

Secure Offline Legitimation Systems

**Dissertation
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
der Universität Dortmund
am Fachbereich Informatik**

**von
Gerrit Bleumer**

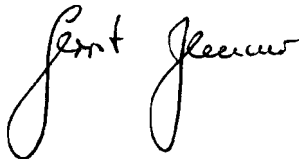
**Dortmund
2001**

Tag der mündlichen Prüfung: 19. Oktober 2001

Dekan: Prof. Dr. Bernd Reusch

Gutachter: Prof. Dr. Joachim Biskup (Erstgutachter),
Prof. Dr. Birgit Pfitzmann (Zweitgutachterin),
Prof. Dr. Horst Wedde,
Prof. Dr. Heiko Krumm (Vorsitzender des Prüfungsausschusses),
Dr. Peter Kemper.

Schildow, den 07. September 2004

A handwritten signature in black ink, appearing to read 'Gerrit Bleumer'. The signature is written in a cursive style with a large initial 'G' and a long horizontal stroke.

(Gerrit Bleumer)

Foreword

*“Engineers must study not only what technologies can do FOR people
but also what they do TO people,
and they must learn to steer technology
more sensitively and skillfully through the political process.”*

— Edward Wenk [225]

(Science Advisor to three US presidents)

While our modern societies rapidly turn into information societies, powerful players like governments, secret services and public prosecutors ever more strongly demand for complete surveillance of fax, phone, e-mail, payment transactions and more. However, this thesis advocates to design the information infrastructures so that they can respect and enforce the legitimate security interests of ALL participants, be they active users or passive uses¹ of the computer systems. So the pleading at the heart of this thesis is:

*As little observability of citizens in every day’s transactions and
as much security against misuse and fraud as possible.*

This is not an impossible dream, this is a vision that can become reality if citizens are getting more conscious and demanding rather than getting distracted by the exciting features of today’s applications. The customers, employers, tax payers, voters, i.e., all individuals of an information society, perform numerous transactions with each other and with provider organizations every day. Almost any of these transactions leaves digital traces about individual clients at the provider’s organization. Since digital traces are easily accumulated into digital profiles on individual behavior, the privacy of any individual is at risk. The problem should neither be disregarded as a hobbyhorse of some frustrated researchers or as the paranoia of some radical dropouts; it is a serious threat to democratic societies. Privacy threats are insidious for two reasons. (i) They are not easy to quantify because its impacts are

1) The term “usee” describes those whose data is processed by computer systems but who usually do not use these computer systems themselves.

diffuse: What happens if patients face the fact that their medical records including genetic fingerprints are released or sold to third parties, e.g., employers, insurance companies, pharmaceutical suppliers? How will citizens (and also small enterprises) react if information about their consuming behavior, social and political activities is available as digital goods on the Web? It is unrealistic to assume that conformity to majority opinions would not increase under such conditions. (ii) Privacy threats are easily overlooked because individuals do not *feel* to be observed, therefore do not feel to be threatened individually, and therefore feel little need to defend themselves appropriately. Unlike countries or large enterprises engaged in *information warfare* [97], individuals seldom know their observers, can hardly measure their loss of privacy, are usually not organized and only few are skilled to take appropriate countermeasures. (iii) Privacy threats are ubiquitous through the installation of video cameras and other biometric scanning technology. Places of public interest, roads, tunnels, bridges, gas stations, train stations, airports, and ATM are only a few examples of non-stop video monitoring. The next generation of public key infrastructures will replace passwords by biometric recognition facilities. A profound overview of surveillance technologies has been compiled by DuncanCampbell [55] for the STOA unit of the European Parliament and was presented to the European Parliament. Simson Garfinkel has published a thorough analysis of privacy threats in the US [115].

The threat to privacy is illustrated by an episode in 1996 that has been partially documented at the Cambridge Workshop on “Personal Medical Information — Security, Engineering, and Ethics” [2]. The British National Health Service (NHS) had proposed to build a UK-wide medical network in order to increase efficiency of all transactions between General Practitioners (GPs), clinics, hospitals, pharmacies and other points of care. After serious and persistent requests, it was promised that patient data should not be sent in clear but only in encrypted form and the NHS as a national organization had therefore looked for a method that was acceptable to the intelligence community. The NHS was advised (if not oppressed) to employ an unpublished encryption mechanism called “redpike”. The service’s obvious intention was to keep easy access to all data sent along the medical network. Had only the patients been affected, this proposal supposedly would have been accepted without much noise. In this case however, many medical doctors have felt not only their patients’ privacy threatened but also their own, and so the British Medical Association (BMA) started a campaign against the NHS proposal. (The controversy died out later because the NHS did not pursue the original plan further.)

Evidently, anonymity is not an end in itself. In small communities, anonymity can be counterproductive, and even in large societies it has to be balanced against other legitimate interests like for example fighting organized crime, terrorism and money laundry. It shall be shown that for not so small classes of applications fair privacy protecting solutions exist. It must be left to the democratic process to decide about which technical infrastructures we want to face in the next millennium.

Abstract

Organizing the interdependencies within and between communities is one of the ongoing challenges of mankind. Once organizations are formed, companies run their businesses, and a legal system is in place, there is an urgent need for procedures to perform legally binding transactions. This in turn brings up the need for unforgeable documents or tokens of legitimation. Traditional examples are letters and cheques with handwritten signatures or seals, hard-to-counterfeit bills, drivers licences and passports with hardly removable pictures imprinted, etc. The implementations of legitimations change as the technological paradigms change, but the need for legitimations persists. In information societies, many of the traditional implementations are obsolete because they are no longer efficient and often too costly. In addition, information technology often provides better approximations to the ideal properties of legitimations, e.g. unforgeability. Electronic commerce is one if not the pioneering area where the new implementations of legitimations are developed, tested and put into everyday's practice. Examples are electronic wallets, phone cards, e-cash, e-tickets, etc.

While an amount of money can be regarded as a legitimation to consume a corresponding portion of the national gross product, there are also other kinds of legitimations. This work starts by categorizing them and identifying important examples in real life. Namely, we distinguish *personal* and *coin legitimations*. The former cannot be transferred between holders and the latter cannot be used more often than a pre-specified limit. Orthogonal to these categories then are privacy requirements. This is where electronic implementations are really superior to traditional implementations: Not only are they more efficient, but they can achieve more privacy for holders of legitimations than the conventional paper based implementations can. Such electronic implementations have been introduced in 1985 by Chaum [60] as *credentials*. Holders can get a credential from an issuer and later show it to a verifier without letting the issuer and verifiers recognize that they have issued and verified a credential of the same holder (*unlinkability*). Although several cryptographic mechanisms for credentials have been suggested since, formal definitions have been given only for the special case of electronic cash. We propose a formal modular framework to define the different categories of credentials sketched above (including electronic cash). Furthermore, we suggest the first mechanism for personal credentials that can be shown many times in an unlinkable way. In order to achieve non-transferability, we suggest the use of

biometric verification of holders without releasing any biometric data to more or less centralized databases where they could be aggregated, analyzed and re-used in unintended ways.

In addition to privacy of holders, we also consider privacy of issuers of credentials (against verifiers). This turns out to be useful in more complex applications. The final section presents the detailed design of how compulsory health insurances can be billed without the health insurers even learning which physician is treating which patient, let alone which patient gets which therapy or medicament. This way, the trust relationship between patients and physicians can be protected optimally, and it is nevertheless possible to identify falsely claiming physicians after the fact.

Kurzfassung

Eine ständige Herausforderung jeder Gesellschaft ist es, einen verlässlichen Rahmen für die Beziehungen ihrer Mitglieder (Individuen und Gruppen) herzustellen und aufrechtzuerhalten. Sobald Organisationen gegründet sind, Firmen ihre Geschäfte betreiben und ein Rechtssystem installiert ist, werden Verfahren zur rechtsverbindlichen Interaktion benötigt. Dies wiederum erfordert fälschungssichere Dokumente oder Ausweise. Traditionelle Beispiele sind gesiegelte oder unterschriebene Briefe, unterschriebene Schecks, schwer fälschbare Geldscheine, Führerscheine oder Reisepässe mit aufgedruckten Passbildern. Die Form der Legitimationen mag sich entsprechend der technologischen Paradigmen einer Gesellschaft verändern und weiterentwickeln, aber die grundsätzliche Notwendigkeit von Legitimationen bleibt bestehen. In einer Informationsgesellschaft sind viele der herkömmlichen, d.h. papiergestützten Formen überholt, weil sie zu ineffizient und oft auch zu teuer sind. Überdies erlaubt Informationstechnologie häufig bessere Annäherungen an die idealen Eigenschaften von Legitimationen, z.B. Unfälschbarkeit. E-Commerce, ist eines wenn nicht sogar das führende Gebiet, auf dem die zukünftigen Formen von Legitimationen entwickelt, erprobt, und wahrscheinlich auch flächendeckend eingesetzt werden. Beispiele sind elektronische Brieftaschen, Geldkarten, e-cash, e-tickets, etc.

Es gibt neben Geld weitere Sorten von Legitimationen², und die vorliegende Arbeit beginnt mit ihrer Klassifizierung illustriert durch praktische Beispiele. Im wesentlichen unterscheiden wir zwischen persönlichen und Münz-Legitimationen. Erstere können unter Besitzern nicht weitergegeben werden, während letztere nur begrenzt oft benutzt werden können. Orthogonal zu dieser Unterscheidung betrachten wir Anonymitätsanforderungen—oder stärker Unverkettbarkeitsanforderungen der Besitzer von Legitimationen. Auf diesem Gebiet bieten digitale Implementierungen von Legitimationen qualitative Vorteile gegenüber herkömmlichen: Sie sind nicht nur effizienter herzustellen, zu speichern und zu prüfen, sondern können tatsächlich Unverkettbarkeit der Transaktionen desselben Besitzers erzielen. Kryptographische Implementierungen sind erstmals 1985 von Chaum [60] untersucht und unter dem

2) Volkswirtschaftlich kann Geld als Legitimation oder Anspruch auf einen entsprechenden Teil des Bruttosozialprodukts angesehen werden.

Begriff *Credentials* eingeführt worden. Hier kann ein Besitzer sein Credential von einem Anbieter bekommen und es später einem Dritten (Prüfer) zeigen, ohne daß Anbieter und Prüfer hinterher erkennen könnten, daß sie mit demselben Besitzer zu tun hatten. Obwohl seitdem mehrere Verfahren für Credentials vorgeschlagen worden sind, gibt es formale Definitionen bisher nur für den Spezialfall Münz-Credentials. Wir geben eine formale modulare Definition für alle oben beschriebenen Arten von Credentials. Weiterhin geben wir die erste Konstruktion für persönliche Credentials, die mehrfach unverkettbar gezeigt werden können. Um Weitergabe der Credentials zu verhindern, untersuchen wir den Einsatz biometrischer Erkennungsverfahren, wobei die biometrischen Daten der Credentialbesitzer nicht in zentrale Datenbanken gelangen können, in denen sie gesammelt, analysiert und in unerwünschter Weise weiterverwendet werden könnten.

Über die Unverkettbarkeitsforderungen von Besitzern hinaus betrachten wir hier erstmals auch Anonymitätsforderungen der Anbieter gegen Prüfer von Credentials. Dies kann in komplexeren Anwendungsgebieten wünschenswert oder nötig sein. Im letzten Kapitel entwerfen wir detailliert, wie mit gesetzlichen Krankenversicherungen so abgerechnet werden kann, daß die Versicherer nicht einmal erfahren, welcher Arzt welchen Versicherten behandelt, geschweige denn welcher Patient welche Behandlung und welches Medikament bekommt. Auf diese Weise wird das Vertrauensverhältnis zwischen Arzt und Patient optimal geschützt, und dennoch können Ärzte nachträglich identifiziert und zur Verantwortung gezogen werden, wenn sie nicht erbrachte Leistungen abrechnen oder überhöhte Gebühren in Rechnung stellen.

Acknowledgments

My research period at the University of Hildesheim started with Joachim Biskup as senior supervisor and Andreas Pfitzmann and Birgit Pfitzmann as junior supervisors. I have much appreciated the liberal and productive atmosphere that Joachim Biskup has created and has let grow. He did not get nervous when I took several weeks looking after a new kind of protocol but showed interest in everything I did. Without this period of unfettered research this thesis would not have been finished. Back in 1990, Joachim Biskup proposed to explore security issues in medical payment systems [18] under the AIM program (Advance Informatics in Medicine) [78], which was sponsored by the European Commission from 1992 through 1995 by about 120 Mio. ECU. Under that program, I have made a lot of experience about security and other aspects of computerizing the medical sector.

About five years ago, Andreas Pfitzmann suggested to me the high level idea of credentials that do not only protect the privacy of holders but also that of issuers. At that time, none of us had the faintest idea how to arrive at practical solutions. The cryptographic primitives that finally turned out to help solving the problem had only just been published and in a sense, the idea was ahead of its time.

At about that time, Birgit Pfitzmann pointed out to me that the concept of personal credentials, i.e., credentials that refer to a particular human being, need to include some biometric mechanism in order to link the digital credentials to the biological beings in a non-repudiable way. This problem had been considered earlier by Chaum in his patent [62], and was later reconsidered by Damgård in the concluding paragraph of [83]. Birgit has supported my work more than anyone else over the years; she has suggested designs of definitions, motivated me to lay as formal foundations as possible in this area, relentlessly cryptanalyzed my protocols and did thorough proof reading.

Together with Matthias Schunter I have looked for applications of the new cryptographic mechanisms. His background in electronic commerce (EU-CAFE) and my own background in security of health information systems (EU-SEISMED, EU-ISHTAR) made us write a paper on charging and reimbursing medical treatment in case of compulsory health insurances. Matthias was a creative partner in playing the “yes, it must work — no, it can’t” game, that has been reported to make engineering of new cryptographic schemes both productive and entertaining and sometimes causing headaches. (See Ron Rivest when he found the RSA algorithm in 1977 [114,p74].) It is even more exciting if you

change the roles from time to time. If I am asked why I am researching, I say “curiosity”, if I am asked why in the field of computer security, I say “social responsibility to a large extent”, but if I am asked, what makes me go on with research, I must admit it is the stimulation and inspiration I get from experiences like the above.

Michael Waidner has become a “background partner” to me. Although extremely busy, he has continued motivating me, has pointed me to important related work and always showed interest in this work.

I thank all my colleagues in the SEISMED and ISHTAR consortia (both sponsored by the Commission of the European Union) for patiently introducing a non-medical fellow like me into the field of security in medical informatics and the corresponding working group of the international medical informatics association (IMIA). I owe important insights to Ab Bakker, Barry Barber, Bernd Blobel, John Davey, Sokratis Katsikas, Eike-Henner Kluge, Erik Flikkenschild, Kees Louwerse and many others.

During two years of this work, I have been supported by AT&T Labs and I have much enjoyed the hospitality and encouragement of David Maher and his group. It was a pleasure to discuss parts of this work with Matt Franklin, Andrew Odlyzko, Mike Reiter and Serge Vaudenay.

The layout of this book is influenced by “Concrete Mathematics” [116]. In their book, Graham, Knuth and Patashnik not only provide a steady source of mathematical and humorous creativity, but also a paragon of excellent typesetting and layout.

Finally, I am deeply indebted to my wife Anne and my children Thilo, Tobias and Viola for their support and patience with me.