ELSEVIER

Computer Networks 37 (2001) 205–219

COMPUTER NETWORKS

www.elsevier.com/locate/comnet

Identity management and its support of multilateral security

Sebastian Clauß [a,*], Marit Köhntopp [b]

[a] *Technische Universität Dresden, Fakultät Informatik, D-01062, Dresden, Germany*

[b] *Independent Centre for Privacy Protection Schleswig–Holstein, Unabhängiges Landeszentrum für Datenschutz Schleswig–Holstein, Holstenstraße 98, D-24103 Kiel, Germany*

Abstract

We show our approach in developing an identity management system with respect to multilateral security. After examining digital pseudonyms and credentials as basic concepts of such a system, we give an introduction to technologies for multilateral security and describe an architecture which enables multilaterally secure communication. By means of different scenarios we show requirements of an identity management system, and outline an approach in developing an identity manager and its infrastructure. Finally, we discuss problems and risks of identity management systems which must be considered when using such a system. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Identity management; Multilateral security; Privacy; Credential; Pseudonym

1. Introduction

Recent surveys (e.g., [10,13]), have demonstrated that the lack of trust in privacy and security is a main hinderance for the success of e-commerce. Therefore, methods to establish privacy and security have to be directly implemented in IT systems. That way, users may justifiably develop trust when using an IT system, e.g., for e-commerce. Achieving trust is an aim of multilateral security, which empowers the user to assert her rights, e.g., to informational self-determination. Identity management systems enable the user to control the nature and amount of personal information released. This is an important feature for users' informational self-determination. Thus, identity management systems can act as means for realizing or at least supporting central requirements of privacy laws like the European Union Directive on Data Protection [8].

Currently, the e-commerce world has two specific problems. It lacks anonymity, i.e., every user leaves traces while using the Internet, and it lacks authenticity, i.e., communication data can easily be faked. Solutions to these problems, including the infrastructure required, are being developed. In most applications, neither total anonymity nor total identification with a huge amount of personal data are reasonable. Instead, a differentiated, integrating approach, where only the necessary personal data – not inevitably *identifying* – is disclosed, would be suitable. This can be realized with a comprehensive identity management system based on a communication network providing anonymity. The core components of such a system include digital pseudonyms built with various kinds of digital signatures. Thus, the possibility exists for modelling properties, specific to different application contexts.

[*] Corresponding author.

E-mail addresses: sc2@inf.tu-dresden.de (S. Clauß), marit@koehntopp.de (M. Köhntopp).

PII: S1389-1286(01)00217-1

In our project, we are developing an identity management system. It will be implemented as a module in the SSONET project (security and privacy in open networks, "Sicherheit und Schutz in offenen Datennetzen"), which provides a tool for multilateral security. SSONET enables the user to configure her security preferences. In order to establish a connection, the preferences of all communications partners are negotiated. This is particularly relevant to e-commerce scenarios.

2. Overview

First, we introduce the concept of identities and identity management systems in Section 3. The focus lies on essential properties and mechanisms of pseudonyms as basic building blocks of identity management. In addition, we describe related work and motivate developing a comprehensive and scalable identity management system. Section 4 outlines the concept of multilateral security and its technologies. As an example, SSONET, an architecture for multilateral security, is explained. We show why it suits as underlying architecture of a comprehensive identity management system. Section 5 centres around the design of an identity management system: the requirements, infrastructure, and the identity manager itself are described, and the planned integration into SSONET is outlined. Problems and risks with respect to identity management are addressed in Section 6. Finally, Section 7 gives a conclusion and an outlook for the topic.

3. Identity management

3.1. What is identity management?

The identity of a person comprises a huge amount of personal data with respect to individuals. All subsets of the identity represent the person (or components of the person). Some of these "partial identities" uniquely identify the person, others do not. Depending on the situation and the context, the person may be represented by different partial identities. An identity management system provides the tools for managing these partial identities in the digital world. For example, a person may use one or more partial identities for work, others for leisure activities, e.g., with the family, doing sports, or dealing with companies like a bank, an Internet service provider, or a supermarket. Some partial identities containing the information which other communication partners typically know about a person, are shown in Fig. 1.

Thus, identity management in the digital world relates to the behaviour of persons in everyday activities. Each person decides what to tell the other about herself, after having considered the situational context and the role each has while currently acting in the respective relationship to the communication partners. Sometimes different names – nicknames, pseudonyms – are bound to the chosen identity.

Occasionally it is suitable to remain entirely anonymous, e.g., while buying something at a kiosk. In very rare cases it is necessary to reveal identifying personal data, e.g., when being asked by a governmental representative for showing the identity card. Often, anonymity is not acceptable, but nevertheless only some personal data or credential is needed. The differentiated choices depending on the user's wishes and the application's prerequisite are supported by identity management systems.

Nevertheless, both techniques for anonymity and authenticity are required to fulfil the requirements of an identity manager: In the digital world where all disclosed personal data can be stored and linked, it is necessary to guarantee anonymity and unobservability as a privacy protection baseline, especially on the communication network against providers or observers [1]. On the other hand, digital signatures, embedded into an appropriate infrastructure, providing authenticity are needed to realize a trustworthy communication and to prevent from identity theft.

3.2. Basic mechanisms of an identity management system: pseudonyms

Pseudonyms act as identifiers of subjects or sets of subjects (in the latter case called *group pseudonyms*). Whereas anonymity on the one side and

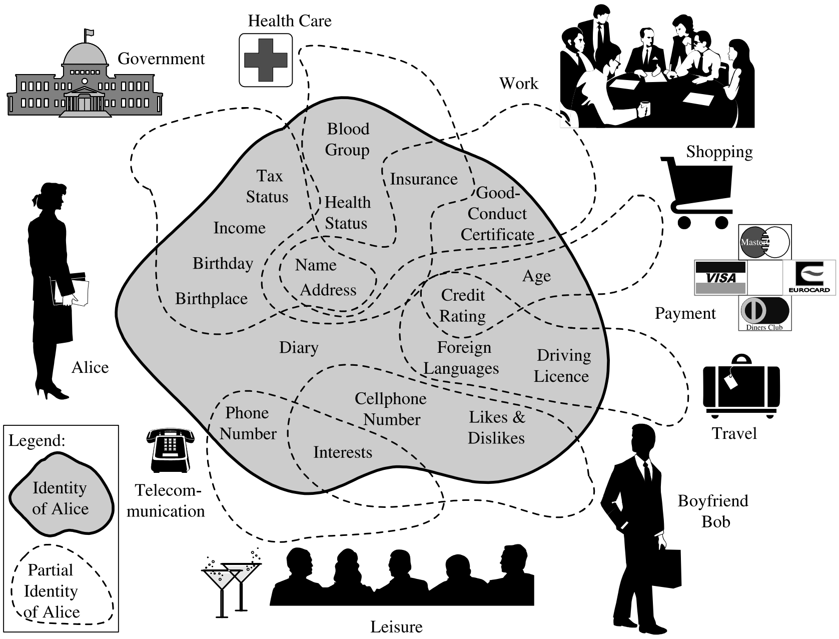

Fig. 1. Partial identities of Alice.

unambiguous identifiability on the other are extremes with respect to linkability to subjects, pseudonymity comprises the entire field between and including these extremes [15]. Therefore, pseudonyms serve as the core mechanism of an identity manager.

Using the same pseudonym more than once, the holder may take advantage of an established reputation. Some kinds of pseudonyms enable dealing with claims in case of abuse of unlinkability to holders: Third parties may have the possibility to reveal the identity of the holder in order to provide the means for investigation or prosecution, or they may act as liability brokers of the holder to clear a debt or settle a claim.

A pseudonym together with the data linked to it forms a partial identity. Important properties of pseudonyms include:

- *Proof of holdership*: *Digital pseudonyms* could be realized as a public key to test digital signatures where the holder of the pseudonym can prove holdership by forming a digital signature which is created using the corresponding private key. E.g., the public keys of PGP, bound to e-mail addresses, are digital pseudonyms.
- *Initial knowledge of the linking between the pseudonym and its holder*: Pseudonyms can be created by the user, or they can be generated and assigned by an application provider or by a third party. In the context of identity management, the linkage between a pseudonym and its holder would not be publicly known.
- *Linkability due to the use of a pseudonym in different contexts* [18]: If the same pseudonym is used in many cases, the corresponding data about the holder, which is disclosed through each use, can be linked. In general, anonymity is the stronger, the less often and the less context-spanning the same pseudonyms are used. We distinguish between *transaction pseudonyms*, which are only used for one transaction, *situation pseudonyms* which are used in a specific context (e.g., according to the role of the holder or the relationship to the communication partner), and context-spanning *person pseudonyms* as substitutes for the holder's name respectively civil identity.
- *Convertability, i.e., transferability of attributes of one pseudonym to another*: The user can obtain

a convertible credential from one organization using one of her pseudonyms, but can demonstrate possession of the credential to another organization without revealing her first pseudonym. For this purpose, a credential can be converted into a credential for the currently used pseudonym. Therefore the use of different credentials is unlinkable. Chaum published the first credential system by [5]. Other systems have been proposed (e.g., Brands [3] and Camenisch/Lysyanskaya [4]).

- *Authorizations*: Authorizations can be realized by credentials or attribute certificates bound to digital pseudonyms, but – in case of digital vouchers transferable to other people – by blind digital signatures or certificates as well.

3.3. Related work

Basic ideas of identity management systems focussed on anonymity and authenticity have already been outlined by David Chaum [6]. Ten years later, the concept of an identity protector was published in the context of privacy enhancing technologies [19]. Now, some application-specific identity protectors have been built, but in most cases not directly controlled by the user, or at least not in her own sphere of control.

The "personal reachability and security management" for callers and callees saw development and prototypical implementation in the context of the Kolleg "security in communication technology" as an example of multilateral security [7]. Focussing on reachability, it contains a concept for user identification and the way users handle identity functions. Users can communicate anonymously, or through a pseudonym – having the freedom of choice and using a negotiation protocol. Furthermore, users may present themselves in different roles by means of different identity cards that are issued as pseudonyms. For the purposes of identification and recognition, each user participating in the communication deploys digital identity cards, which are stored as data structures in her personal digital assistant (PDA). They may contain several data items including a cryptographic key pair used for digital signatures and the encryption of communication contents. Certificates issued from some certification authorities (CAs) confirm the validity of the identity card and its data.

On the Internet, several services enable the user to choose between different appearances (see [12]). Many e-mail clients and Web browsers offer the use of different user profiles. Different digital signatures may be bound to different e-mail addresses, (e.g., with Pretty Good Privacy (PGP), http://www.pgpi.org). Similarly, anonymizing e-mail services like Freedom (http://www.freedom.net) or Privada (http://www.privada.com) comprise several user pseudonyms.

Other Web services provide the management of different personae. Whereas most of them (e.g., Novell's digitalme, http://www.digitalme.com, or PrivaSeek's Persona, http://www.privaseek.com) process the user's personal data on the provider's server, a few store the (encrypted) information locally on the user's computer (e.g., Passlogix's v-GO, http://www.passlogix.com). The possibility for managing different (pseudonymous) certificates is given (e.g., by TrueSign from Privador, http://www.privador.com).

In the project ATUS – a toolkit for usable security – from Freiburg University, Germany, one of the modules is called "identity manager" [11]. Installed like a proxy firewall, it supports the user in managing different profiles, realized as views on a set of personal data consisting of typical attributes like name, postal address, and e-mail address. The current prototype supports four profiles, which can be bound to specific URLs in the World Wide Web. Like SSONET, the ATUS identity manager has an interface to an underlying Web anonymity service from Dresden University [1] and provides anonymity as a default. The current ATUS identity manager serves as a form filler and warns the user when disclosing predefined additional information, e.g., manually provided in a form. In later versions, the developers want to integrate modules for digital signatures and for some identity negotiation.

This project ATUS focusses on usability aspects. It does not provide the use of specific pseudonyms or credentials; thus the user can only control the *amount* of given personal data.

Because its current concept is oriented towards a mainly user-side technology, many important functions of a comprehensive identity management system like negotiation, privacy requests, or fine-granular choice of pseudonyms according to the specific situation (see Section 5) cannot be implemented.

Deficiencies and disadvantages of today's identity management approaches include:

- no sufficient privacy and security protection baseline; not all services provide privacy and security mechanisms;
- no sufficient user control, but requirement to trust the (single) provider, especially when the personal data is stored there; in the cases where identity management components are installed at the user side, lack of flexibility and comprehensiveness;
- no or only little support in using the appropriate pseudonym;
- no universal or standardized approach, only specific to some applications.

4. Technologies for multilateral security

4.1. Basic concept of multilateral security

Consider an action that involves communication between different parties. *Multilateral security* means providing security for all parties concerned in that communication. *Multilateral security* requires that each party only minimally trusts the others [14]. The basic concept includes:

1. Each party has its particular protection goals.
2. Each party can formulate its protection goals.
3. Security conflicts are recognized and compromises negotiated.
4. Each party can enforce its protection goals within the agreed compromise.

Multilateral security does not necessarily enable every participant to enforce all of her individual security goals, but at least it provides transparency of the security of an action for all parties involved.

4.2. Classification of technologies for multilateral security

Pfitzmann [14] introduces a classification of technologies for multilateral security according to the number of cooperating parties at runtime and distinguishes unilateral, bilateral, trilateral, and multilateral technologies. This classification can easily be used for categorizing mechanisms: (e.g., encryption of local storage media is *unilateral*, cryptography to achieve confidentiality of communication content is *bilateral*, a public key infrastructure (PKI) is *trilateral*, and mechanisms which provide for anonymity with regard to communication are *multilateral*).

Identity management is a more complex technology built together from various mechanisms which are not restricted to runtime. Thus, simply counting the involved parties at runtime does not cover all essential building blocks and does not give an indication about the necessary scale of coordination and negotiation needed for identity management.

In the sequel, we use a slightly modified model for classifying technologies for multilateral security by structuring them according to some typical properties of the parties. The definitions are quite similar to the x-laterality definitions in [14], but it seems to be easier to use the new classification of properties in a practical context.

- Each party for itself can decide on *user-side technologies*. Therefore, neither coordination nor negotiation is needed concerning their usage.
- *Communication-partners technologies* function only if the communication partners cooperate. This means that some coordination and negotiation is needed concerning their usage.
- *Third-parties technologies* need a third party involvement to fulfil a specific task for other participating parties. This means that more coordination and negotiation is needed concerning their usage compared to user-side – and in most cases as well communication-partners technologies.
- *Distributed technologies* require many independent parties to cooperate. This means that coordination and negotiations must function on a large scale.

4.3. SSONET – an architecture for multilateral security

In the SSONET project [16], an architecture which enables multilateral security in communications between two partners was developed. It is implemented as a prototype including a sample application, which uses this architecture. Here we will give a short description of this architecture, because it will be the basic architecture for our approach to implementing an identity management system.

According to the given description of the concept of multilateral security, the architecture is essentially composed of the components shown in Fig. 2.

Using the *application programming interface* (API), applications built on top of the SSONET architecture are enabled to include security mechanisms.

The *security management interface* (SMI) offers users the possibility to configure their security goals and preferred security mechanisms. This can be done for each part of an application where a communication with the partner is required.

The *configuration* component saves the user's settings.

During the phase for establishing a connection to the communication partner, the *negotiation* component negotiates between the users' security preferences in order to reach a fair compromise for a security base, which is acceptable to both communication partners. If the security goals or the mechanism preferences are contradictory, the result of the negotiation may also be a deliberate renouncement of the communication itself.

If the partners agree on security goals, but do not have common security mechanisms to achieve these goals, they may use a security gateway. For some security goals a *security gateway* is able to transform between different security mechanisms used by the communication partners.

The SSONET architecture includes *key exchange protocols* for symmetric and asymmetric cryptographic mechanisms. These protocols use X.509-certificates. After a successful negotiation of the cryptographic mechanisms, the appropriate keys are exchanged and verified.

The system is developed in Java, so it is object-oriented and platform independent. A drawback of Java is the lack of performance. Due to the API the SSONET architecture can be used for any desired application. Because of encapsulation of the cryptographic mechanisms the architecture is independent of specific implementations. The architecture uses mechanism implementations of existing crypto libraries, e.g., the freely available library Cryptix 3.2.0 (http://www.cryptix.org).

The SSONET architecture implements configuration interfaces and negotiation protocols for:

- security goals (confidentiality, anonymity, integrity, accountability, furthermore hiding, unobservability, availability, and reachability [20]),
- security mechanisms (one or more for each security goal),
- mechanism details according to the mechanisms (e.g., key length, number of iterations, operation modes).

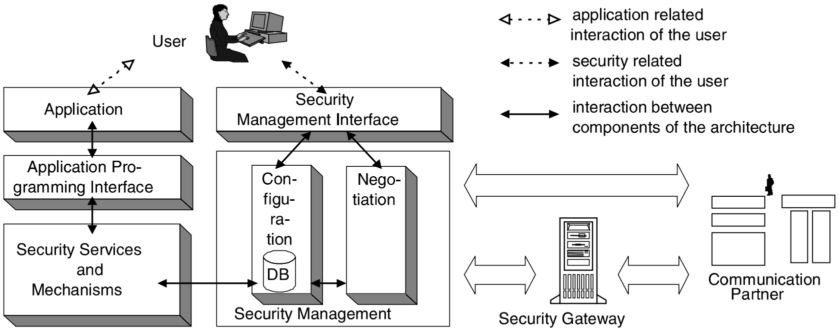
User
Application
Security Management Interface
Application Programming Interface
Security Services and Mechanisms
Configuration
DB
Negotiation
Security Management
Security Gateway
Communication Partner
application related interaction of the user
security related interaction of the user
interaction between components of the architecture

Fig. 2. Structure of the SSONET security architecture.

In particular, SSONET integrates the anonymity service of the project Anonymity Online (AN.ON), which can also be used separately as a stand-alone application for anonymous Web surfing [1] (http://www.anon-online.de). AN.ON will be extended to handle other Internet services as well.

5. Designing an identity management system

5.1. Requirements concerning identity management

In this section we show some scenarios where identity management can be used. By means of these scenarios we will deduce identity management requirements. A scenario of e-commerce in the WWW and another of sending and receiving e-mail will be explained in detail. We will also briefly describe requirements of an identity management used in auctions, electronic elections, and e-government applications.

5.1.1. E-commerce in the WWW

We discuss a scenario of an online bookstore where a customer wants to buy a book. For each situation we will explain how the communication must be secured and which types of pseudonyms are suitable. Fig. 3 gives an overview about different phases of online shopping and mentions some appropriate mechanisms.

Getting information by "browsing": A customer in this situation can be compared to someone who is reading advertisements in a newspaper. Generally, the customer remains entirely *anonymous* in this action. The merchant does not need to get any information about the customer. Inversely the customer should be able to know if the information which she gets from the merchant is authentic. Otherwise the information is of no use to the customer. So the integrity of the information should be protected. The information does not need to be accountable, because the customer does not necessarily need to be able to prove the authenticity of the information to third parties.

The customer's identity manager must verify the merchant's authenticity. If the customer wants to be entirely anonymous and unobservable, her anonymity must be protected by using a service that provides anonymity and unobservability.

Personal consulting: In this case, the merchant needs to know some information about the customer, because otherwise the merchant is unable to fulfil the customer's wishes, (e.g., an interest in a specific literary genre or in a certain author). For a personalized consultation, the customer has to disclose all necessary information. As in the "browsing" situation, the merchant should prove her authenticity to the customer (e.g., by an appropriate certificate). The integrity of the data, which is exchanged between customer and merchant, should also be protected.

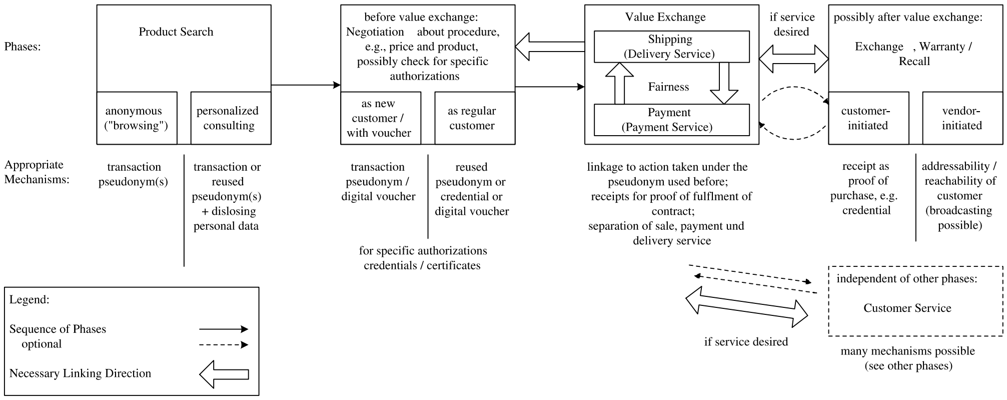
Phases:
Product Search
anonymous ("browsing")
personalized consulting
before value exchange: Negotiation about procedure, e.g., price and product, possibly check for specific authorizations
as new customer / with voucher
as regular customer
Value Exchange
Shipping (Delivery Service)
Fairness
Payment (Payment Service)
if service desired
possibly after value exchange:
Exchange , Warranty / Recall
customer-initiated
vendor-initiated
Appropriate Mechanisms:
transaction pseudonym(s)
transaction or reused pseudonym(s) + dislosing personal data
transaction pseudonym / digital voucher
reused pseudonym or credential or digital voucher
for specific authorizations credentials / certificates
linkage to action taken under the pseudonym used before; receipts for proof of fulflment of contract; separation of sale, payment und delivery service
receipt as proof of purchase, e.g. credential
addressability / reachability of customer (broadcasting possible)
independent of other phases:
Customer Service
if service desired
many mechanisms possible (see other phases)
Legend:
Sequence of Phases
optional
Necessary Linking Direction

Fig. 3. Typical phases of online shopping and mechanisms with respect to identity management.

Negotiation: The customer needs to specify her *preferences* about the data she agrees to transmit to the merchant and what use restrictions apply to this data.

Using stated *policies*, the merchant can specify the data she needs from the customer and the uses and collection purpose for this data.

The task of the identity manager is to negotiate between the preferences of the customer and the policies of the merchant. If no agreement can be found, the action cannot take place.

Value exchange: If the customer wants to buy a book from the merchant, the transaction should be legally binding. Therefore the customer must use the same pseudonym for the entire transaction. If the customer wants to pay with digital money, she must be able to transfer this money using her pseudonym. If she wants to pay using traditional means of payment, she must link some personal data to her pseudonym (e.g., her credit card number and a proof of ability to pay). This personal data must be certified by trusted third parties so that the merchant can be sure that the customer does not cheat.

Other data (e.g., a delivery address) need not be certified because the customer would only harm herself by giving a wrong address.

During the buying transaction the messages transferred between customer and merchant must be accountable. Thus, errors which may occur during the transaction can be proven to third parties (e.g., courts). Accountability is needed to create a legally binding contract of purchase which can also be proven to third parties.

The first task of the identity manager in this situation is to create the appropriate pseudonym. In some cases it is reasonable that the customer uses the same pseudonym in multiple purchases (e.g., if the merchant gives discounts when a customer buys in the merchant's store frequently). In this case the identity manager has to give the customer the option to choose between different pseudonyms: a newly created pseudonym providing more anonymity, or an already used pseudonym with advantages in the purchase.

If a credential is needed, the identity manager must request it from the issuing organization and link it to the pseudonym.

Complaint or exchange: In case of a complaint or desire for exchanging the book, the customer must prove to the merchant that she really did buy the book at the merchant's store. Therefore she must have stored the electronic contract or a receipt of the purchase and show it to the merchant. In this situation, the customer can reuse the pseudonym of the purchase.

Customer service: This phase is independent of the others because customer service has no fixed location in the sequence of shopping phases. It may consist of different tasks which are already described in the other phases, e.g., consulting, negotiation, value exchange, or complaint. Customer service is not always merchant-initiated, but according to the idea of "request marketing" – may be customer-initiated as well.

Additional services: In the scenario of an online purchase we can think of some additional services (e.g., gifts to third parties, payment by third parties, or issuance of credit notes or vouchers):

Gifts to third parties can be made if the customer specifies a different delivery address. Therefore, the identity manager must offer the customer the possibility to individually choose the data linked to the pseudonym.

If a customer wants a third party to pay, she must own an authorization which tells the merchant that the third party will pay. This authorization can be given to the merchant in terms of a credential that is linked to the customer's pseudonym.

Likewise anonymous credit notes or vouchers can be issued by the merchant in terms of credentials. If the customer wants to cash in the credit note, she can do it using any desired pseudonym where the credential can be linked to. Thus issuance cannot be linked to cashing in the credit note respectively redeeming a voucher, and the customer remains anonymous.

According to privacy laws like [8], other kinds of additional service have to be provided with respect to personal data: grant of consent, access to personal data, desire for change, desire for removal, and revocation of consent [9] (project DASIT (privacy protection in teleservices, "Datenschutz in Telediensten")). An identity manager should support such user-controlled privacy functions for identifiable and pseudonymous personal data wherever possible.

5.1.2. E-mail

In e-mail communication, the identity manager can be used to send and receive email using different addresses. The identity manager can create and store these addresses as different pseudonyms. There are some different types of addresses respectively pseudonyms the user could imagine:

- One-time pseudonyms enable the user to send e-mails entirely anonymously.
- Pseudonyms function as invisible implicit addresses [17] and facilitate receiving e-mails in a totally anonymous manner.
- Situation pseudonyms support different communication situations which should remain unlinkable for third parties. For example, a user may want to use a pseudonym for her submissions to a discussion panel and another pseudonym for her business-related e-mails.
- Group pseudonyms can be used in a company. Various employees can use the same e-mail address when they act as representatives of the company. Therefore, one could imagine different kinds of group pseudonyms (e.g., pseudonyms where the recipient of a pseudonymous message cannot distinguish between different senders, but within the group using the same pseudonym it may be known which member sent the message).

Additionally the pseudonyms may possess different properties. The task of the identity manager is to create pseudonyms of the intended type and with the suitable properties. The user must be able to choose different pseudonyms for sending e-mail. Furthermore, keys for concealing and authenticating e-mails can be linked to the pseudonyms, similar to the way PGP manages keys in relation to e-mail addresses.

5.1.3. Other applications

There are many other applications where pseudonyms can be used (e.g., auctions, digital elections or e-government):

In an *auction* each user must be recognizable, especially because the offerer must be prevented from bidding for own goods in order to pull up the price. So a type of pseudonyms with restriction to only one per user in an auction must be used. Bidders must not be able to deny their biddings and they must prove their ability to pay the bidden amount of money. When an auction is finished, goods and money must be exchanged between the successful bidder and the offerer in a legally binding manner. Using the same pseudonyms in different auctions, the holder can get feedback ratings from other bidders in order to create a reputation (as in today's online auctions, e.g., http://www.ebay.com). By the reputation, people determine whether or not they want to trade with that user.

Similar to conventional elections, in *digital elections* only entitled voters may vote. Voting authorizations may not be transferred to other persons. Therefore, credentials issued by governmental institutions can be used. No voter may be able to vote multiple times. This must also be enforced if there are different types of votes in one election possible (e.g., absentee, electronic, and personal voting). No vote may be lost, the voter must be able to verify that her vote is counted. After casting a ballot, the voter may not be able to change the vote. To prevent vote buying and voter extortion, the voter must not be able to prove her vote to third parties, and the voting must be executed anonymously (using a pseudonym) so that the ballot box does not know which vote belongs to which user. The ballot box must authenticate itself to the users.

In *e-government applications*, one may be able to get information anonymously from an authority. Employees of an authority may have group pseudonyms to act as a representative of their authority. Also, collections of signatures can be realized in a digital way by using an "is-a-person pseudonym", restricted to one per person, to prevent from signing many times. Of course, user-controlled privacy functions as described at the end of 5.1.1 should fully be implemented in all e-government applications.

5.1.4. Requirements for identity management derived from these scenarios

In most situations, pseudonyms can be used which possess attributes certified by the holder of the pseudonym (*self-authentication*) or by other parties (*external authentication*) where the credentials issued by third parties are linked. Thus, the holder of a pseudonym must be able to transfer properties and credentials to other personal pseudonyms without showing to other parties that these pseudonyms belong to the same holder. In some situations special types of pseudonyms are desired (e.g., group pseudonyms in e-mail communications). We recognize the need for a fluid transition between situations where different types of pseudonyms may be appropriate. With a mere user-side technology and thus without the cooperation of communication partners or third parties, the user cannot reliably be supported in the pseudonym management, but would be on her own to explicitly choose the appropriate pseudonym. Not having the possibility for a more seamless and computer-aided pseudonym switching is quite inconvenient and often difficult. Furthermore, only self-authentication is possible with user-side technology; to increase accountability, the external authentication by other parties is required [18]. Communication-partners technologies and third-parties technologies make both external authentication and the implicit and explicit use of pseudonyms possible. Examining predefined labels characterizing a change of situation (e.g., from browsing to buying) or expressing the need for specific properties or for reusing pseudonyms can lead to seamless use. Additionally, warnings to the user may inform her about specific requirements. An expert mode could be provided for every user to explicitly configure the deployment of pseudonyms or at least to be aware of it.

5.2. Infrastructure

When a user wants to disclose personal data to a communication partner using a pseudonym, it can be linked to the pseudonym by a digital signature, which is issued on this pseudonym. To prevent the user from modifying the data beyond recognition, it must be certified by third parties. For instance, if a service can only be used by authorized users, but the users want to remain anonymous to the service, the users need to show authorizations to the service which are issued by a third party and which are unlinkable to the users' pseudonyms.

Thus, for a comprehensive identity management, third parties must issue such authorizations (i.e., credentials, to the users). In the following, these third parties are called *organizations*. By issuing a credential, an organization certifies that the user owns a specific property or right. For instance, a governmental institution, such as a registration office, may issue credentials on the user's identification data like the name or the date of birth. One could also imagine credentials on the driving licence, age or rights of vote. A bank could certify that a user disposes of a specific amount of money. As stated in the e-commerce scenario, credit notes can also be issued by means of credentials.

When a user gets a credential, she can link it on demand to a pseudonym used during an action. The communication partner receiving the pseudonym verifies the credentials to get the information certified by the credential issuing organizations.

If a communication partner wants to verify a credential, she needs some information of the credential issuing organization enabling her to perform the verification. For this purpose a PKI may be used. The organizations publish keys that can be used to verify the validity of credentials. These keys must be certified by the organizations and published on key servers, so that each potential verifier has access to them. The keys which are needed to verify the certificates of the organizations may be mutually certified and managed by using a PKI.

Thus, we need the following instances (see Fig. 4):

- certification authorities where organizations and users can obtain certificates from,
- key servers where all published (certified) keys can be fetched from, especially the keys used to verify credentials,
- organizations which issue credentials to the users and publish keys to verify these credentials.

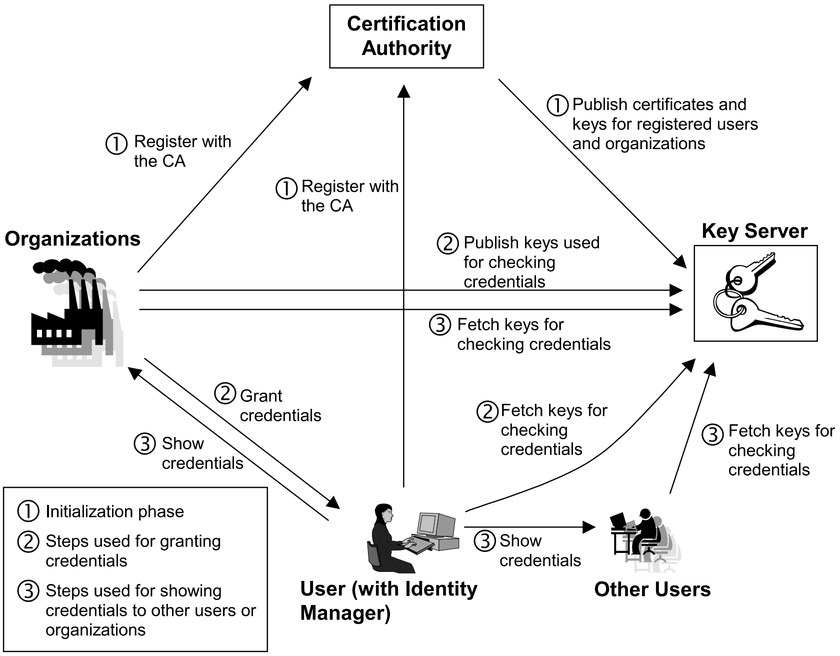
Certification Authority
① Register with the CA
① Register with the CA
① Publish certificates and keys for registered users and organizations
Organizations
Key Server
② Publish keys used for checking credentials
③ Fetch keys for checking credentials
② Grant credentials
③ Show credentials
②Fetch keys for checking credentials
③ Fetch keys for checking credentials
① Initialization phase
② Steps used for granting credentials
③ Steps used for showing credentials to other users or organizations
③ Show credentials
User (with Identity Manager)
Other Users

Fig. 4. Infrastructure of an identity management system using credentials.

A credential system based on [4] is already implemented and will be used in our identity management system.

Additional parties can support the user with her identity management and thus form a particular infrastructure. These third parties comprise trustee services who may act as mediators like identity trustees, value trustees, or liability services. They may specialize on specific actions like payment or delivery services. Providing information about security and privacy risks with respect to deployed identity management systems, is another important task which may be fulfilled by privacy information services or privacy emergency response teams (PERT) analogous to today's computer emergency response teams (CERT).

5.3. Construction of the identity manager

The task of an identity manager is to enable the user to control the nature and amount of personal information that she releases during her electronic communication. To prevent data leaks, the identity manager must be in a trusted device under control of the user. The identity manager should be as universal as possible and not be restricted to specific applications.

Summarized from the descriptions in the sections above, the following requirements to an identity manager exist:

- creation and management of pseudonyms,
- linking of self-certified properties and credentials to pseudonyms,
- management of credentials and requesting credentials from organizations,
- management of preferences about the disclosure and use of personal data,
- management of policies about which personal data one communication partner expects from the other and how to use it,
- configuration and negotiation of user preferences, policies, and types of pseudonyms,
- transmission of pseudonyms to communication partners and verification of certificates and credentials,
- determination of linkability between different pseudonyms of a user; this includes visualization of the user's profile, as far as the identity man-

ager is able to ascertain a profile from the information it gets from the data which is transmitted during an action.

The configuration of the user preferences, policies, and types of pseudonyms can be done in different ways. One option involves the user explicitly defining her wishes and requirements about a communication. On the other hand the preferences, policies, types of pseudonyms, and additional properties can be (pre)configured by the current applications. Many applications will have specific requirements, so that the user will not have to configure many options by hand. For most applications, both ways of configuration will be used.

Policies about demand of personal data and how to use it can be specified using P3P (http://www.w3.org/P3P/). At present there is no standard for the specification of preferences about disclosure and usage of personal data, but there exists a proposal for a language for specification of preference collections regarding P3P, called P3P Preference Exchange Language (APPEL), http://www.w3.org/TR/P3P-preferences.html).

When an application uses the identity manager to communicate with a partner, the following steps will be performed:

1. The application specifies its requirements for the type of pseudonym, the user preferences and policies, and the security of the communication. Most of this can be done by using the data structures of P3P [2].
2. The user is asked to configure the options that the application did not determine according to personal wishes.
3. The identity manager initiates a communication link to the desired partner. First it exchanges the configuration data about the desired security of the communication, the types of pseudonyms to use, and the policies which specify requirements of personal data with the communication partner (respectively her identity manager).
4. The negotiation determines how the communication must be secured, which pseudonyms to use, and what personal data to disclose to the communication partner with a priority on eliminating discovered conflicts during negotiations. This may require interaction with the user. Exchange of configuration data and negotiation must be performed in such a way that it does not affect the anonymity of the user.
5. If conflicts remain, the identity manager aborts the communication and notifies the user about the reasons.
6. Otherwise, the data needed to initiate the communication is exchanged. This data consists of the users' pseudonyms with their properties and credentials, and the information used to initialize the mechanisms to secure the communication link.
7. After initialization, the application starts to communicate using the secured connection to the communication partner.

The identity manager must have interfaces which enable an application to get access to the initialization data of a communication connection. For instance, an application may require the same pseudonym for different connections. Therefore the application must be able to get some information about the pseudonym which is used in a connection.

There exist also requirements for applications that use the identity manager:

- All communication of an application must be performed using the identity manager and the underlying security infrastructure.
- An application should be able to use the configuration interfaces of the identity manager, so that the identity manager is able to do preconfigurations that determine specific requirements of the application and simplify the configuration for the user.
- The application should be designed to disclose the user's personal data, explicitly deploying the identity manager (by means of properties of pseudonyms or credentials). If this is not possible, an application should notify the identity manager of the additionally transmitted personal data by using the corresponding interfaces. The identity manager must control the degree of anonymity of the user.
- Services must be able to communicate to the security infrastructure of the user. Especially they

must specify policies about which personal data they demand from the user and how to use this data.

This shows that traditional applications need modifications for use within a comprehensive identity management system. As a temporary solution, proxies could be used, but in most cases this does not realize the full potential of an identity manager.

The described identity manager is not yet implemented. It will be implemented in SSONET and in a few prototype applications. These are necessary steps towards a comprehensive, application-spanning, and standardized identity management system.

5.4. Integrating identity management into SSONET

In our project, a comprehensive identity manager will be integrated into the security management interface and the underlying security management of SSONET (see Section 4.3). In addition to the configuration of security goals and mechanisms the user will be able to decide which pseudonym she wants to use in the communication and which attributes this pseudonym should possess. She will also be able to configure which personal data she is willing to disclose under which conditions. The configuration and negotiation components must be extended accordingly. The modules at the users' side desired in a comprehensive identity management are shown in Fig. 5.

The lowest layer consists of the anonymous network functions (provided by SSONET and AN.ON), on top we present a library of security functions. SSONET originally only had a few configuration files, which might be regarded as elements in the database layer (see Fig. 2). Now, the user's personal data, including her pseudonyms, credentials, and certificates are stored in a database. Context data, i.e., a structured logfile of known or configured privacy-relevant activity and possibly data of privacy information services, may influence the negotiation components like the defined rules stored in the rule database. All this data may be used from a data mining system on the users' side in order to visualize the current strength of anonymity with respect to pseudonyms and context information and thus gain awareness. Privacy control functionality like in DASIT [9] can supplement the identity management system. The highest layer should provide appropriate interfaces to the user and to applications at the users' side, which should communicate with or via the identity management system.

As can be seen in Fig. 5, SSONET already implements important functionality of identity management. Therefore, it is suitable as an underlying architecture for our system being built. Other technology or methods like credentials, P3P, or DASIT can be added.

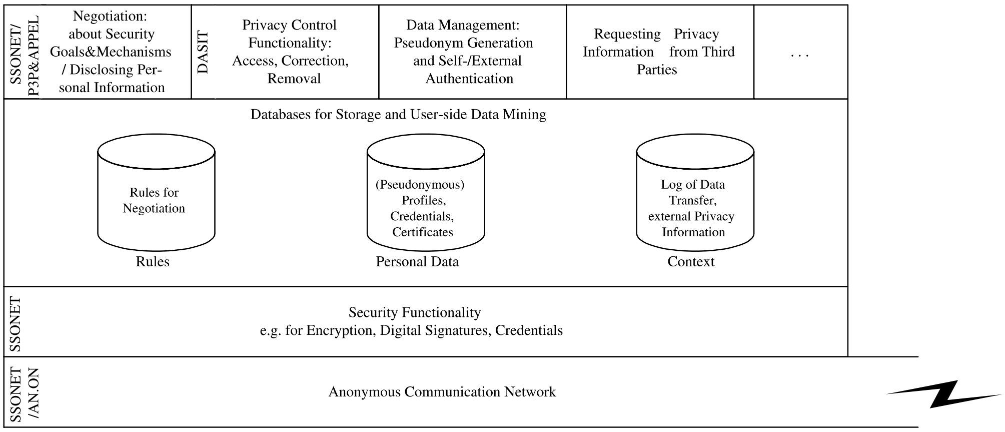
SSONET/ P3P&APPEL
Negotiation: about Security Goals&Mechanisms / Disclosing Personal Information
DASIT
Privacy Control Functionality: Access, Correction, Removal
Data Management: Pseudonym Generation and Self-/External Authentication
Requesting Privacy Information from Third Parties
. . .
Databases for Storage and User-side Data Mining
Rules for Negotiation
Rules
(Pseudonymous) Profiles, Credentials, Certificates
Personal Data
Log of Data Transfer, external Privacy Information
Context
SSONET
Security Functionality
e.g. for Encryption, Digital Signatures, Credentials
SSONET /AN.ON
Anonymous Communication Network

Fig. 5. Modules of an identity management system.

6. Problems with respect to identity management

The growing complexity and decreasing transparency of our world is a serious problem that we cannot solve entirely by an identity manager. This growing complexity increases the difficulty of the identity manager to visualize the degree of privacy in supporting the user, because a potential risk could easily be under- or over-estimated.

If the identity manager serves as the central gateway for personal data in the digital world as it is required for full functionality, users become dependent on such systems. Therefore, confidentiality and integrity as well as availability of the system itself have to be guaranteed; unauthorized use (getting access to the stored data or even taking over the digital identity of the user) has to be prevented.

The identity manager and its infrastructure have to be realized in as trustworthy a fashion as possible (e.g., supported by means of utmost transparency, evaluation, and certification by independent experts for all modules (software, hardware, infrastructure)).

Furthermore, even a trustworthy identity manager could become a risk for privacy itself. Because the identity manager mirrors a great part not only of the user's life, but also parts of the communication partners' lives, other parties such as, e.g., marketing companies, employers, insurances, landlords, or criminals may get the user to disclose stored personal data. Thus, an identity manager is an attractive target for attackers – with all kinds of methods including social engineering or the pressure to accept an adverse compromise. These aspects will have to be discussed further.

7. Conclusion and outlook

After an overview on the state of the art of research and practice in the field of identity management, we described the basic building blocks used in such systems: digital pseudonyms with certified properties and credentials as well as technologies for multilateral security. Thereby we briefly outlined the architecture of SSONET, which enables multilateral security for communication between two parties. Our identity management system will be built as a module or extension to that architecture.

By analyzing different scenarios for an identity management system, we extracted requirements of such a system. Based on these requirements, we described our approach in developing an identity manager, which is under the control of the user, and the infrastructure needed to support it. Finally, we explained problems and risks which arise when using an identity manager and which have to be taken into account while building such a system.

In order to use the Internet as a platform for e-commerce in a secure and privacy-respecting way, identity management systems are essential. On one hand they enable the user to assert her right to informational self-determination and protect her from becoming a "transparent consumer" while using open networks. On the other hand they enable the merchants to perform secure transactions without unacceptably invading into the privacy of their customers.

Identity management supports "multilateral privacy" which can be regarded a subset of multilateral security. Of course multilateral privacy is based on the security functionality implemented, e.g., in SSONET. The combination of security and privacy aspects including the negotiation of the amount of personal data and pseudonym properties is necessary for comprehensive multilateral security. Whereas nowadays mostly isolated pieces for multilaterally secure components exist, comprehensive identity management systems can unite those modules in a complete privacy suite.

Acknowledgements

We would like to thank Andreas Pfitzmann and Mike Gurski for their constructive and very helpful advice.

References

[1] O. Berthold, H. Federrath, M. Köhntopp, Project "Anonymity and unobservability in the Internet", Workshop on Freedom and Privacy by Design, in: Proceedings of the

Tenth Conference on Computers, Freedom & Privacy, April 2000, ACM, New York, 2000, pp. 57–65.

[2] O. Berthold, M. Köhntopp, Identity management based on P3P, in: H. Federrath (Ed.), Designing Privacy Enhancing Technologies, Proceedings of the Workshop on Design Issues in Anonymity and Unobservability, July 2000, LNCS 2009, Springer, Heidelberg, 2001, pp. 141–160.

[3] S. Brands, Rethinking public key infrastructure and digital certificates – building in privacy, thesis, 1999, second edition, MIT Press, Cambridge, MA, August 2000.

[4] J. Camenisch, A. Lysyanskaya, Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation, Research Report RZ 3295 (#93341), IBM Research, November 2000.

[5] D. Chaum, Showing credentials without identification. Signatures transferred between unconditionally unlinkable pseudonyms, in: F. Pichler (Ed.), Advances in Cryptology – EUROCRYPT '85, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, April 1985, LNCS 219, Springer, Heidelberg, 1986, pp. 241–244.

[6] D. Chaum, Security without identification: transaction systems to make big brother obsolete, Communications of the ACM 28 (10) (1985) 1030–1044.

[7] H. Damker, U. Pordesch, M. Reichenbach, Personal reachability and security management – negotiation of multilateral security, in: G. Müller, K. Rannenberg (Eds.), Multilateral Security in Communications, vol. 3, Addison-Wesley, Reading, MA, 1999, pp. 95–111.

[8] 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.

[9] R. Grimm, N. Löhndorf, A. Roßnagel, E-commerce meets E-privacy, in: H. Bäumler (Ed.), E-Privacy, Vieweg, Braunschweig, 2000, pp. 133–140.

[10] L. Harris & Associates, Inc., IBM multi-national consumer privacy survey, New York, October 1999, http://www.ibm.com/services/files/privacy_survey_oct991.pdf.

[11] U. Jendricke, D. Gerd tom Markotten, Usability meets security – the identity-manager as your personal security assistant for the Internet, in: Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC 2000), New Orleans, USA, December 11–15, 2000.

[12] M. Köhntopp, Collection of information on identity management and link list [partly in German and partly in English], 1999–2001, http://www.koehntopp.de/marit/pub/idmanage/.

[13] Pew Internet & American Life Project, Trust and privacy online: why Americans want to rewrite the rules, 2000-08-20, http://pewinternet.org/reports/toc.asp?Report = 19.

[14] A. Pfitzmann, Multilateral security: enabling technologies and their evaluation, in: R. Wilhelm (Ed.), Informatics – 10 Years Back, 10 Years Ahead, LNCS 2000, Springer, Heidelberg, 2001, pp. 50–62.

[15] A. Pfitzmann, M. Köhntopp, Anonymity, unobservability, and pseudonymity – a proposal for terminology, in: H. Federrath (Ed.), Designing Privacy Enhancing Technologies, Proceedings of the Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, Springer, Heidelberg, 2001, pp. 1–9; updated version at http://www.koehntopp.de/marit/pub/anon/Anon_Terminology.pdf.

[16] A. Pfitzmann, A. Schill, A. Westfeld, G. Wicke, G. Wolf, J. Zöllner, A Java-based distributed platform for multilateral security, IFIP/GI Working Conference "Trends in Electronic Commerce", June 1998, Hamburg, LNCS 1402, Springer, Heidelberg, 1998, pp. 52–64.

[17] A. Pfitzmann, M. Waidner, Networks without user observability, Computers & Security 6 (2) (1987) 158–166.

[18] B. Pfitzmann, M. Waidner, A. Pfitzmann, Secure and anonymous electronic commerce: providing legal certainty in open digital systems without compromising anonymity, IBM Research Report RZ 3232 (#93278) 05/22/00 Computer Science/Mathematics, IBM Research Division, Zurich, May 2000, translated and revised version from 1990.

[19] H. van Rossum, H. Gardeniers, J. Borking et al., Privacy-enhancing technologies: the path to anonymity, volume I+II, Achtergrondstudies en Verkenningen 5a/5b, Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Canada, August 1995, http://www.ipc.on.ca/english/pubpres/sum_pap/papers/anon-e.htm.

[20] G. Wolf, A. Pfitzmann, Properties of protection goals and their integration into a user interface, Computer Networks 32 (6) (2000) 685–700.

Sebastian Clauß. From 1994 to 2000 Sebastian Clauß studied computer science at Technische Universität Dresden, Germany. Since then he has been engaged in research on data security and privacy at the same university. He is especially interested in technologies for anonymity and identity management.

Marit Köhntopp received her diploma in computer science in 1995. Since then she has been working at the Privacy Commission Schleswig-Holstein, now called Independent Centre for Privacy Protection. There she is head of the section "privacy enhancing technologies" and involved in several privacy projects, e.g., on anonymity, biometrics, P3P, and the Virtual Privacy Office. Her main interest is realizing privacy protection by identity management systems.