy) and the CPS (certification practice statement) play an important role. One of the critical issues is the scalability of revocation mechanisms; another is the lack of ontologies to write credentials, which can be used throughout Europe.

The famous example for the likely conceptual failure of cross-border use of credentials is the statement "Mr X is married." issued by a Dutch government agency. The statement does not declare the gender of the marriage partner of Mr X and thus will not be accepted by countries where same sex marriage is not admissible, even if that statement itself is accepted as his marriage partner is a woman. The famous example for the likely practical failure is the proverbial English power bill used to prove evidence of living place, but probably not understood as such by a German authority. Other examples for conceptual and/or practical problems are the unique Italian concept of auto-certification or the German 'unwillingness' to issue any digital certificates (as we could observe it in the eMayor project: http://www.emayor.org). Thus, the two key problems that may hinder a European-wide use of identity management based on credential technology are identical terms describing similar but different concepts and differences in certification cultures.

Empirical studies differentiating target groups according to age, social position, and cultural identity. The bottom line of any research agenda on trust and confidence should be that it addresses the fears and cultural traditions of the people. This requires extensive empirical studies in order to understand the security concerns of citizens

9.1 Roadmap for Research

Summing up, we conclude that a lot of transdisciplinary co-operation is required due to the complex interplay of very different issues, which have to be handled by experts from different disciplines. The roadmap for R&D should be as follows

1. Building a set of trust models for e-government, which depict the full heterogeneity of Europe and which are based on empirical investigations (on a much broader scale than those presented in this paper)
2. Designing a new social and organisational 'architecture' for the future public sector, which is based on a role structure and new co-operation models (which reflect dissolving boundaries and trust structures as well as the growing self-responsibility of citizens and the growing importance of trusted non-profit organisations)
3. Rethinking and renegotiating legal requirements for IT-architectures providing global digital identity management and (nearly) ubiquitous, cross-organisational and cross-border access to e-government services (based on a flexible concept for the interface between Law and IT architecture)
4. Developing a PCI and ontologies for European-wide e-government and developing a security framework architecture for government

application integration, for government-to-government co-operation and for (the thus enabled) secure, borderless one-stop e-government services for citizens

5. Developing user-friendly and barrier-free digital identity management systems, which enable users to control their 'digital identity' in a complex information society (and which are part of a general concept for the presentation tier in government application integration)

These R&D activities should be accompanied by two transversal activities

- Basic research on transparency engineering, which addresses the citizen to e-government/e-business/e-commerce applications interaction
- Public discussion of emerging e-government solutions to gain democratic support for the future reorganisation of the public sector

In order for such a roadmap to become reality, significant efforts are needed to nurture interdisciplinary co-operation and the convergence of existing expertises.

9.2 Looking Beyond European Borders

The quality of e-government has to be measured with respect to several different yardsticks, probably the most important of which is the joint existence of trust and confidence and of freedom in society. Some of the issues discussed in this paper, e.g. the heterogeneity of Europe, are typically European. But is the whole world less complex than its part? Is data protection only a need of young Swiss people, young Europeans, the European society? Are Swiss or European people special and more critical of data misuse? Is post-modern reality only a European phenomenon? We suggest that the research vision pursued targets the development of holistic IT solutions for digital identity, which scale to a world-wise usage both in the public and the private sector.

ACKNOWLEDGEMENTS

This paper is in parts based on the theses written by several students of our research group: Niklas Auerbach, András Király, Michael Pfleghart, Christof Roduner, Andreas Sidler, and Franziska Zumsteg.

REFERENCES

[Auerbach 2004] N. Auerbach, Anonymous Digital Identity in e-Government, Thesis, University of Zurich (to appear)

[Austin 2001] T. Austin, PKI – A Wiley Tech Brief, John Wiley & Sons, 2001

[Bayley 2002] T. Bailey, On Trust and Philosophy http://www.open2.net/trust/downloads/docs/ontrust.pdf

[Brands 2000] S. A. Brands, Rethinking Public Key Infrastructures and Digital Certificates, MIT Press, Cambridge, Mass., USA, August 2000

[Camenisch 1999] J. Camenisch and A. Lysyanskaya, An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation, vol 2045 of Lecture Notes in Computer Science, 93-118, Springer Verlag, January 1999

[Coleman 1990] J.S. Coleman, Foundations of Social Theory, Cambridge, Mass. USA 1990.

[Chaum 1985] D. Chaum, Security without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, 28(10), 1030-1044, October 1985

[Drucker 2001] P. Drucker, Management for the 21st Century, Chapter 1, Harper Business 2001

[Egger 2000] F.N. Egger, Towards a Model of Trust for E-Commerce System Design, http://www.zurich.ibm.com/~mrs/chi2000/contributions/egger.html

[Hobbes 1994] T, Hobbes, Leviathan, with Selected Variants From the Latin Edition of 1668, edited by E. Curley, Hackett, 1994.

[Hume 1994] D. Hume, A Treatise of Human Nature, edited by L.A. Selby-Bigge, revised by P.H. Nidditch, Oxford University Press, 1978

[Király 2003] A. Király, Credential-Based Implementations of Digital Indentity for Non-Traceable Access to E-Government-Services (in German), http://www.ifi.unizh.ch/egov/Diplom_Kiraly.pdf, Master's Thesis, November 2003.

[Köhntopp 2001] M. Köhntopp, A. Pfitzmann, Identity Management and ist Support of Multi-lateral Security, Computer Networks, 37: 205-219, 2001

[Knöri 2003] D. Knöri, e-Voting des Kantons Zürich, http://www.statistik.ch/projekte/evoting/e-Voting.ppt

[Leitner 2003] C. Leitner (editor), J.-M. Eymeri, K. Lenk, M.M. Nielsen, R. Traunmüller (authors), F. Heinderyckx, A. Moussalli, M.A. Wimmer (contributors), eGovernment in Europe: The State of affairs, European Institute of Public Administration, 2003.

[Luhmann 2000] N. Luhmann, Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität., 4. Auflage. Stuttgart: Lucius und Lucius, 2000.

[McKnight 2002] D.H. McKnight, V. Choudhury, and C. Kacmar, The Impact of Initial Consumer Trust on Intentions to Transact with Web Sites: A Trust Building Model, Journal of Strategic Information Systems 11,297 – 323, 2002.

[Papadopoulou 2001] P. Papadopoulou, A. Andreou, P. Kanellis, D. Matakos, Trust and Relationship in Electronic Commerce, Internet Research: Electronic Networking Applications and Policy, Vol 11, No 4, 322 – 332, 2001

[Pfleghart 2003] M. Pfleghart, E-Voting im Kanton Zürich aus der Perspective junger Bürgerinnen, http://www.ifi.unizh.ch/egov/Diplom_Roduner.pdf, Master's Thesis, January 2003.

[Popp 2004] R. Popp, T. Armour, T. Senator, and K. Numtych, Contering Terrorism through Information Technology, Communications of the ACM, Vol 47, No 3, 36-43, 2004

[Riedl 2004] R. Riedl, A. Király, Anonyme digitale Identität im E-Commerce and E-Government, in preparation for Tagungsband des Rechtsinformatiksymposiums IRIS 2004

[Roduner 2003] C. Roduner, Citizen Controlled Data Protection in a Smart World, http://www.ifi.unizh.cn/egov/Diplom_Roduner.pdf, Master's Thesis, November 2003.

[Sidler 2003] A. Sidler, Datenschutz im E-Government, http://www.ifi.unizh.ch/egov/Diplom_Sidler.pdf, Master's Thesis, December 2003

[Zachar 2002] T. Zachar Antropomorhe Agenten in kommerziellen Webseiten und ihr Einfluss auf das Nutzervertrauen, http://www.cmr.fu-berlin.de/research/diplom/documents/zachar.pdf, Master's Thesis, 2002,

[Zumsteg 2004] F. Zumsteg, Die Bedeutung von Vertrauen flur den Erfolg von E-Government, http://www.ifi.unizh.ch/egov/Diplom_Zumsteg.pdf, Master's Thesis, January 2004