Privacy-Enhancing Identity Management

Sebastian Clauß, Andreas Pfitzmann, Dresden University of Technology, Marit Hansen, Independent Centre for Privacy Protection Schleswig-Holstein and Els Van Herreweghen, IBM Research Lab Zurich

Issue: Individual privacy is an increasingly important issue in the context of the information society. Privacy-enhancing identity management (IM) offers a means whereby individuals controls the nature and amount of personal information about them that is disclosed. In particular, to achieve privacy, individuals can use pseudonyms and determine the degree of linkability between different occurrences of their data. Through the secure and authenticated use of pseudonyms, accountability of an individual for his or her actions can be achieved without giving away personal data. Thus, privacy-enhancing identity management systems (IMSs) enable users to assert their right to "informational self-determination" better than before. Such systems are needed in all computer-mediated communications, even more so now with the advent of new technologies like mobile communication, UMTS, or ubiquitous computing.

Relevance: Surveys have shown that the lack of trust in privacy and security is an important hindrance for the success of e-commerce. Identity management implements the concept of notification and choice and empowers users. Transparency and putting users in control is expected to enhance users' trust. Today's existing identity management systems have no, or limited, privacy goals or functionality, or may even threaten users' privacy if they store and process personal information without appropriate protection measures. Thus there is a need for new systems to be designed and built into the infrastructure.

The views expressed here are the author's and do not necessarily reflect those of the European Commission.

Introduction

In today's world, we are used to living with traditional concepts of identity (e.g., "I am what I think", "I am what I eat", "I am what I want to be in groups or in society at large"). People act according to roles and are usually able to solve role conflicts in their behaviour. They have an intuitive understanding of whom to tell what about themselves, depending on the situation and depending on their role and the other party/parties in the communication process.

People have an intuitive understanding of whom to tell what about themselves, depending on the situation and their role

In the Information Society users are likely to define and handle their digital identities and roles in a similar way, and assert and enforce their right to privacy. In the digital world, this is a real challenge: Technology trends like the dissemination of (mobile) personal devices, ubiquitous access and computing, together with the e-transformation of business, government, and work processes, raise usability, security, and management issues which often are (but need not be) addressed by increasing the degree of linking, centralization, and logging of information. In the digital world, there is not only the possibility of creating new identities for oneself, but every user leaves data trails while using digital applications or services. Most people are not aware of how much the data they leave says about them and have no way of effectively controlling this data leakage. On the other hand, there is no guarantee that data in digital networks is authentic. In particular, fake identities can be created, and even identities of existing people can be "borrowed" – meanwhile identity theft is a fast growing problem (**http://www.identitytheft.org**). Thus today's digital world lacks both privacy and authenticity.

In the digital world, most people are not aware of how much the data they leave says about them and have no way of effectively controlling this data leakage

In the Information Society envisioned, privacy-enhancing identity management systems (IMSs) enable us to perform our roles, use our identities, and retain our privacy in society in the same way we have been allowed to up until now. Our personal environment and devices, rather than being just huge data repositories of our on-line actions, passwords, etc. also help us to keep track of, and protect the privacy of, our digital identities including their rights and obligations; and to choose when and to whom to give personal information. Communication networks allow us to hide our "coordinates" such as physical location, network or e-mail addresses and protect them from being misused, while still allowing network administrators to manage their networks securely. We can use electronic equivalents of every-day items such as library, gym or bus passes, phone books, or cash, without enabling extensive tracking and profiling of our behaviour across the different areas of our lives.

Privacy-enhancing IM combines privacy with authenticity. It requires technologies that allow users to control the release of personal information and to control the linkability of different occurrences of this information in different contexts (Pfitzmann/Köhntopp 2001) by acting under pseudonyms or anonymously. Authenticity can be achieved in combination with varying degrees of anonymity (Chaum 1984, Clarke 1999, Pfitzmann/Waidner/Pfitzmann 2000).

Privacy-enhancing IM combines privacy with authenticity. It requires technologies that allow users to control the release of personal information and to control the linkability of different occurrences of this information in different contexts

Box 1. The State of the Art

Nowadays, a whole range of systems exist which address different aspects of identity management. Only a few systems or tools primarily have privacy-oriented goals whereas most focus on usability and convenience, such as having a single sign-on. For example, several e-mail clients and web browsers offer the option of different user profiles. Specific e-mail addresses can be associated with different digital signature and encryption keys, e.g., with PGP (Pretty Good Privacy, **http://www.pgpi.org**). Some privacy tools provide user-configurable security or privacy functionality, e.g. to control the behaviour of cookies in order to limit user profiling, blocking identifying information from the normal "browser chatter", or using encryption programmes. The W3C standard P3P (Platform for Privacy Preferences, **http://www.w3.org/P3P/**) provides a format for specifying the privacy policies of web servers; P3P-enabled web browsers allow users to specify privacy preferences, which are matched against a web server's privacy policies. The W3C has been specifying the language APPEL (A P3P Preference Exchange Language, **http://www.w3.org/TR/P3P-preferences/**), which provides the use of different personae in the user's preferences file.

Personae management is also performed by a number of web services. Most of them (e.g., Microsoft .NET Passport (**http://www.passport.com**), Novell digitalme (**http://www.digitalme.com**), PrivaSeek Persona (**http://www.privaseek.com**), and iPrivacy (**http://www.iprivacy.com**) process users' personal data on the provider's server; a few store information locally on the user's computer (e.g., Passlogix's (**http://www.passlogix.com**) v-GO, Freedom Security and Privacy Suite (**http://www.freedom.net**)); the TrueSign technology from Privador Inc. (**http://www.privador.com**), which can be integrated with existing public-key infrastructures, allows users to manage different (pseudonymous) certificates.

The need for handling on-line identities also led to the creation of the Liberty Alliance Project (**http://www.projectliberty.org**), a business alliance formed to deliver a solution for managing identities on the Internet, to enable single sign-on with decentralized authentication and open authorization from multiple providers, and to provide an open standard for network identity spanning all devices. No public results are available yet.

Some academic projects deal with identity management, too. A "personal reachability and security management" prototype enables the use of different pseudonyms in personal communication (Damker/Pordesch/Reichenbach 1999). The pseudonyms can contain public keys for encrypting or signing communications; and they can be issued by a certification authority (CA), or created by users themselves. Another project, ATUS (A Toolkit for Usable Security) from Freiburg University, Germany, is designing and implementing an "identity manager" module (Jendricke/Gerd tom Markotten 2000). It acts as a proxy firewall on the user's system, and supports the user in managing different profiles, implemented as views of a set of personal data consisting of typical attributes such as name, postal address, and e-mail address. The profiles can be linked to specific URIs, allowing an automated choice of profile when contacting specific web servers. The ATUS identity manager by default connects anonymously to any Internet service (currently using the AN.ON/JAP (Berthold/Federrath/Köhntopp 2000) technology from Dresden University). It serves as form filler and warns the user when he or she discloses predefined additional information, e.g., manually provided in a form. It mainly focuses on controlling the amount of personal data in a given transaction, and does not support secure transactions under the different profiles.

Approaches to Identity Management

Approaches to IM mainly differ in terms of the location where user profiles are stored and processed (user's side only / user's and server side / server side only) and in the provision of authentication mechanisms and additional security and privacy functionality. Having in mind the design of a comprehensive privacy-enhancing IMS, various shortcomings of the existing approaches can be enumerated:

- **Lacking support for users' sovereignty:**

In most cases users cannot choose where and how their personal data are managed: They have to trust central IM providers who have full access to their data.

- **Limited privacy functions:**

Few systems help the users' awareness or assertion of their right to privacy.

- **No pseudonymous authentication:**

Currently, the state of the art in pseudonymous and anonymous credential systems (cf. Camenisch/Lysyanskaya 2001) allows for provably secure implementations of authenticated anonymous transactions and user-controlled release of certified attributes. In particular, they allow each user to use a credential with multiple pseudonyms without these pseudonyms becoming linkable. Through optional anonymity revocation (or anonymity reversal) by designated trusted third parties, these systems support accountability and thus law enforcement measures despite the use of pseudonyms. Such systems are currently not exploited by existing IMSs.

- **Restricted to specific applications:**

The existing systems cannot be used universally, but they are tailored specifically for use with a certain application or set of applications. Open standards for IMS interfaces which can be implemented in all kinds of computer-mediated communications do not yet exist.

The lack of privacy in existing systems highlights the need for new privacy-enhancing technological solutions, taking into account existing legal systems and possible business models

Legal or organizational measures alone are not sufficient to help users with their IM. The lack of privacy in existing systems highlights the need for new privacy-enhancing technological solutions, taking into account existing legal systems and possible business models. There is also a need for actions to educate and train users in privacy and IMSs.

Moreover, privacy-enhancing IM requires new technologies and third party services to be provided as part of an IM infrastructure (see below). Therefore, a comprehensive approach to IM is needed, which is not offered by any of the existing systems discussed above.

Design of an IMS: Requirements and Functionality

A privacy-enhancing IMS makes the user aware of and gives him/her control over the flow of personal data. To show the user that flow of data, the IMS must give him or her meaningful history and context representations. History information includes the extent, nature, and linkability of data released in the past; context information may include additional information, e.g., specific tags to express when actions have to be linked or what properties a new pseudonym should have, and can be provided by communication partners, third parties such as a privacy information service or even the Internet community.

In order to give the user control over the flow of personal data, the IMS supports each user in deciding and enforcing which identifiable or pseudonymous personal data he or she releases. It enables the user to minimize the dissemination of personal data and to determine the degree of linkability of his data by choosing which pseudonyms are used with which properties, and whether to re-use pseudonyms or to generate new ones.

It gives the user the mechanisms and interfaces to implement his privacy rights, e.g., to get information from a server about what personal data that server holds about him or her, to access these data, to correct or remove these data, or to grant or revoke consent.

Usability and a good user interface are essential and may include support by on-line privacy information services providing information about security and privacy risks with respect to the IMSs deployed.

The user should be able to access his IM tool from a variety of devices (e.g., a mobile phone or PDA) and locations. Also, less capable devices should provide a usable interface and at least minimal functionality.

Ideally, the user’s IMS is located in the user’s trusted environment. For various reasons (e.g., reachability of the system when using different devices, convenient replication, or back-up services), users may want to outsource all or part of their IMS to a provider. The user should be able to select the provider.

Privacy and identity management should not hinder the enforcement of security measures or the effectiveness of intrusion detection systems. In many cases there need not be a contradiction between law enforcement requirements and full privacy

Privacy and identity management should not hinder the enforcement of security measures orthe effectiveness of intrusion detection systems. In many cases there need not be a contradiction between law enforcement requirements and full privacy: appropriate design of applications can prevent misuse so that the user’s anonymity need not be reversible (Pfitzmann/Waidner/Pfitzmann 2000). When designing IMSs and deploying anonymous and unlinkable transactions, systems and tools enforcing security may have to be reconfigured or adapted in order to deal with these varying degrees of anonymity or pseudonym properties such as restricting users to a fixed number of pseudonyms per subject, transferability to other subjects, possibility and frequency of pseudonym changeover, limitation of the number of uses, validity (e.g., time limit, restriction to a specific application), possibility of revocation or blocking, or participation of users or other parties in forming the pseudonyms (Pfitzmann/Köhntopp 2001).

When users act under pseudonyms or anonymously, law enforcement and security considerations may require that the anonymity supported by the IMS be reversible, or that a pseudonym can be traced back to a specific user

When users act under pseudonyms or anonymously, law enforcement and security considerations may require that the anonymity supported by the IMS be reversible, or that a pseudonym can be traced back to a specific user. The task of reversing anonymity is typically assigned to dedicated trusted third parties such as identity brokers or authorities certifying anonymous credentials. It is of utmost importance that users can trust and, if possible, choose, the third parties that are able to reveal their identities or link their actions. In addition, measures must be taken to ensure public control and accountability of the actions of these third parties.

In the IM infrastructure, users will be supported by, and share information with, not only IMS providers and certifying authorities, but many more third-party services. For all these services, the system should support distribution of trust, and separation of knowledge and power (e.g., a user may trust a third party or provider to know selected personal information, but not to act on behalf of the user). This means the user should be able to decide which third party or provider to trust and to what extent.

Basic Techniques for Achieving Unlinkability and Anonymity

If users wish, the IMS supports unlinkability of different user actions so that communication partners involved in different actions by the same user cannot combine the personal data disseminated during these actions for the purposes of user profiling. Maintaining unlinkability of authenticated data is possible only if users are allowed to act under different (unlinkable) pseudonyms which may have specific properties or attributes (Pfitzmann/Köhntopp 2001).

If users wish, the IMS supports unlinkability of different actions of a user so that communication partners involved in *different actions by the same user cannot combine the personal data disseminated during these actions for the purposes of user profiling*

Most actions require secure communication and authentication of some of the communicating parties' properties or attributes. If users act under pseudonyms, service providers can enforce security and authenticity only if they accept pseudonymous or anonymous credentials. Anonymous credential systems such as (Camenisch/ Lysyanskaya 2001) allow accountability and law enforcement despite the use of pseudonyms. In many cases, misuse may be prevented (rather than traced) by building appropriate security into the application.

A prerequisite for achieving unlinkability of actions at the application level is support of anonymity by the network, e.g. realized with Mix-based anonymity services (Chaum 1981, Berthold/Federrath/Köhntopp 2000).

Architecture Overview

A comprehensive privacy-enhancing IMS would include the following components (Clauß/Köhntopp 2001):

- an Identity Manager (IDM) on the user's side;
- IDM support in applications (e.g. at content providers, web shops, etc.);
- various third-party services.

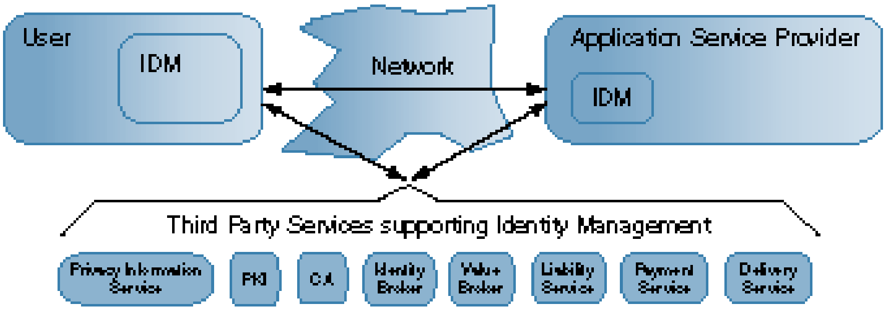
A comprehensive privacy-enhancing IMS needs to include an identity manager, IDM support in applications, and various third-party services

Some third parties provide the certification services needed for secure authentication of users. They may support various degrees of data minimization, e.g., by allowing pseudonymous (but accountable) authentication. Trustees may offer different mediator services: Identity brokers, for instance, reveal the identity of a pseudonym holder under specific circumstances. Liability services clear a debt or settle a claim on behalf of the pseudonym holder. A value broker may perform the exchange of goods without revealing additional personal data. Unlinkability of the 'who (buys)' and the 'what (is bought)' in a partially on-line purchase may be achieved by applying 'separation of knowledge' between payment and delivery services (i.e. neither the party handling payment nor the party handling delivery has the full details of the user). Also, the communication infrastructure needs to support basic security and privacy (e.g., network layer authentication, confidentiality, and possibly anonymity) as well as robustness. The principles of distribution of trust and separation of knowledge and power should be applied in the design of these third party services, in order to limit the threat of information sharing between third parties. Also, it should be possible for users to enforce their trust preferences.

The user's IDM acts as a central gateway for all communication between different applications, like browsing the web, buying in Internet shops, or carrying out administrative tasks with governmental authorities

The user's IDM acts as a central gateway for all communication between different applications, like browsing the web, buying in Internet shops, or carrying out administrative tasks with governmental authorities. By acting as a central gateway, it allows the user to be aware of the flow of personal data, and to control the release of data, in accordance with the specified requirements.

Figure 1. Basic Components of an IMS


User
IDM
Network
Application Service Provider
IDM
Third Party Services supporting Identity Management
Privacy Information Service
PKI
CA
Identity Broker
Value Broker
Liability Service
Payment Service
Delivery Service

As discussed above, distributed implementation of the user's IDM is possible. For example, the graphical user interface (GUI) can be implemented on (less capable) mobile devices while the other modules are located at a more powerful fixed station, using secure communication to the external GUI. Also, part of the user's IDM may be located at an IDM proxy provider.

The IDM tools at the application services are needed primarily to handle anonymous or pseudonymous requests, and especially pseudonymous authentication of users. It also provides the user with context information about the transaction, e.g. information about pseudonym properties needed.

To provide maximum interoperability, common standards for protocols and interfaces need to be defined, so as to permit a combination with existing systems to enhance their privacy functionality.

Outlook

Privacy-enhancing IM is necessary to preserve and update the concept of privacy for the Information Society. Our vision of privacy-enhancing IM can only be fully achieved if we design applications, middleware, and communication infrastructures so that they support the IM architecture and technologies proposed. Of course, its implementation will happen using an evolutionary approach, as technologies supporting it will be introduced gradually and will coexist with today's systems.

Privacy-enhancing IM is necessary to preserve and update the concept of privacy for the Information Society

Educating Users

With Identity Management Systems (IMSs), individuals can let computers explicitly handle their identities (e.g., roles) which humans have handled mostly implicitly for centuries. This may be a chance for new awareness – and even the emergence of new properties of the self that are invisible without an appropriate medium (Turkle 1995). This means that both inter-personal and intra-personal aspects of identity management (IM) have to be addressed by IMSs. But the impossibility of purely implicit handling of identities as well as the option of directly asserting one's right to privacy may also be difficult to grasp for many people. To avoid a gap between privacy-haves and privacy-have-nots, the implementation of IMSs has to be accompanied by a process of educating users. Users should be trained both in digital privacy-related concepts and in using real IMSs. It is necessary to learn about the limitations of digital identity management (IM), e.g., that IMSs cannot enforce privacy, or that they cannot give users complete information as they are unaware of the full set of processing operations carried out on any disclosed data (communication infrastructure adding routing or addressing information; communication partners mining, selling, merging data …). When considering the complex digital world and privacy rights, it is a real challenge to design appropriate GUIs for different devices, given also that they may need to be specifically tailored to a particular cultural background or legal framework.

The trustworthiness of the system is very important, but even experienced users are not normally able to evaluate the security of their identity manager (IDM) or other parts of the identity management system (IMS). They have to be given support such as professional evaluation of the system according to security and privacy criteria, audits by privacy advisers, or help from privacy information services.

With IMSs, individuals can let computers explicitly handle their identities thus taking over which humans have handled mostly implicitly for centuries, which means that both inter-personal and intra-personal aspects of IM have to be addressed by IMSs

IMS as Target

The concentration of sensitive personal data in an IMS makes it an attractive target for attackers. Today no really secure devices exist. Demand for such devices should support and enable industry efforts to build them. But even with secure devices, IMSs may become a risk to privacy themselves: They mirror a great part not only of the user's life, but also parts of the communication partners' lives. Therefore other parties such as marketing companies, employers, insurers, landlords, or even criminals may get the user to disclose his or other people's personal data. It is not always the case that data should be available in authenticated form, for instance it is a requirement of secret ballots that the voter is unable to reveal his vote in order to prevent blackmail. This should be taken into account in IMS-compatible applications.

The concentration of sensitive personal data in an IMS makes it an attractive target for attackers. Clearly technologies need to be developed to ensure it is secure

Updating Legal Regulations

IMSs make it possible to bring privacy technology up-to-date in a way that complies with privacy legislation. Existing regulations which authorize and regulate the processing of personal data may have been written without knowledge of these new technologies and how they can enhance privacy without compromising security. In fact, these regulations should be re-evaluated with respect to allowing the use of anonymous or pseudonymous transactions.

IMSs make it possible to bring privacy technology up-to-date in a way that complies with privacy legislation

Not all kinds of invasions of privacy depend on identifiable personal data. Even when pseudonyms are used, discrimination against, or nuisance to, an individual are possible, and cannot entirely be prevented by IMSs. These kinds of invasion of privacy are not fully covered by today's right to "informational self-determination". When updating laws like the EU Directive on Data Protection, one can consider whether a broader view on privacy should be implemented.

Drivers for Privacy-Enhancing IMSs

We see three main drivers for developing privacy-enhancing IMSs, each contributing their specific interests:

- privacy law (EU Directive 1995), enforced by the government, also taking into account the requirements of law enforcement agencies;

- users who demand such systems to achieve better privacy;
- economic considerations, calling for the creation of new IMS business models or adapting them to enable lasting customer relationships without expensive processing of personal data with all its privacy obligations.

The issue of whether these driving forces are sufficient to develop good privacy-enhancing IMSs, and the need for users to be appropriately informed and educated, are no doubt of interest to policy-makers. Moreover, any regulations in this field need to be specific and up-to-date with privacy-enhancing technologies, such that they provide the correct incentives for enterprises to create and put in place the IMS-supportive business models.

There is a need for an interdisciplinary discussion on the future of identity and privacy (Bogdanowicz/Beslay 2001), which should lead the way to comprehensive privacy-enhancing IMSs. Technological know-how is necessary for this discussion: The digital world works differently from the physical world; it may threaten privacy, but it also provides the means to cope with such threats or even shows opportunities for better privacy protection than before.

Keywords

privacy, identity management, security, trust

References

- Berthold, O., Federrath, H., and Köhntopp, M. *Anonymity and Unobservability in the Internet*", Workshop on Freedom and Privacy by Design. In Proceedings of the Tenth Conference on Computers, Freedom & Privacy, CFP 2000: Challenging the Assumptions, Toronto/Canada, April 4-7, 2000. ACM, New York 2000. 57-65.
- Bogdanowicz, M., and Beslay, L., *Cyber-Security and the Future of Identity*. In The IPTS Report No. 57, JRC Seville, September 2001. **http://www.jrc.es/pages/iptsreport/vol57/english/ICT4E576.htm**
- Camenisch, J. and Lysyanskaya, A. *Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation*. In B. Pfitzmann (Ed.), Advances in Cryptology – EUROCRYPT 2001. LNCS 2045. Springer Verlag, 2001. 93-118.
- Clauß, S. and Köhntopp, M. *Identity Management and Its Support of Multilateral Security.* In Computer Networks 37 (2001). Special Issue on Electronic Business Systems. Elsevier, North-Holland 2001. 205-219. **http://www.elsevier.com/gej-ng/10/15/22/67/33/34/article.pdf**
- Chaum, D. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* Communications of the ACM, 24(2) February 1981.
- Chaum, D. *Security without identification: Transaction systems to make big brother obsolete*. Communications of the ACM, 28(10) October 1985, 1030-1044. **http://www.chaum.com/articles/Security_Wthout_Identification.htm**
- Clarke, R. *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice*. In S. Fischer-Hübner, G. Quirchmayr, L. Yngström (Eds.), User Identification & Privacy Protection: Applications in Public Administration & Electronic Commerce. Kista, Schweden, Juni 1999, IFIP WG 8.5 and WS 9.6. **http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html**
- Damker, H., Ulrich Pordesch, and Martin Reichenbach. Personal Reachability and Security Management – Negotiation of Multilateral Security. In G. Müller, K. Rannenberg (Eds.), Multilateral Security in Communications. Vol. 3, Addison Wesley, 1999. 95-111.
- Enzmann, M. and Schulze, G. DASIT: Privacy Protection in the Internet by User Control. Electronic Payment Systems Observatory (ePSO) Newsletter Vol. 9, September 2001. **http://epso.jrc.es/newsletter/vol09/4.html**
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the free Movement of such Data, Official Journal L 281, 23/11/1995, pp. 0031-0050, **http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html**
- Jendricke, U. and Gerd tom Markotten, D., *Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet.* In Proc. 16th Annual Computer Security Applications Conference (ACSAC 2000), New Orleans, USA, December 11-15, 2000.
- Pfitzmann, A. and Köhntopp, M., *Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology*; Draft v0.12, 2001-06-17, **http://www.koehntopp.de/marit/pub/anon/** V0.8 in H. Federrath (Ed.), Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability. LNCS 2009. Springer Verlag, 2001. 1-9.
- Pfitzmann, B., Waidner, M., and Pfitzmann, A. *Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity*. IBM Research Report RZ 3232 (#93278) 05/22/00, IBM Research Division, Zürich, May 2000. **http://www.semper.org/sirene/publ/PWP_00.ps.gz**
- Turkle, S. *Life on the Screen – Identity in the Age of the Internet.* Simon & Schuster, New York 1995.

Contacts

Sebastian Clauß, Dresden University of Technology,

Tel.: +49 35 146 33 82 72, fax: +49 35 146 33 82 55, e-mail: **sc2@inf.tu-dresden.de**

Andreas Pfitzmann, Dresden University of Technology,

Tel.: +49 35 14 63 38 277, fax: +49 35 14 63 38 255, e-mail: **pfitza@inf.tu-dresden.de**

Marit Hansen, Independent Centre for Privacy Protection Schleswig-Holstein, Kiel,

Tel.: +49 43 198 81 214, fax: +49 43 198 81 223, e-mail: **marit.hansen@datenschutzzentrum.de**

Els Van Herreweghen, IBM Research Lab Zurich,

Tel.: +41 17 24 86 28, fax: +41 17 24 89 53, e-mail: **evh@zurich.ibm.com**

Laurent Beslay, IPTS

Tel.: +34 95 448 82 06, fax: +34 95 448 82 08, e-mail: **laurent.beslay@jrc.es**

About the authors

***Sebastian Clauß** has a diploma degree in informatics from Dresden University of Technology, Germany, where he studied from 1994 to 2000 and where he is currently engaged in research into data security and privacy. His research interests and published work focus in particular on technologies for anonymity and identity management.*
***Andreas Pfitzmann** is a professor of computer science at Dresden University of Technology. His research interests include privacy and multilateral security, mainly in communication networks, mobile computing, and distributed applications. He has authored or coauthored about 70 papers in these fields. He received diploma and doctoral degrees in computer science from the University of Karlsruhe. He is a member of ACM, IEEE, and GI, where he serves as chairman of the Special Interest Group on Dependable IT-Systems.*
***Marit Hansen** is a computer scientist and is head of the "Privacy Enhancing Technologies (PET)" Section at the Independent Centre for Privacy Protection Schleswig-Holstein (the state privacy commission), Germany. Since her diploma in 1995 she has been working on security and privacy aspects especially concerning the Internet, anonymity, pseudonymity, identity management, biometrics, multilateral security, and e-privacy from both the technical and the legal perspectives. In several projects she and her team actively participate in technology design in order to support PET and give feedback on legislation.*
***Els Van Herreweghen** has Masters degrees in Chemical Engineering (Ingenieur Scheikunde en Landbouwindustrieen) and Computer Science (Licentiaat Informatika) from the Katholieke Universiteit Leuven, Belgium, in 1988 and 1992, respectively. Since 1992, she has been a Research Staff Member in the Network Security group at the IBM Zurich Research Laboratory, Switzerland. Her research focuses on security and privacy issues related to electronic communication and electronic transactions.*

Contents Report 67

About **The IPTS Report**

Subscriptions

E-Mail: **ipts_secr@jrc.es**